



REPUBLIC OF SINGAPORE

# GOVERNMENT GAZETTE

## BILLS SUPPLEMENT

*Published by Authority*

---

---

NO. 20]

WEDNESDAY, NOVEMBER 5

[2025

---

---

First published in the *Government Gazette*, [www.egazette.gov.sg](http://www.egazette.gov.sg), on 5 November 2025 at 5 pm.

**Notification No. B 20** — The Health Information Bill is published for general information. It was introduced in Parliament on 5 November 2025.



# Health Information Bill

---

---

**Bill No. 20/2025.**

*Read the first time on 5 November 2025.*

## HEALTH INFORMATION ACT 2025

(No. of 2025)

### ARRANGEMENT OF SECTIONS

Section

1. Short title and commencement

#### PART 1

#### PRELIMINARY

2. General interpretation
3. Meaning of “health information”, “administrative information”, “clinical information”, “accessible health information”, “individually-identifiable health information” and “anonymised health information”
4. Purposes of Act
5. Application of Act

#### PART 2

#### NATIONAL ELECTRONIC RECORDS SYSTEM

##### *Division 1 — General*

6. Interpretation of this Part
7. National electronic records system
8. System Operator
9. Application of this Part to contributors, etc., acting through relevant HDI or directly
10. Health information to which this Part applies
11. Consent of individual not required for purposes of this Part

*Division 2 — Contribution of health information*

Section

12. Contribution by specified contributors
13. Contribution by approved contributors
14. Obligations of contributors
15. Directions relating to contribution of health information

*Division 3 — Access, collection and disclosure of accessible health information*

16. Restriction on access, collection or disclosure of accessible health information
17. Access and collection of individual's own accessible health information
18. Authorised individuals of users
19. Access and collection of accessible health information by specified users
20. Access and collection of accessible health information by approved users
21. Disclosure of accessible health information accessed and collected under section 19 or 20
22. Obligations of users
23. Directions relating to access and collection of accessible health information

*Division 4 — Derived information*

24. Interpretation of this Division
25. Applications for derived information
26. Access, collection, disclosure and use of derived information
27. Obligations of requestors
28. Directions relating to requestors

*Division 5 — Access restrictions*

29. Access restrictions
30. Effect of access restrictions
31. Imposition and revocation of access restrictions
32. Access restrictions relating to health information about deceased individuals
33. Transitional provision for this Division

*Division 6 — Action taken in response to contraventions of this Part*

34. Action against contravening contributors, users, etc.

## Section

- 35. Procedure for action against contributors, users, etc., under section 34
- 36. Appeal to Minister
- 37. Minister may designate others to hear appeals

*Division 7 — Offences under this Part*

- 38. Offences relating to improper access or collection of accessible health information by users or authorised individuals of users
- 39. Offences relating to access or collection of accessible health information by unauthorised persons
- 40. Offences relating to unauthorised disclosure of accessible health information
- 41. Offences relating to derived information — requestors
- 42. Offences relating to derived information — other persons

*Division 8 — Miscellaneous*

- 43. Directions relating to access, collection, possession and control of accessible health information by unauthorised persons
- 44. Transitional provisions for this Part

## PART 3

SHARING OF RELEVANT INFORMATION FOR  
SPECIFIED USE CASES

- 45. Interpretation of this Part
- 46. Meaning of “relevant information”
- 47. Meaning of “use case”
- 48. Application of this Part
- 49. Application of this Part to disclosers, etc., acting through health data intermediaries or directly
- 50. Individual’s consent not required under this Part
- 51. Sharing of relevant information under this Part
- 52. Data sharing agreements
- 53. Discloser’s obligations
- 54. Recipient’s obligations
- 55. Collection of relevant information
- 56. Use of relevant information
- 57. Subsequent disclosure of relevant information by recipient
- 58. Notification of data sharing agreements
- 59. Directions for purposes of this Part
- 60. Offences under this Part

## PART 4

SECURITY OF HEALTH INFORMATION AND  
RELEVANT INFORMATION*Division 1 — General*

## Section

61. Interpretation of this Part
62. Meaning of “data breach”
63. Relevant computers or computer systems
64. Application of this Part
65. Designated individual of relevant person

*Division 2 — Data security requirements*

66. Data security and handling of health information and relevant information
67. Retention, disposal and destruction of health information and relevant information

*Division 3 — Cybersecurity requirements*

68. Cybersecurity of relevant computer or computer system

*Division 4 — Miscellaneous*

69. Policies and practices for ensuring data security and cybersecurity
70. Incident management framework
71. Directions relating to relevant persons

## PART 5

NOTIFICATION OF CYBERSECURITY INCIDENTS  
AND DATA BREACHES*Division 1 — General*

72. Interpretation of this Part
73. Application of this Part

*Division 2 — Notification of cybersecurity incidents*

74. Duty to conduct assessment of cybersecurity incident
75. Duty to notify occurrence of notifiable cybersecurity incident

*Division 3 — Notification of data breaches*

76. Interpretation of this Division
77. Notifiable data breaches

## Section

- 78. Duty to conduct assessment of data breach
- 79. Duty to notify occurrence of notifiable data breach
- 80. Duty to notify affected individuals of occurrence of notifiable data breach
- 81. Obligations of relevant HDI of public agency

*Division 4 — Miscellaneous*

- 82. Offences under this Part

## PART 6

RESPONSES TO THREATS AND INCIDENTS  
AFFECTING HEALTH INFORMATION AND  
RELEVANT INFORMATION

- 83. Application of this Part
- 84. Emergency measures and requirements
- 85. Delegation by Minister of powers under this Part

## PART 7

PORTABILITY OF HEALTH INFORMATION  
IN ELECTRONIC FORM

- 86. Application of this Part
- 87. Portability of health information
- 88. Directions under this Part

## PART 8

ADMINISTRATION AND ENFORCEMENT

- 89. Administration of Act
- 90. Codes of practice
- 91. Power to obtain documents and information — authorised officers
- 92. Power to obtain documents and information — investigation officers
- 93. Powers of entry and inspection — authorised officers
- 94. Powers of entry, inspection and search, etc. — investigation officers
- 95. Offence of obstructing, etc., authorised officer or investigation officer in exercise of powers, etc.
- 96. False or misleading statements, documents or information

## Section

97. Disposal of things and documents

## PART 9

## MISCELLANEOUS

98. Legal protections — contributors
99. Legal protections — users
100. Legal protections — requestors
101. Legal protections — System Operator, etc.
102. Legal protections — disclosers
103. Legal protections — recipients
104. Legal protections — others
105. Offences by corporations
106. Offences by unincorporated associations or partnerships
107. Service of documents
108. Jurisdiction of court
109. Composition of offences
110. Exemption
111. Amendment of Schedules
112. Regulations
113. Related amendment to Human Organ Transplant Act 1987
114. Saving and transitional provision
- First Schedule — Contribution of health information by specified contributors
- Second Schedule — Access and collection of accessible health information
- Third Schedule — Written laws under which specified examinations carried out for purposes of section 19(3)
- Fourth Schedule — Disclosure, collection and use of relevant information
-

## A BILL

*intituled*

An Act to provide for a national electronic records system for the safe and secure contribution, collection, storage and disclosure of health information about individuals, to facilitate the collection, disclosure and use of health and other information about individuals to maintain and improve their physical and mental health and wellbeing, and to make a related amendment to the Human Organ Transplant Act 1987.

Be it enacted by the President with the advice and consent of the Parliament of Singapore, as follows:

## Short title and commencement

1. This Act is the Health Information Act 2025 and comes into operation on a date that the Minister appoints by notification in the *Gazette*.

## PART 1

### PRELIMINARY

#### General interpretation

2. In this Act —

“access restriction”, in relation to accessible health information about any individual, has the meaning given by section 29(1);

“approved contributor” means a person or public agency that is approved under section 13(1);

“approved user” means a person or public agency that is approved under section 20(1);

“authorised officer” means a public officer, an officer of a public authority or any other individual who is appointed as such under section 89(1)(a);

“community health service” means a service (other than a licensable healthcare service) that is provided to an individual for or in relation to any of the following purposes:

(a) disease prevention;

(b) the detection of any disease or condition that the individual is or may be suffering from;

(c) where the individual suffers or has suffered from any disease or condition, the rehabilitation of the individual or the alleviation of the disease or condition;

(d) where the individual is or is at risk of being socially isolated or physically or mentally frail, the prevention or mitigation of the individual’s social isolation or frailty;

(e) the assessment of the individual’s need for any healthcare service or another community health service, and the planning for and coordination of the provision of any such service to the individual;

(f) any other purpose that may be prescribed;

5

“computer” means any electronic, magnetic, optical, electrochemical or other data processing device performing logical, arithmetic or storage functions, and includes any data storage facility directly related to or operating in conjunction with any such device, but does not include any device as the Minister may, by notification in the *Gazette*, prescribe;

10

“computer system” means an arrangement of interconnected computers that is designed to perform one or more specific functions, and includes —

(a) an information technology system; and

15

(b) an operational technology system such as an industrial control system, a programmable logic controller, a supervisory control and data acquisition system or a distributed control system;

“contribute”, in relation to health information about an individual, means to contribute that health information to the national electronic records system for the purposes of Part 2;

20

“contributor”, in relation to the national electronic records system, means a specified contributor or an approved contributor;

25

“HCSA licensee” means a person to whom a licence is granted under the Healthcare Services Act 2020 to provide a licensable healthcare service;

“health data intermediary” means a person that processes health information or relevant information on behalf of another person for the purposes of this Act, but does not include an employee of that other person;

30

“health product” has the meaning given by section 2(1) of the Health Products Act 2007;

“healthcare service” and “licensable healthcare service” have the meanings given by section 3(1) of the Healthcare Services Act 2020;

“investigation officer” means a public officer or an officer of a public authority who is appointed as such under section 89(1)(b);

“national electronic records system” means the computer system mentioned in section 7(1);

“process”, in relation to health information or relevant information, means to carry out any operation or set of operations in relation to the health information or relevant information (as the case may be), and includes any of the following:

- (a) to record;
- (b) to hold;
- (c) to organise, adapt or alter;
- (d) to retrieve;
- (e) to combine;
- (f) to transmit or convey;
- (g) to erase or destroy,

and “processing” has a corresponding meaning;

“public agency” means any ministry, department or Organ of State of the Government or a public authority;

“public authority” means a body established or constituted by or under a public Act to perform or discharge a public function, excluding a Town Council established under section 4 of the Town Councils Act 1988;

“qualified pharmacist” means a person who —

- (a) is registered as a pharmacist under the Pharmacists Registration Act 2007;

(b) holds a valid practising certificate granted under that Act; and

(c) is practising pharmacy, whether on a full-time or part-time basis or as a locum;

“relevant HDI” means a health data intermediary that operates a computer or computer system that — 5

(a) processes health information about individuals for the purposes of facilitating and organising the provision of any healthcare service or community health service; and 10

(b) is interconnected with the national electronic records system;

“relevant information” has the meaning given by section 46(1);

“retail pharmacy” and “retail pharmacy business” have the meanings given by regulation 2 of the Health Products (Licensing of Retail Pharmacies) Regulations 2016 (G.N. No. S 330/2016); 15

“retail pharmacy licensee” means a person who holds a licence issued under the Health Products Act 2007 to carry on a retail pharmacy business at or from the retail pharmacy specified in the licence; 20

“specified contributor”, in relation to the national electronic records system, means a person mentioned in section 12(1);

“specified user”, in relation to the national electronic records system, means a person mentioned in section 19(1); 25

“System Operator”, in relation to the national electronic records system, means a person designated under section 8(1);

“user”, in relation to the national electronic records system, means a specified user or an approved user.

**Meaning of “health information”, “administrative information”, “clinical information”, “accessible health information”, “individually-identifiable health information” and “anonymised health information”**

5     **3.—(1)** For the purposes of this Act, “health information” about an individual means administrative information and clinical information about the individual but does not include any administrative information or clinical information that may be prescribed.

10     **(2)** For the purposes of this Act, “administrative information” about an individual means —

(a) information relating to the individual’s use of any healthcare service or community health service;

(b) information relating to the provision of any healthcare service or community health service to the individual;

15     (c) information relating to the individual’s eligibility for financial assistance under any public scheme in respect of the cost or expense of any healthcare service or community health service provided to the individual; or

(d) any other information that may be prescribed,

20     but does not include any clinical information.

*Illustration*

The name, identification number, address and telephone number of an individual who uses a healthcare service or community health service are examples of administrative information about that individual.

25     **(3)** For the purposes of this Act, “clinical information” about an individual means information relating to either or both of the following:

(a) the physical or mental health of the individual;

(b) the diagnosis, treatment or care of the individual.

30     **(4)** For the purposes of this Act, “accessible health information” about any individual means health information about the individual that is made available on the national electronic records system by a System Operator in accordance with this Act.

(5) To avoid doubt, accessible health information about an individual (*P*) does not include the following:

(a) administrative information about *P* that is part of any record made or maintained by a person (*X*) in respect of *P* —

(i) that is identical or substantially similar to administrative information about *P* made available on the national electronic records system; and

(ii) regardless of whether *X* collected that administrative information from the national electronic records system or obtained that administrative information by any other means;

(b) clinical information about *P* that is part of the medical records made or maintained by *X* in respect of *P* —

(i) that is identical or substantially similar to clinical information about *P* made available on the national electronic records system; and

(ii) regardless of whether *X* collected that clinical information from the national electronic records system or obtained that clinical information by any other means.

(6) Health information about an individual is “individually-identifiable health information” for the purposes of this Act if the individual can be identified by a person —

(a) from that health information alone; or

(b) from that health information and other information to which that person has or is likely to have access.

(7) Health information about an individual is “anonymised health information” for the purposes of this Act if it is not individually-identifiable health information.

## Purposes of Act

### 4. The purposes of this Act are —

(a) to provide for the collection, storage and disclosure of health information about individuals using the national electronic records system, including providing for —

(i) the contribution of health information about individuals to the national electronic records system;

(ii) the access and collection of health information about individuals that is made available on the national electronic records system for or in relation to the provision of healthcare services and other purposes permitted under this Act; and

(iii) the access, collection, disclosure and use of information derived from health information about individuals in the national electronic records system for purposes permitted under this Act;

(b) to provide a framework to facilitate the sharing of individually-identifiable information about individuals for purposes relating to —

(i) the provision of healthcare services and community health services; and

(ii) the implementation and facilitation of programmes and schemes to maintain or improve the physical or mental health and wellbeing of individuals; and

(c) to ensure that the confidentiality, integrity and availability of health information and relevant information about individuals is protected.

## Application of Act

5.—(1) Except as provided in subsection (2), the following provisions of this Act apply to the Government:

(a) Part 3, except section 58;

(b) sections 12, 13, 14, 16, 18, 19, 20, 21, 22, 25, 26 and 27.

(2) Nothing in this Act renders the Government liable for prosecution for an offence under this Act.

(3) To avoid doubt, a person is not immune from prosecution for any offence under this Act by reason only that the person —

(a) is employed by, seconded to or engaged to provide services to the Government; or 5

(b) provides, as a volunteer, any service —

(i) to the Government; or

(ii) to any other person acting on behalf of the Government. 10

(4) Unless otherwise expressly provided in this Act, nothing in this Act affects any authority, right, privilege or immunity conferred, or any obligation or limitation imposed, by or under any other written law or any rule of law, contract or rule of professional conduct or ethics. 15

## PART 2

### NATIONAL ELECTRONIC RECORDS SYSTEM

#### *Division 1 — General*

#### **Interpretation of this Part**

6. In this Part — 20

“derived information” means health information that is derived from accessible health information about one or more individuals, and includes an extract or a copy of any such accessible health information;

“enlisted personnel” means an individual who — 25

(a) is a person mentioned in section 3 of the Singapore Armed Forces Act 1972; or

(b) is appointed to, or is enlisted or deemed to be enlisted in, the Singapore Civil Defence Force constituted under the Civil Defence Act 1986; 30

“excluded purpose”, in relation to the access or collection of accessible health information about an individual (*P*), means any of the following purposes:

- 5                   (a) determining *P*’s suitability or eligibility for —
- (i) employment or appointment to office;
- (ii) promotion in employment or office or continuance in employment or office; or
- (iii) removal from employment or office;
- 10                  (b) determining *P*’s suitability or eligibility to be engaged by any person under a contract for services and the terms on which *P* is so engaged;
- (c) determining whether —
- (i) *P*’s engagement by any person under a contract for services should be terminated; or
- 15                   (ii) the terms of a contract for services between *P* and any person should be modified;
- (d) determining *P*’s suitability or eligibility to enter into a platform work agreement with any platform operator and the terms of any such platform work agreement;
- 20                  (e) where *P* is a platform worker, determining whether —
- (i) a platform work agreement between *P* and any platform operator should be terminated; or
- 25                   (ii) the terms of a platform work agreement between *P* and any platform operator should be modified;
- 30                  (f) deciding whether to insure *P* or any other individual, or to continue or renew the insurance (whether on the same or different terms) of *P* or any other individual;

(g) making a claim on the insurance of *P* or any other individual, or processing a claim made on the insurance of *P* or any other individual;

(h) any other purpose that may be prescribed;

“platform operator” has the meaning given by section 4(1) of the Platform Workers Act 2024; 5

“platform work agreement” has the meaning given by section 2 of the Platform Workers Act 2024;

“platform worker” has the meaning given by section 5(1) of the Platform Workers Act 2024; 10

“requestor” means a person who is approved to obtain derived information under section 25(2) or (3);

“specified purpose”, in relation to the access or collection of accessible health information about any individual, means a purpose mentioned in section 19(2). 15

### **National electronic records system**

7.—(1) For the purposes of this Act, “national electronic records system” means the computer system established by the Government for the collection, storage and disclosure of health information about individuals and operated by a System Operator in accordance with this Part, and which comprises — 20

(a) the repository of that health information; and

(b) the electronic means that is operated, maintained and used for the collection, storage and disclosure of that health information. 25

(2) The national electronic records system includes the computer servers and network equipment operated, maintained or used by a System Operator for the purposes of or in relation to the computer system mentioned in subsection (1), whether or not the computer servers and network equipment are owned by the System Operator. 30

## System Operator

8.—(1) The Minister may, by order in the *Gazette*, designate any person as a System Operator to operate, administer and maintain the national electronic records system.

5 (2) To avoid doubt, the operation, administration and maintenance of the national electronic records system include —

(a) the collection of health information contributed by contributors in accordance with this Part;

(b) the making available, in accordance with this Part, of —

10 (i) accessible health information to users; and

(ii) derived information to requestors; and

(c) the processing of health information for the purposes of and in accordance with this Act.

15 (3) A System Operator must operate, administer and maintain the national electronic records system in accordance with any directions given by the Minister.

## Application of this Part to contributors, etc., acting through relevant HDI or directly

20 9.—(1) This Part applies equally to both a contributor who contributes health information through a relevant HDI, and a contributor who contributes health information directly.

(2) This Part applies equally to both a user who accesses or collects accessible health information through a relevant HDI, and a user who accesses or collects accessible health information directly.

25 (3) This Part applies equally to both a requestor who obtains derived information through a relevant HDI, and a requestor who obtains derived information directly.

## Health information to which this Part applies

30 10.—(1) This Part applies to and in relation to health information about any individual who —

(a) is a citizen or permanent resident of Singapore;

- (b) is issued with a foreign identification number; or
- (c) belongs to any other class of individuals that may be prescribed.

(2) In subsection (1)(a), “permanent resident of Singapore” has the meaning given by section 2 of the Immigration Act 1959. 5

### **Consent of individual not required for purposes of this Part**

**11.—**(1) Despite any other written law or rule of law, or any obligation under contract, the consent of an individual (*P*) is not required for any of the following that is done in accordance with and for the purposes of this Part: 10

- (a) the contribution of health information about *P*;
- (b) the access, collection and disclosure of accessible health information about *P*;
- (c) the access, collection, disclosure and use of derived information derived from accessible health information about *P*. 15

(2) Nothing in this Part allows a person to access, collect, disclose or use accessible health information about an individual on the basis that the individual consents or has consented to the person accessing, collecting, disclosing or using (as the case may be) the accessible health information. 20

#### *Division 2 — Contribution of health information*

### **Contribution by specified contributors**

**12.—**(1) A person (called a specified contributor) that is —

- (a) an HCSA licensee specified in, or belonging to a class of HCSA licensees specified in, the first column of Part 1 of the First Schedule; 25
- (b) a retail pharmacy licensee specified in, or belonging to a class of retail pharmacy licensees specified in, the first column of Part 1 of the First Schedule; or 30

(c) a person (other than an HCSA licensee or a retail pharmacy licensee) or public agency specified in, or belonging to a class of persons or public agencies specified in, the first column of Part 1 of the First Schedule,

5 must contribute health information about any individual in accordance with this Part.

(2) An HCSA licensee mentioned in subsection (1)(a) must contribute the types of health information specified opposite the HCSA licensee in the second column of Part 1 of the First Schedule  
10 about any individual who is a patient of the HCSA licensee.

(3) A retail pharmacy licensee mentioned in subsection (1)(b) must contribute the types of health information specified opposite the retail pharmacy licensee in the second column of Part 1 of the First Schedule about any individual to whom a qualified  
15 pharmacist employed or engaged by the retail pharmacy licensee sells or dispenses any health product.

(4) A person or public agency (*X*) mentioned in subsection (1)(c) must contribute the health information specified opposite *X* in the second column of Part 1 of the First Schedule about any individual to  
20 whom *X*, or any individual employed or engaged by *X* or any enlisted personnel of *X*, provides any healthcare service or community health service.

### **Contribution by approved contributors**

13.—(1) The Minister may approve any person or public agency to  
25 contribute health information about any individual in accordance with this Part.

(2) The Minister must, as soon as is practicable after a person or public agency is approved as an approved contributor, publish a notification in the *Gazette* specifying all of the following:

- 30
- (a) the class or classes of individuals whose health information the approved contributor may contribute;
  - (b) subject to subsection (3), the types of health information that the approved contributor may contribute;

- (c) the conditions and restrictions (if any) that the approved contributor must comply with in relation to the contribution of health information.

(3) Where a person or public agency, at the time the person or public agency is approved under subsection (1), is concurrently a specified contributor, the types of health information mentioned in subsection (2)(b) must not include any type of health information that the person or public agency is required to contribute in accordance with section 12.

(4) An approved contributor must, in relation to the contribution of health information under this section, comply with all conditions and restrictions mentioned in subsection (2)(c), if applicable.

(5) The Minister may, by written notice at any time, revoke the approval of an approved contributor.

### **Obligations of contributors**

**14.—**(1) In addition to the conditions and restrictions mentioned in section 13(2)(c) (if applicable), a contributor must comply with all requirements, conditions and restrictions relating to the contribution of health information that may be prescribed.

(2) Without limiting subsection (1), the requirements, conditions and restrictions mentioned in that subsection include the following:

(a) requirements relating to —

(i) the format in which the health information is to be contributed; or

(ii) the software (including any Application Programming Interface) that a contributor or a relevant HDI of a contributor is to use in or for any computer or computer system that interconnects with the national electronic records system;

(b) requirements relating to the accuracy and completeness of health information that is or is to be contributed;

(c) the time at which or period within which the contributor is to contribute health information;

(d) any computer or computer system, or any website, that the contributor may use to contribute health information.

5 (3) For the purposes of subsection (1), different requirements, conditions or restrictions may be prescribed in relation to different contributors or classes of contributors and different types of health information.

10 (4) A contributor must comply with every administrative instruction or technical requirement of a System Operator in relation to the contribution of health information.

### **Directions relating to contribution of health information**

15 **15.**—(1) If a specified contributor fails or neglects to contribute health information about one or more individuals in accordance with section 12(2), (3) or (4), the Minister may, by written notice, direct the specified contributor to contribute the health information about that individual or those individuals within the time and in the form and manner specified by the Minister.

(2) If a specified contributor fails or neglects to comply with —

20 (a) any requirement, condition or restriction mentioned in section 14(1); or

(b) any administrative instruction or technical requirement of a System Operator mentioned in section 14(4),

25 the Minister may, by written notice, direct the specified contributor to comply with the requirement, condition, restriction, administrative instruction or technical requirement (as the case may be) within the time and in the form and manner specified by the Minister.

(3) If an approved contributor fails or neglects to comply with —

(a) any condition or restriction mentioned in section 13(2)(c);

30 (b) any requirement, condition or restriction mentioned in section 14(1); or

- (c) any administrative instruction or technical requirement of a System Operator mentioned in section 14(4),

the Minister may, by written notice, direct the approved contributor to comply with the requirement, condition, restriction, administrative instruction or technical requirement (as the case may be) within the time and in the form and manner specified by the Minister.

(4) A person who, without reasonable excuse, fails to comply with the Minister's direction under subsection (1), (2) or (3) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$20,000 or to imprisonment for a term not exceeding 12 months or to both and, in the case of a continuing offence, to a further fine not exceeding \$1,000 for every day or part of a day during which the offence continues after conviction.

### *Division 3 — Access, collection and disclosure of accessible health information*

#### **Restriction on access, collection or disclosure of accessible health information**

**16.—(1)** A person may access, collect or disclose accessible health information about an individual only if the access, collection or disclosure —

- (a) is carried out in accordance with this Part; or
- (b) is required or permitted under any other written law.

(2) Access, collection or disclosure of accessible health information about an individual is not considered to be required or permitted under any written law merely because the individual has consented or has given his or her consent to it in accordance with Part 4 of the Personal Data Protection Act 2012, or such consent is not required under that Part.

#### **Access and collection of individual's own accessible health information**

**17.—(1)** An individual (*P*) or an authorised representative of *P* may access and collect accessible health information about *P* in any manner prescribed.

(2) In subsection (1), an authorised representative of *P* means any of the following persons:

(a) if *P* is an individual who has not attained 21 years of age —  
*P*'s parent, adoptive parent, step-parent or guardian;

(b) if *P* lacks capacity within the meaning given by section 4 of the Mental Capacity Act 2008 —

(i) a deputy appointed or deemed to be appointed for *P* by the court under that Act with power in relation to *P*'s personal welfare;

(ii) a donee under a lasting power of attorney registered under that Act with power in relation to *P*'s personal welfare; or

(iii) where there is no deputy mentioned in sub-paragraph (i) or donee mentioned in sub-paragraph (ii), an individual who is 21 years of age or older and is —

(A) *P*'s spouse;

(B) a son or daughter of *P*;

(C) *P*'s parent, adoptive parent, step-parent or guardian;

(D) a brother or sister of *P*; or

(E) any other person who is responsible for the care and wellbeing of *P*;

(c) if *P* is an individual who is 21 years of age or older and does not lack capacity within the meaning given by section 4 of the Mental Capacity Act 2008 — an individual whom *P* has authorised to act on *P*'s behalf to access and collect accessible health information about *P*.

(3) A System Operator must comply with any directions given by the Minister in relation to the type or types of accessible health information about *P* that *P* or an authorised representative of *P* may access and collect under subsection (1).

## Authorised individuals of users

**18.—(1)** For the purposes of this Part, “authorised individual” of a specified user means any individual who —

(a) is any of the following:

(i) an individual who is employed or engaged by the specified user; 5

(ii) an enlisted personnel of the specified user;

(iii) an individual who provides, as a volunteer, any service to the specified user or to any other person acting on behalf of the specified user; 10

(b) is specified, or belongs to any class of individuals specified opposite the specified user in the second column of Part 1 of the Second Schedule;

(c) is authorised by the specified user to access and collect accessible health information about any individual in the ordinary course of the individual’s duties for the specified user; and 15

(d) is approved by a System Operator.

**(2)** For the purposes of this Part, “authorised individual” of an approved user means an individual who — 20

(a) is any of the following:

(i) an individual who is employed or engaged by the approved user;

(ii) an enlisted personnel of the approved user;

(iii) an individual who provides, as a volunteer, any service to the approved user or to any other person acting on behalf of the approved user; and 25

(b) is specified (by name or description), or belongs to a class of individuals specified, in the notification published in respect of the approved user in accordance with section 20(2). 30

## Access and collection of accessible health information by specified users

19.—(1) A person (called a specified user) that is —

- 5 (a) an HCSA licensee specified in, or belonging to a class of HCSA licensees specified in, the first column of Part 1 of the Second Schedule;
- (b) a retail pharmacy licensee specified in, or belonging to a class of retail pharmacy licensees specified in, the first column of Part 1 of the Second Schedule; or
- 10 (c) any other person or any public agency specified in, or belonging to a class of persons or public agencies specified in, the first column of Part 1 of the Second Schedule,

may access and collect accessible health information about an individual (*P*) in accordance with this Part, but only for a purpose specified in subsection (2) (called in this Part a specified purpose).

(2) The purposes mentioned in subsection (1) are the following:

- 15 (a) the provision of a healthcare service to *P* (other than carrying out any specified examination of *P*), but not the provision of a healthcare service for an excluded purpose;
- 20 (b) carrying out any specified examination of *P*, and any purpose relating to the carrying out of the specified examination.

(3) In subsection (2), “specified examination” of an individual means any medical, dental, psychiatric or psychological examination, test or assessment of the individual that is required or authorised by or under, or is necessary for the purpose of complying with, any written law specified in the Third Schedule or any order made under a written law specified in that Schedule.

(4) An authorised individual (*X*) of a specified user may access and collect accessible health information about *P* if, and only if, all of the following are satisfied:

- 30 (a) the access and collection of the information by *X* is necessary to enable *X* to perform or discharge his or her duties for the specified user;

- (b) *X*'s duties mentioned in paragraph (a) relate to the specified user carrying out a specified purpose.

### **Access and collection of accessible health information by approved users**

**20.**—(1) The Minister may approve any person or public agency to access and collect accessible health information about any individual (*P*) for any of the following purposes: 5

- (a) the provision of any healthcare service to *P* by the person or public agency or any individual employed or engaged by that person or public agency, but not the provision of any healthcare service for an excluded purpose; 10
- (b) the provision of any community health service to *P* by the person or public agency or any individual employed or engaged by that person or public agency, but not the provision of any community health service for an excluded purpose; 15
- (c) any public health purpose.

(2) The Minister must, as soon as is practicable after a person or public agency is approved as an approved user, publish a notification in the *Gazette* specifying all of the following: 20

- (a) the class or classes of individuals whose accessible health information the approved user may access and collect;
- (b) the purpose or purposes mentioned in subsection (1) for which the approved user may access and collect accessible health information; 25
- (c) the types of accessible health information that the approved user may access and collect;
- (d) the authorised individuals (by name or description) or class or classes of authorised individuals of the approved user who may access and collect those types of accessible health information; 30

(e) the conditions and restrictions (if any) that the approved user must comply with in relation to the access, collection and retention of accessible health information.

5 (3) An approved user must, in relation to the access and collection of accessible health information under this section —

(a) comply with all conditions and restrictions mentioned in subsection (2)(e); and

10 (b) ensure that every authorised individual mentioned in subsection (2)(d) complies with the conditions and restrictions mentioned in subsection (2)(e).

(4) The Minister may, by written notice at any time, revoke the approval of an approved user.

### **Disclosure of accessible health information accessed and collected under section 19 or 20**

15 **21.**—(1) A specified user must not disclose accessible health information about any individual that is accessed and collected in accordance with section 19 except to any individual employed or engaged by the specified user (*X*) in accordance with subsection (3).

20 (2) An authorised individual of a specified user must not disclose accessible health information about any individual that is accessed and collected in accordance with section 19 except to any other individual employed or engaged by the specified user (also *X*) in accordance with subsection (3).

25 (3) The specified user or authorised individual of the specified user may disclose the accessible health information to *X* if, and only if, all of the following are satisfied:

(a) the disclosure of the accessible health information to *X* is necessary to enable *X* to perform or discharge his or her duties for the specified user;

30 (b) *X*'s duties mentioned in paragraph (a) relate to the carrying out of a specified purpose;

- (c) the accessible health information disclosed to *X* is no more than is necessary to enable *X* to perform or discharge those duties.

(4) An approved user must not disclose accessible health information about any individual that is accessed and collected in accordance with section 20 except to any individual employed or engaged by the approved user (*Y*) in accordance with subsection (6).

(5) An authorised individual of an approved user must not disclose accessible health information about any individual that is accessed and collected in accordance with section 20 except to any other individual employed or engaged by the approved user (also *Y*) in accordance with subsection (6).

(6) The approved user or authorised individual of the approved user may disclose the accessible health information to *Y* if, and only if, all of the following are satisfied:

- (a) the disclosure of the accessible health information to *Y* is necessary to enable *Y* to perform or discharge his or her duties for the approved user;
- (b) *Y*'s duties mentioned in paragraph (a) relate to the carrying out of a purpose specified in the notification published in respect of the approved user in accordance with section 20(2);
- (c) the accessible health information disclosed to *Y* is no more than is necessary to enable *Y* to perform or discharge those duties.

## Obligations of users

22.—(1) A user must —

- (a) in addition to the conditions and restrictions mentioned in section 20(2)(e) (if applicable), comply with all requirements, conditions and restrictions relating to the access, collection, retention and disclosure of accessible health information that may be prescribed;
- (b) establish and implement appropriate policies and practices to ensure that the authorised individuals of the user access,

collect, retain and disclose accessible health information in accordance with this Part; and

(c) ensure that every authorised individual of the user complies with —

5 (i) the requirements, conditions and restrictions mentioned in paragraph (a); and

(ii) the policies and practices mentioned in paragraph (b).

10 (2) Without limiting subsection (1)(a), the requirements, conditions and restrictions mentioned in that provision include the following:

15 (a) requirements relating to the software (including any Application Programming Interface) that a user or a relevant HDI of a user is to use in or for any computer or computer system that interconnects with the national electronic records system;

(b) any computer or computer system, or any website, that a user may use to access and collect accessible health information.

20 (3) For the purposes of subsection (1)(a), different conditions or restrictions may be prescribed for different users or classes of users.

(4) For the purposes of subsection (1)(b), the policies and practices mentioned in that provision must include policies and practices in respect of any prescribed matters relating to the access, collection, retention and disclosure of accessible health information.

25 (5) A user and every authorised individual of a user must comply with every administrative instruction or technical requirement of a System Operator in relation to the access, collection and disclosure of accessible health information.

30 (6) A user must notify a System Operator, within the prescribed time, and in the form and manner prescribed (if prescribed), of —

(a) the cessation of any individual as an authorised individual of the user for any reason; or

(b) any change in the designation or role in the user's organisation of any authorised individual of the user.

(7) A user who contravenes subsection (1) or (6) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$50,000 or to imprisonment for a term not exceeding 2 years or to both.

5

### **Directions relating to access and collection of accessible health information**

**23.—**(1) The Minister may, by written notice, direct a person concerned to do all or any of the following:

10

(a) stop the access or collection of accessible health information about any individual;

(b) delete or destroy all copies of accessible health information about any individual that are in the possession or under the control of the person concerned;

15

(c) take all reasonable steps —

(i) to retrieve all copies of accessible health information about any individual from any person to whom the person concerned has disclosed the accessible health information; and

20

(ii) to delete or destroy all copies of the accessible health information that are retrieved in accordance with sub-paragraph (i).

(2) If the Minister directs a person concerned to take any action under subsection (1)(b) or (c)(ii), the Minister may additionally direct the person concerned —

25

(a) to delete or destroy the copies of the accessible health information in the manner specified by the Minister; or

(b) to certify that the copies of the accessible health information have been deleted or destroyed.

30

(3) A person who, without reasonable excuse, fails to comply with the Minister's direction under subsection (1) or (2) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding

\$50,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a continuing offence, to a further fine not exceeding \$1,000 for every day or part of a day during which the offence continues after conviction.

5 (4) In this section, “person concerned” means any of the following persons:

(a) an HCSA licensee, where —

10 (i) the HCSA licensee’s licence has expired or lapsed, has been revoked or suspended or is otherwise no longer valid under the Healthcare Services Act 2020; or

(ii) the HCSA licensee voluntarily stops providing any licensable healthcare service to which the licence relates under section 17(1)(a) of that Act;

15 (b) a retail pharmacy licensee whose licence is suspended or revoked under section 27 of the Health Products Act 2007;

(c) a specified user, where —

20 (i) the specified user contravenes section 19(1), 21(1) or (3) or 22(1)(b) or (c);

(ii) any authorised individual of the specified user contravenes section 19(4) or 21(2) or (3);

(iii) the specified user fails to comply with any requirement, condition or restriction mentioned in section 22(1)(a);

25 (iv) the specified user or any authorised individual of the specified user fails to comply with any administrative instruction or technical requirement of a System Operator mentioned in section 22(5);

30 (v) in a case where the specified user accesses or collects accessible health information through a relevant HDI, the relevant HDI fails to comply with any administrative instruction or technical requirement of a System Operator mentioned in section 22(5);

- (vi) the Minister has reason to believe that the specified user or any authorised individual of the specified user is contravening or has contravened section 38(1) or (3) or 40(1), and it is necessary for the specified user to take any action mentioned in subsection (1) in order to prevent or minimise any harm or damage to any individual pending the outcome of any proceedings against the specified user or authorised individual of the specified user (as the case may be) for an offence arising from that contravention; or
  - (vii) the specified user or any authorised individual of the specified user is convicted of an offence arising from a contravention of section 38(1) or (3) or 40(1);
- (d) an approved user, where —
- (i) the approved user's approval is revoked under section 20(4);
  - (ii) the approved user contravenes section 21(4) or (6) or 22(1)(b) or (c);
  - (iii) any authorised individual of the approved user contravenes section 21(5) or (6);
  - (iv) the approved user fails to comply with any requirement, condition or restriction mentioned in section 22(1)(a);
  - (v) the approved user or any authorised individual of the approved user fails to comply with any administrative instruction or technical requirement of a System Operator mentioned in section 22(5);
  - (vi) in a case where the approved user accesses or collects accessible health information through a relevant HDI, the relevant HDI fails to comply with any administrative instruction or technical requirement of a System Operator mentioned in section 22(5);

(vii) the Minister has reason to believe that the approved user or any authorised individual of the approved user is contravening or has contravened section 38(2) or (3) or 40(1), and it is necessary for the approved user to take any action mentioned in subsection (1) in order to prevent or minimise any harm or damage to any individual pending the outcome of any proceedings against the approved user or authorised individual of the approved user (as the case may be) for an offence arising from that contravention; or

(viii) the approved user or any authorised individual of the approved user is convicted of an offence arising from a contravention of section 38(2) or (3) or 40(1).

(5) For the purposes of subsection (4)(c)(vii) and (d)(viii), the Minister must accept the person's conviction as final.

#### *Division 4 — Derived information*

### **Interpretation of this Division**

**24.** In this Division —

“section 25 approval” means an approval granted under section 25(6)(a);

“type 1 derived information” means derived information that is in the form of individually-identifiable health information;

“type 2 derived information” means derived information that is in the form of aggregated or anonymised health information.

### **Applications for derived information**

**25.—(1)** A person who satisfies the prescribed criteria and requirements or a public agency may apply to the Minister to obtain derived information in accordance with this section.

(2) The Minister may approve an application to obtain type 1 derived information if the application is made for a purpose that relates to or promotes public health.

(3) The Minister may approve an application to obtain type 2 derived information if the Minister is satisfied, having regard to the purpose for which the application is made, that it is in the public interest to do so.

(4) An application made under subsection (2) or (3) must — 5

(a) be made to the Minister in the form and manner, and within the time, specified by the Minister;

(b) specify —

(i) every purpose for which the application is made; and

(ii) whether the applicant intends to disclose the derived information obtained (if the application is approved) to any other person or class of persons; and 10

(c) be accompanied by —

(i) any information that may be prescribed; and

(ii) any other information that the Minister may require to decide on the application. 15

(5) If the applicant specifies, in accordance with subsection (4)(b)(ii), that the applicant intends to disclose the derived information obtained (if the application is approved) to any other person or class of persons, the applicant must additionally specify — 20

(a) the identity or description of that person or class of persons; and

(b) every purpose for which the derived information will be disclosed to that person or class of persons. 25

(6) Upon receiving an application under subsection (2) or (3), the Minister may —

(a) approve the application and provide the type 1 derived information or type 2 derived information (as the case may be) to the applicant, subject to any conditions or restrictions in relation to the access, collection, disclosure and use of the derived information that the Minister thinks fit; or 30

(b) reject the application.

(7) If —

(a) the application is an application to obtain type 1 derived information under subsection (2); and

5 (b) the Minister is of the opinion that the purpose specified in the application will be satisfied by the provision of type 2 derived information instead,

the Minister may provide the applicant with type 2 derived information.

10 (8) In deciding whether to approve or reject an application to obtain type 1 derived information under subsection (2), the Minister must have regard, and give such weight as the Minister considers appropriate, to all of the following matters:

15 (a) whether allowing the applicant to obtain type 1 derived information is in the public interest;

(b) whether it is feasible and reasonable for the applicant to obtain the prior consent of the individual or individuals to whom the type 1 derived information relate for the access, collection, disclosure and use of the type 1 derived information;

20

(c) whether the purpose for which the applicant seeks to obtain the type 1 derived information can be satisfied if the applicant is provided with type 2 derived information instead.

25 (9) To avoid doubt, the Minister is not confined to consideration of the matters mentioned in subsection (8) and may take into account any other matter and evidence that may be relevant.

(10) Where the Minister approves an application under subsection (2) or (3), the approval must specify all of the following:

30 (a) the purpose for which the approval is granted;

(b) the individuals (by name or description) or class of individuals employed or engaged by the requestor who

are allowed to access and collect the derived information, each of whom must be an individual who —

- (i) is employed or engaged by the requestor; or
- (ii) provides, as a volunteer, any service to the requestor or to any other person acting on behalf of the requestor;
- (c) if applicable, the person (by name or description) or class of persons to whom the requestor may disclose the derived information and the purpose or purposes of any such disclosure;
- (d) if applicable, whether the requestor may retain the derived information after the purpose specified under paragraph (c) has been fulfilled or otherwise ceases to apply.

(11) The Minister may, upon approving an application under subsection (6)(a), direct the System Operator to provide the type 1 derived information or type 2 derived information (as the case may be) specified in the application to the requestor.

(12) The Minister may, by written notice, revoke an approval granted under subsection (2) or (3).

(13) A requestor who fails to comply with any condition or restriction imposed under subsection (6)(a) on the section 25 approval granted to the requestor shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$50,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a continuing offence, to a further fine not exceeding \$1,000 for every day or part of a day during which the offence continues after conviction.

### **Access, collection, disclosure and use of derived information**

**26.** A requestor may, subject to any condition or restriction imposed on the section 25 approval granted to the requestor, access, collect, disclose and use derived information that the requestor obtained under the section 25 approval for any purpose specified in that approval without the prior consent of any individual to whom the derived information relates.

## Obligations of requestors

27.—(1) A requestor must establish and implement policies and practices to ensure that derived information obtained by the requestor under the section 25 approval granted to the requestor is accessed, collected, disclosed and used in accordance with this Act.

(2) For the purposes of subsection (1), the policies and practices mentioned in that subsection must include policies and practices in respect of any matters prescribed relating to the access, collection, disclosure and use of derived information.

(3) In relation to any type 1 derived information obtained by a requestor in accordance with section 25, the requestor —

(a) must not, except with the prior written approval of the Minister, disclose to any person or class of persons other than a person or class of persons specified in the section 25 approval granted to the requestor (if any) —

(i) the type 1 derived information; or

(ii) aggregated or anonymised health information derived from the type 1 derived information;

(b) must not use, for any purpose other than a purpose specified in the section 25 approval —

(i) the type 1 derived information; or

(ii) aggregated or anonymised health information derived from the type 1 derived information; and

(c) subject to subsection (6) or unless this Act or the section 25 approval otherwise specifies, must delete or destroy the type 1 derived information and all copies thereof after the purpose specified in the section 25 approval has been fulfilled or otherwise ceases to apply.

(4) Subsection (3)(a) includes the disclosure, by the requestor to another person, of aggregated or anonymised health information derived from type 1 derived information where —

(a) the requestor —

- (i) discloses that aggregated or anonymised health information together with any other information; or
- (ii) knows or has reason to believe that the other person has, or is likely to have access to, any other information; and

5

(b) the other information mentioned in paragraph (a)(i) or (ii), when used in conjunction with the aggregated or anonymised health information, identifies or allows for the identification of any individual.

10

(5) Where a requestor obtains type 2 derived information, in accordance with section 25, the requestor —

(a) except with the prior written approval of the Minister, must not disclose the type 2 derived information to any person;

(b) must not use the type 2 derived information for any purpose other than a purpose specified in the section 25 approval granted to the requestor;

15

(c) must not do any act or take any step to identify or cause the identification of any individual from the type 2 derived information except —

20

(i) where it is necessary to do so in connection with the administration or execution of anything under this Act;

(ii) where the identification of the individual is required or permitted under this Act or any other written law, or by an order of court;

25

(iii) where, in the opinion of the Minister, the identification of the individual is necessary for any purpose related to public health; or

(iv) in any other circumstances that may be prescribed; and

30

(d) subject to subsection (6) or unless this Act or the section 25 approval otherwise specifies, must delete or destroy the

type 2 derived information and all copies thereof after the purpose specified in the section 25 approval has been fulfilled or otherwise ceases to apply.

5 (6) Subsection (3)(c) or (5)(d) does not apply to the extent that the requestor is required to retain the type 1 derived information or type 2 derived information (as the case may be) by or under, or for the purpose of complying with, any written law, rule of law or rule of professional conduct or ethics.

10 (7) A requestor who contravenes subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$50,000 or to imprisonment for a term not exceeding 2 years or to both.

### **Directions relating to requestors**

15 **28.**—(1) The Minister may, by written notice, direct a requestor to do all or any of the following:

(a) subject to subsection (2), delete or destroy the derived information the requestor obtained under the section 25 approval granted to the requestor, and all copies of the derived information in the possession or under the control of the requestor;

(b) take all reasonable steps —

(i) to retrieve all copies of the derived information the requestor obtained under the section 25 approval from any person to whom the requestor has disclosed the derived information; and

25 (ii) to delete or destroy all copies of the derived information that are retrieved under sub-paragraph (i).

(2) If the Minister directs the requestor to take any action under subsection (1)(a) or (b)(ii), the Minister may additionally direct the requestor —

(a) to delete or destroy the derived information or the copy or copies of the derived information (as the case may be) in the manner specified by the Minister; or

- (b) to certify that the derived information has been, or the copy or copies of the derived information have been (as the case may be), deleted or destroyed.

(3) A requestor who fails to comply with the Minister's direction under subsection (1) or (2) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$50,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a continuing offence, to a further fine not exceeding \$1,000 for every day or part of a day during which the offence continues after conviction.

### *Division 5 — Access restrictions*

#### **Access restrictions**

**29.—(1)** For the purposes of this Act, an access restriction is a measure that —

(a) prevents the access, collection and disclosure of any accessible health information about an individual (*P*) under this Part (called in this Division a class 1 access restriction); or

(b) restricts the access, collection or disclosure of any accessible health information about an individual (also *P*) under this Part in respect of one or more of the following matters (called in this Division a class 2 access restriction):

(i) the type or types of accessible health information about *P* that may be accessed, collected or disclosed;

(ii) any attribute of or relating to any type of accessible health information about *P* that may be prescribed;

(iii) the applicable person or applicable persons (by name or description) or class of applicable persons who may access, collect or disclose accessible health information about *P*;

(iv) the purpose or purposes for which accessible health information about *P* may be accessed, collected or disclosed;

(v) the time or times at which, or the period or periods during which, accessible health information about *P* may be accessed, collected or disclosed.

(2) For the purposes of subsection (1)(b), the Minister may prescribe different types of class 2 access restrictions in relation to —

(a) different classes of individuals;

(b) different types of accessible health information about an individual;

(c) different attributes of or relating to any type of accessible health information about an individual;

(d) different applicable persons or classes of applicable persons;

(e) different purposes for which accessible health information about an individual may be accessed, collected or disclosed; and

(f) different times at which or different periods during which accessible health information about an individual may be accessed, collected or disclosed.

(3) In this section, “applicable person” means —

(a) a specified user; or

(b) an approved user who is approved to access and collect accessible health information about any individual for a purpose mentioned in section 20(1)(a) or (b),

and includes an authorised individual of any of them.

### **Effect of access restrictions**

**30.—(1)** This section applies in relation to an access restriction in respect of accessible health information about an individual (*P*) that is in force, and applies despite anything in this Part.

(2) Subject to subsections (3), (4) and (5) —

(a) a class 1 access restriction prevents the access, collection and disclosure of accessible health information about *P*; and

(b) a class 2 access restriction allows the access, collection or disclosure of accessible health information about *P* only to the extent permitted under that access restriction. 5

(3) An access restriction does not prevent or restrict the access, collection or disclosure by a user in accordance with section 19, 20 or 21 of any type of accessible health information about *P* that may be prescribed for the purposes of this subsection. 10

(4) An access restriction does not prevent or restrict the access, collection or disclosure of accessible health information about *P* by a user in accordance with section 19, 20 or 21, if the access, collection or disclosure is necessary to respond to an emergency that threatens the life or health of *P*, whether or not *P* consents or is able, at the material time, to consent to the access, collection or disclosure. 15

(5) An access restriction does not prevent or restrict —

(a) the provision of derived information to a requestor in relation to an approval granted by the Minister under section 25(2) or (3); or 20

(b) the access, collection or disclosure of accessible health information about *P* by any person if the access, collection or disclosure is permitted or required under any other Act or by an order of court. 25

(6) The access, collection or disclosure of accessible health information about *P* is not considered to be permitted or required under any Act merely because the individual has consented or has given his or her consent to it in accordance with Part 4 of the Personal Data Protection Act 2012, or such consent is not required under that Part. 30

(7) To avoid doubt, an access restriction does not prevent or restrict —

- (a) the contribution of health information about *P* by a contributor in accordance with this Part; or
- (b) the collection of that health information by a System Operator, in relation to the operation, administration and maintenance of the national electronic records system.

### **Imposition and revocation of access restrictions**

**31.**—(1) An individual may, in respect of accessible health information about the individual, request for —

- (a) the imposition of an access restriction; or
- (b) the revocation of an access restriction that is in force.

(2) Despite subsection (1) or anything in the Mental Capacity Act 2008, a person mentioned in subsection (3) may, in relation to accessible health information about an individual (*P*) who lacks capacity within the meaning given by that Act, request for —

- (a) the imposition of an access restriction in respect of accessible health information about *P*; or
- (b) the revocation of an access restriction in respect of accessible health information about *P* that is in force.

(3) The persons mentioned in subsection (2) are the following:

- (a) a donee of a lasting power of attorney granted by *P* under the Mental Capacity Act 2008, under which *P* confers on the donee authority to make decisions on *P*'s behalf for the purposes of this Part;
- (b) a deputy appointed or deemed to be appointed by the court under section 20 of the Mental Capacity Act 2008 to make decisions on *P*'s behalf for the purposes of this Part.

(4) A request mentioned in subsection (1) or (2) must —

- (a) be made to a System Operator in the form and manner prescribed; and
- (b) be accompanied by any document or information required by the System Operator.

(5) Without limiting subsection (4)(b), a request to impose a class 2 access restriction must be accompanied by information about any matter mentioned in section 29(1)(b) relating to the access restriction to be imposed.

(6) A System Operator may, in relation to a request under subsection (1) or (2), require the individual or person to provide any additional document or information required by the System Operator.

(7) Upon receiving a request mentioned in subsection (1) or (2), the System Operator must impose the access restriction or revoke the access restriction, as the case may be.

### **Access restrictions relating to health information about deceased individuals**

**32.** Section 31 does not apply to or in relation to the revocation of any access restriction imposed in respect of accessible health information about a deceased individual, where the access restriction is in force immediately before the date of death of the deceased individual.

### **Transitional provision for this Division**

**33.** If —

(a) an individual (*P*), before the date of commencement of section 31, notifies the Government to take any measure to prevent or restrict access to accessible health information about *P*; and

(b) the measure mentioned in paragraph (a) is in force immediately before that date,

a class 1 access restriction or class 2 access restriction (as the case may be) in relation to accessible health information about *P* is deemed to be imposed with effect from that date.

*Division 6 — Action taken in response to  
contraventions of this Part*

**Action against contravening contributors, users, etc.**

5 **34.**—(1) Subject to this section and section 35, an authorised officer may in writing direct a System Operator to take any action described in subsection (2) against a contributor or user or an authorised individual of a user (each *X*) if —

10 (a) the authorised officer is satisfied that *X* is contravening or has contravened any requirement under this Part, the contravention of which is not an offence under this Act;

(b) the authorised officer —

15 (i) has reason to believe that *X* is contravening or has contravened any provision of this Act, the contravention of which is an offence under this Act; and

20 (ii) is satisfied that it is necessary to take the action in order to prevent or minimise any harm or damage to the national electronic records system pending the outcome of any proceedings against *X* for an offence arising from any contravention mentioned in sub-paragraph (i);

(c) *X* has been convicted of an offence under this Act; or

(d) the authorised officer is satisfied that the public interest so requires.

25 (2) The actions that an authorised officer may direct a System Operator to take against *X* in respect of any of the circumstances mentioned in subsection (1) are as follows:

(a) where *X* is a contributor — prevent *X* from contributing health information about any individual;

30 (b) where *X* is a user —

(i) prevent *X* and any authorised individual of *X* from accessing or collecting accessible health information about any individual; or

(ii) allow  $X$  and any authorised individual of  $X$  to access or collect only —

(A) the types of accessible health information about any individual that are specified by the authorised officer; or 5

(B) accessible health information about the classes of individuals that are specified by the authorised officer;

(c) where  $X$  is an authorised individual of a user —

(i) prevent  $X$  from accessing or collecting accessible health information about any individual; 10

(ii) allow  $X$  to access or collect only —

(A) the types of accessible health information about any individual that are specified by the authorised officer; or 15

(B) accessible health information about the classes of individuals that are specified by the authorised officer; or

(iii) require the user to appoint an individual approved by the authorised officer to supervise  $X$ 's access and collection of accessible health information; 20

(d) where  $X$  is an authorised individual of a specified user — revoke the approval of  $X$  under section 18(1)(a)(iv).

(3) For the purposes of subsection (1)(c), the authorised officer must accept the person's conviction as final. 25

### **Procedure for action against contributors, users, etc., under section 34**

**35.—**(1) Before giving a direction under section 34, an authorised officer must, unless the authorised officer considers it not practicable or desirable to do so in any particular case, give notice to the contributor, user or authorised individual of a user (each  $X$ ) concerned — 30

- (a) stating that the authorised officer intends to direct a System Operator to take action against *X* under section 34;
- (b) specifying the type of action mentioned in section 34(2) that the authorised officer proposes to direct a System Operator to take, and each instance of contravention that is the subject of the proposed action or the reason or reasons for the proposed action; and
- (c) specifying the time (being not less than 14 days after the date the notice is served on *X*) within which written representations may be made to the authorised officer with respect to the proposed action.

(2) The authorised officer may decide to issue a direction under section 34 for the appropriate action to be taken —

- (a) after considering any written representation made to the authorised officer pursuant to the notice mentioned in subsection (1); or
- (b) after the time specified in the notice under subsection (1)(c), if no representation is so made or any written representation made is subsequently withdrawn.

(3) However, subsection (2) does not apply where *X* has died, is adjudged bankrupt, has been dissolved or wound up or has otherwise ceased to exist.

(4) Where the authorised officer decides to issue a direction under section 34 for the appropriate action to be taken against *X*, the authorised officer must serve a notice of the decision on —

- (a) *X*; and
- (b) a System Operator.

(5) A decision by an authorised officer takes effect only on the date specified in the notice.

(6) A System Operator, on receiving a notice of an authorised officer's decision under subsection (4)(b), must take the action specified in the notice with effect from the date that the decision takes effect under subsection (5).

## Appeal to Minister

**36.—**(1) A contributor or user or an authorised individual of a user that is aggrieved by the decision of an authorised officer to direct a System Operator to take any action against the contributor, user or authorised individual of a user (as the case may be) under section 34 may appeal to the Minister against the decision. 5

(2) An appeal under this section —

(a) must be in writing;

(b) must specify the grounds on which it is made; and

(c) must be made within the prescribed period after the appellant is notified of the authorised officer’s decision that is appealed against. 10

(3) The Minister may reject an appeal that fails to comply with subsection (2).

(4) After consideration of an appeal, the Minister may — 15

(a) reject the appeal and confirm the authorised officer’s decision; or

(b) allow the appeal and substitute or vary the authorised officer’s decision.

(5) The Minister’s decision on an appeal is final. 20

(6) Every appellant must be notified of the Minister’s decision under subsection (4).

(7) An appeal against an authorised officer’s decision does not affect the operation of the decision appealed against or prevent the taking of action to implement the decision. 25

(8) Unless otherwise directed by the Minister, the decision appealed against must be complied with until the determination of the appeal.

## Minister may designate others to hear appeals

**37.—**(1) The Minister may designate any of the following persons to hear and determine, in the Minister’s place, any appeal or a specific appeal under section 36: 30

- (a) the Second Minister (if any) for his or her Ministry;
- (b) any Minister of State, including a Senior Minister of State, for his or her Ministry;
- (c) any Parliamentary Secretary, including a Senior Parliamentary Secretary, to his or her Ministry.

(2) A reference to the Minister in section 36 includes a reference to a person designated under subsection (1).

### *Division 7 — Offences under this Part*

#### **Offences relating to improper access or collection of accessible health information by users or authorised individuals of users**

**38.**—(1) A specified user or an authorised individual of a specified user must not access or collect accessible health information about any individual except for a specified purpose, or as otherwise required or permitted under this Act.

(2) An approved user or an authorised individual of an approved user must not —

- (a) access or collect any type of accessible health information that is not specified in the notification published in respect of that approved user under section 20(2); or
- (b) access or collect accessible health information about any individual except for a purpose specified in that notification, or as otherwise required or permitted under this Act.

(3) A user or an authorised individual of a user (*X*) must not access or collect accessible health information about any individual if —

- (a) either of the following applies:
  - (i) a class 1 access restriction is in force in respect of accessible health information about that individual;
  - (ii) a class 2 access restriction is in force in respect of accessible health information about that individual, and *X*'s access or collection of that accessible health

information is not in accordance with that access restriction; and

- (b) *X*'s access or collection of accessible health information about that individual is not otherwise permitted under section 30(3), (4) or (5). 5

(4) Except in a case where subsection (5) applies, a person who contravenes subsection (1), (2) or (3) shall be guilty of an offence and shall be liable on conviction —

- (a) to a fine not exceeding \$50,000 or to imprisonment for a term not exceeding 2 years or to both, unless paragraph (b) applies; or 10

- (b) if the person has a prior qualifying conviction — to a fine not exceeding \$100,000 or to imprisonment for a term not exceeding 4 years or to both.

(5) A person who contravenes subsection (1), (2) or (3) by accessing or collecting accessible health information about any individual for an excluded purpose shall be guilty of an offence and shall be liable on conviction — 15

- (a) to a fine not exceeding \$100,000 or to imprisonment for a term not exceeding 4 years or to both, unless paragraph (b) applies; and 20

- (b) if the person has a prior qualifying conviction — to a fine not exceeding \$200,000 or to imprisonment for a term not exceeding 7 years or to both.

(6) In subsections (4) and (5), “qualifying conviction” means a conviction for an offence under subsection (4) or (5). 25

(7) It is not a defence in any proceedings for an offence under subsection (4) or (5) that the accused accessed or collected accessible health information about an individual on the basis that the individual has consented or has given his or her consent in accordance with Part 4 of the Personal Data Protection Act 2012 or such consent is not required under that Part. 30

(8) It is not a defence in any proceedings for an offence under subsection (4) or (5) in relation to a contravention of subsection (1)

that the accused accessed or collected accessible health information about an individual for more than one purpose, and any of those purposes is a specified purpose.

5 (9) It is not a defence in any proceedings for an offence under subsection (4) or (5) in relation to a contravention of subsection (2) that the accused accessed or collected accessible health information about an individual for more than one purpose, and any of those purposes is a purpose mentioned in subsection (2)(b).

### 10 **Offences relating to access or collection of accessible health information by unauthorised persons**

15 **39.**—(1) A person who is not a user or an authorised individual of a user must not access or collect accessible health information about any individual for any purpose, unless the access or collection is required or permitted under this Act or any other written law, or by an order of court.

(2) A person who contravenes subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$100,000 or to imprisonment for a term not exceeding 4 years or to both.

20 (3) It is not a defence in any proceedings for an offence under subsection (1) that the accused accessed or collected accessible health information about an individual on the basis that the individual has consented or has given his or her consent in accordance with Part 4 of the Personal Data Protection Act 2012 or such consent is not required  
25 under that Part.

### **Offences relating to unauthorised disclosure of accessible health information**

30 **40.**—(1) A user or an authorised individual of a user must not disclose accessible health information about any individual, or any document that reproduces (fully or substantially) accessible health information about any individual, to any other person, unless the disclosure —

(a) is necessary for the administration or execution of anything under this Act;

- (b) is required or permitted under this Act or any other written law, or by an order of court; or
- (c) is to any person or class of persons to whom, in the Minister's opinion, it is in the public interest to disclose the accessible health information.

5

(2) A person who is not a user or an authorised individual of a user must not disclose accessible health information about any individual, or any document reproducing (fully or substantially) accessible health information about any individual, unless the disclosure is required or permitted under this Act or any other written law, or by an order of court.

10

(3) A person who contravenes subsection (1) shall be guilty of an offence and shall be liable —

- (a) on the first conviction — to a fine not exceeding \$50,000 or to imprisonment for a term not exceeding 2 years or to both; and
- (b) on a second or subsequent conviction — to a fine not exceeding \$100,000 or to imprisonment for a term not exceeding 4 years or to both.

15

(4) A person who contravenes subsection (2) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$100,000 or to imprisonment for a term not exceeding 4 years or to both.

20

(5) A person does not contravene subsection (1) or (2) only because any information about an individual that is disclosed by the person, or is stated or contained in any document disclosed by the person, is identical or substantially similar to accessible health information about that individual.

25

(6) It is a defence in any proceedings for an offence under subsection (3) or (4) for the accused to prove, on a balance of probabilities, that the accused did not know, and had no reason to believe, that the accused had disclosed accessible health information about an individual or a document reproducing (fully or substantially) accessible health information about an individual, as the case may be.

30

(7) It is not a defence in any proceedings for an offence under subsection (3) or (4) that the accused disclosed accessible health information about an individual on the basis that the individual has consented or has given his or her consent in accordance with Part 4 of the Personal Data Protection Act 2012 or such consent is not required under that Part.

### **Offences relating to derived information — requestors**

**41.—(1)** A requestor or an authorised individual of the requestor who, without reasonable excuse —

(a) discloses any type 1 derived information obtained by the requestor in accordance with section 25, in contravention of section 27(3)(a);

(b) uses any type 1 derived information in contravention of section 27(3)(b); or

(c) fails to delete or destroy any type 1 derived information or copies thereof in contravention of section 27(3)(c),

shall be guilty of an offence.

(2) A requestor or an authorised individual of the requestor who, without reasonable excuse —

(a) discloses any type 2 derived information obtained by the requestor in accordance with section 25, in contravention of section 27(5)(a);

(b) uses any type 2 derived information in contravention of section 27(5)(b);

(c) does any act or takes any step to identify or cause the identification of any individual from any type 2 derived information in contravention of section 27(5)(c); or

(d) fails to delete or destroy any type 2 derived information or copies thereof in contravention of section 27(5)(d),

shall be guilty of an offence.

(3) A person convicted of an offence under subsection (1) or (2) shall be liable on conviction —

(a) to a fine not exceeding \$50,000 or to imprisonment for a term not exceeding 2 years or to both, unless paragraph (b) applies; and

(b) if the person has a prior qualifying conviction — to a fine not exceeding \$100,000 or to imprisonment for a term not exceeding 4 years or to both.

5

(4) In this section —

“authorised individual” of a requestor means an individual who is, or belongs to a class of individuals, specified in the approval granted by the Minister to the requestor in accordance with section 25(10)(b);

10

“qualifying conviction” means a conviction for an offence under subsection (1) or (2);

“type 1 derived information” and “type 2 derived information” have the meanings given by section 24.

15

### **Offences relating to derived information — other persons**

**42.—(1)** A person who —

(a) is not a requestor; and

(b) without reasonable excuse, accesses, collects, discloses or uses any information that the person knows or has reason to believe is derived information,

20

shall be guilty of an offence.

(2) A person who —

(a) is not a requestor;

(b) without reasonable excuse, does any act or takes any step to identify or cause the identification of any individual from aggregated or anonymised health information; and

25

(c) knows or has reason to believe that the aggregated or anonymised health information mentioned in paragraph (b) is type 2 derived information within the meaning given by section 24,

30

shall be guilty of an offence.

(3) A person convicted of an offence under subsection (1) or (2) shall be liable on conviction to a fine not exceeding \$100,000 or to imprisonment for a term not exceeding 4 years or to both.

*Division 8 — Miscellaneous*

5 **Directions relating to access, collection, possession and control of accessible health information by unauthorised persons**

43.—(1) This section applies to a person (*X*) that is not a user, or an authorised individual of a user within the meaning of section 18(1) or (2).

10 (2) If —

(a) the Minister has reason to believe that *X* is contravening or has contravened section 39(1), and it is necessary for *X* to take any action mentioned in paragraph (c) or (d) in order to prevent or minimise any harm or damage to any individual pending the outcome of any proceedings against *X* for an offence arising from that contravention; or

(b) *X* is convicted of an offence arising from a contravention of section 39(1),

the Minister may, by written notice, direct *X* —

20 (c) to stop accessing or collecting accessible health information about any individual; and

(d) to delete or destroy all copies of any such accessible health information that is in the possession or under the control of *X*.

25 (3) If the Minister has reason to believe that —

(a) accessible health information about any individual is in the possession or under the control of *X*; and

- (b) *X*'s possession or control of that accessible health information is not required or permitted under this Act or any other written law, or by an order of court,

the Minister may, by written notice, direct *X* to delete or destroy all copies of that accessible health information that is in the possession or under the control of *X*.

(4) If the Minister directs *X* to take any action under subsection (2)(d) or (3), the Minister may additionally direct *X* —

- (a) to delete or destroy the copies of the accessible health information in the manner specified by the Minister; or  
 (b) to certify to the Minister that the copies of the accessible health information have been deleted or destroyed.

(5) A person who, without reasonable excuse, fails to comply with the Minister's direction under subsection (2), (3) or (4) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$50,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a continuing offence, to a further fine not exceeding \$1,000 for each day or part of a day during which the offence continues after conviction.

(6) For the purposes of this section, the possession or control of accessible health information about an individual is not considered to be required or permitted under any written law merely because the individual has consented or has given his or her consent in accordance with Part 4 of the Personal Data Protection Act 2012, or such consent is not required under that Part.

## Transitional provisions for this Part

44.—(1) If —

- (a) a person is party to any contract or agreement with the Government under which the person contributes or agrees to contribute health information about any individual to the national electronic records system;  
 (b) the contract or agreement mentioned in paragraph (a) is in force immediately before the date of commencement of section 13; and

(c) the person is not a person mentioned in section 12(1),  
then the following applies:

(d) the person is deemed to be an approved contributor approved under section 13(1) with effect from that date;

5 (e) all conditions and restrictions (if any) specified in the contract or agreement mentioned in paragraph (a) are deemed to be conditions and restrictions mentioned in section 13(2)(c) that the person must comply with;

10 (f) the Minister must publish a notification in the *Gazette* in respect of the person specifying the matters in section 13(2).

(2) If —

15 (a) a person is party to any contract or agreement with the Government under which the person is allowed to access and collect health information about one or more individuals that is made available on the national electronic records system;

20 (b) the contract or agreement mentioned in paragraph (a) is in force immediately before the date of commencement of section 20; and

(c) the person is not a person mentioned in section 19(1),

then the following applies:

(d) the person is deemed to be an approved user approved under section 20(1) with effect from that date;

25 (e) all conditions and restrictions (if any) specified in the contract or agreement mentioned in paragraph (a) are deemed to be conditions and restrictions mentioned in section 20(2)(e) that the person must comply with;

30 (f) the Minister must publish a notification in the *Gazette* in respect of the person specifying the matters in section 20(2).

(3) A person that —

(a) is a party to any contract or agreement with the Government under which the person is allowed to access and collect health information about one or more individuals that is made available on the national electronic records system; and 5

(b) before the date of commencement of sections 19 and 20 (called in this subsection the relevant date), accesses and collects health information about any individual so made available, 10

may, subject to the provisions of this Act, retain and use that health information on or after the relevant date for the purposes for which the health information was accessed and collected under the contract or agreement mentioned in paragraph (a).

## PART 3 15

### SHARING OF RELEVANT INFORMATION FOR SPECIFIED USE CASES

#### **Interpretation of this Part**

**45.** In this Part —

“data request” means a request by a recipient to a discloser, pursuant to a data sharing agreement, for the disclosure of relevant information about one or more individuals in the possession or under the control of the discloser; 20

“data sharing agreement” means an agreement between a discloser and a recipient that satisfies the requirements mentioned in section 52; 25

“discloser” means a person or public agency who discloses or intends to disclose relevant information in relation to a use case;

“personnel” — 30

(a) in relation to a discloser or recipient, means an individual who —

(i) is employed or engaged by the discloser or recipient, as the case may be; or

(ii) provides, as a volunteer, any service —

(A) to the discloser or recipient, as the case may be; or

(B) to any other person on behalf of the discloser or recipient, as the case may be; or

(b) in relation to a health data intermediary of a discloser or recipient, means an individual who is employed or engaged by the health data intermediary;

“recipient” means a person or public agency who collects or uses, or intends to collect or use relevant information in relation to a use case.

## Meaning of “relevant information”

**46.—(1)** In this Part, “relevant information” about an individual (*P*) means —

(a) any type of administrative information or clinical information about *P*; or

(b) any other type of individually-identifiable information relating to —

(i) *P*; or

(ii) any individual who provides care to *P*, or is responsible for *P*’s care and welfare,

as may be prescribed for a use case.

### *Illustration*

The name and contact information of an individual who is the caregiver for *P* are examples of relevant information about *P*.

(2) For the purposes of subsection (1), different types of relevant information may be prescribed for different use cases.

## Meaning of “use case”

47. In this Part, “use case” means a use case specified in the third column of Part 1 of the Fourth Schedule in relation to which —

- (a) a discloser discloses relevant information about an individual to a recipient; and
- (b) the recipient —
  - (i) collects that relevant information from the discloser; and
  - (ii) uses that relevant information,

for a purpose that comes within the scope of that use case.

## Application of this Part

48.—(1) This Part does not apply to the disclosure, collection and use of accessible health information about any individual.

(2) This Part does not prevent or restrict the disclosure, collection or use of relevant information about any individual in accordance with any other provision of this Act or any other written law or rule of law or by an order of court.

(3) A person is not to be taken to be a discloser or recipient on the basis that the person is a contributor or user under this Act or a requestor within the meaning given by section 6.

(4) To avoid doubt, nothing in this Part imposes an obligation on a discloser to collect relevant information about any individual for the purpose of enabling the discloser to disclose the relevant information to any recipient under this Part.

## Application of this Part to disclosers, etc., acting through health data intermediaries or directly

49.—(1) This Part applies equally to both a discloser who discloses relevant information about any individual through a health data intermediary, and a discloser who discloses relevant information directly.

(2) This Part applies equally to both a recipient who collects or uses relevant information about any individual through a health data

intermediary, and a recipient who collects or uses relevant information directly.

### **Individual’s consent not required under this Part**

5 **50.**—(1) Despite any other written law or rule of law or any obligation of confidentiality imposed by contract, the consent of an individual (*P*) is not required for the disclosure by a discloser of relevant information about *P* to a recipient in accordance with this Part.

10 (2) Despite any other written law or rule of law or any obligation of confidentiality imposed by contract, *P*’s consent is not required for —

(a) a recipient’s collection of relevant information about *P* disclosed by a discloser to the recipient in accordance with this Part; and

15 (b) the recipient’s use of the relevant information mentioned in paragraph (a) in accordance with this Part.

### **Sharing of relevant information under this Part**

**51.**—(1) A discloser (*A*) must not, in relation to a use case, disclose relevant information about any individual to a recipient (*B*) unless *A* —

20 (a) is a person that is specified (by name or description), or belongs to a class of persons that is specified, in the first column of Part 1 of the Fourth Schedule opposite *B* and that use case; and

(b) complies with the requirements under this Part.

25 (2) *B* must not, in relation to a use case —

(a) collect relevant information about any individual from *A*; or

(b) use the relevant information mentioned in paragraph (a), unless *B* —

30 (c) is a person that is specified (by name or description), or belongs to a class of persons that is specified, in the

second column of Part 1 of the Fourth Schedule opposite *A* and that use case; and

(*d*) complies with the requirements under this Part.

## Data sharing agreements

**52.**—(1) This section applies if —

(*a*) a person or public agency (*A*) intends to disclose relevant information about any individual to another person or public agency (*B*) in relation to a use case; and

(*b*) *B* intends to collect and use the relevant information disclosed by *A* in relation to that use case.

(2) *A* must not disclose relevant information about any individual to *B* unless *A* and *B* have entered into an agreement that satisfies the requirements in this section.

(3) The agreement mentioned in subsection (2) must be in writing and must specify all of the following:

(*a*) the particulars of *A* and *B*, including any particulars that may be prescribed;

(*b*) that the agreement is in respect of the disclosure, collection and use of relevant information about any individual in relation to the use case mentioned in subsection (1) in accordance with this Part;

(*c*) subject to subsection (4), every type of relevant information about any individual that may be disclosed, collected and used under the agreement;

(*d*) the personnel of *A* or a health data intermediary of *A* (if any) who is authorised to disclose relevant information about any individual to *B* under the agreement;

(*e*) the personnel of *B* or a health data intermediary of *B* (if any) who is authorised to collect or use relevant information about any individual disclosed by *A* under the agreement;

(*f*) any other matter that may be prescribed.

(4) The type or types of relevant information about any individual specified in the data sharing agreement in accordance with subsection (3)(c) must be no more than the minimum necessary to implement or facilitate the use case mentioned in subsection (1).

5 (5) An agreement that does not satisfy the requirements in subsections (3) and (4) is not a data sharing agreement for the purposes of this Part.

(6) For the purposes of subsection (3)(d) and (e), every personnel of *A* or *B*, or of a health data intermediary of *A* or *B*, must be an individual —

(a) who is specified by name or description in the agreement; or

(b) who belongs to a class of individuals specified in the agreement.

## 15 **Discloser's obligations**

**53.**—(1) A discloser (*A*) must not, in relation to a use case, disclose relevant information about any individual (*P*) to a recipient (*B*) unless all of the following apply:

20 (a) *B* makes a data request to *A* pursuant to a data sharing agreement (called in this section DSA) between *A* and *B* that relates to that use case;

(b) the purpose for which *B* makes the data request comes within the scope of that use case;

25 (c) at the time *A* discloses the relevant information to *B* in response to *B*'s data request, the DSA is in force.

(2) *A* must ensure, before disclosing relevant information about *P* to *B* in response to *B*'s data request, that every type of relevant information to be disclosed to *B* is a type that is specified in the DSA in accordance with section 52(3)(c).

30 (3) *A* must, in relation to the disclosure of relevant information about *P* to *B* in response to *B*'s data request —

- (a) ensure that the relevant information is disclosed only by a personnel of *A* or a health data intermediary of *A* who is specified in the DSA in accordance with section 52(3)(d);
- (b) ensure that the relevant information is disclosed only to a personnel of *B* or a health data intermediary of *B* who is specified in the DSA in accordance with section 52(3)(e);
- (c) make reasonable efforts to ensure that the relevant information that is disclosed —
  - (i) is no more than the minimum that is necessary to implement or facilitate the use case specified in *B*'s data request; and
  - (ii) is accurate and complete; and
- (d) make reasonable efforts to ensure that the relevant information is disclosed in a manner consistent with the DSA.

(4) In addition to subsections (1), (2) and (3), *A* must comply with any conditions or restrictions relating to the disclosure of relevant information that may be prescribed.

(5) For the purposes of subsection (4), different conditions or restrictions may be prescribed for —

- (a) different disclosers or classes of disclosers;
- (b) different use cases; and
- (c) different types of relevant information about any individual.

## Recipient's obligations

**54.—**(1) A recipient (*B*) must not, in relation to a use case, make a data request to a discloser (*A*) for the disclosure of relevant information about any individual in accordance with this Part unless all of the following apply:

- (a) *B*'s data request is pursuant to a data sharing agreement between *A* and *B* that relates to that use case;

(b) the purpose for which *B* makes the data request comes within the scope of that use case;

(c) *B*, having regard to all the circumstances of the use case, genuinely requires the relevant information for the purpose mentioned in paragraph (b).

(2) Despite any other written law or rule of law or any obligation of confidentiality imposed by contract, *B* may, in relation to a data request to *A*, disclose to *A* any information about any individual to whom the data request relates if the disclosure of that information is necessary —

(a) to identify the individual; or

(b) to substantiate, or explain or elaborate on the purpose or scope of, *B*'s data request.

(3) The information about the individual that *B* discloses to *A* under subsection (2) must not be more than the minimum that is relevant to, and is necessary for, the purposes of subsection (2)(a) or (b), as the case may be.

(4) To avoid doubt, a data request may contain a request for the disclosure of relevant information about one or more individuals and on one or more occasions.

(5) In addition to subsections (1) and (2), *B* must comply with any conditions or restrictions relating to the making of a data request that may be prescribed.

(6) For the purposes of subsection (5), different conditions or restrictions may be prescribed for —

(a) different recipients or classes of recipients;

(b) different use cases; and

(c) different types of relevant information about any individual.

## Collection of relevant information

**55.—**(1) A recipient (*B*) that collects, in relation to a use case, relevant information about any individual that is disclosed by a

discloser (*A*) pursuant to a data sharing agreement between *A* and *B* must —

- (a) ensure that the relevant information is collected only by a personnel of *B* or a health data intermediary of *B* who is specified in the data sharing agreement between *A* and *B* in accordance with section 52(3)(e); 5
- (b) make reasonable efforts to ensure that the relevant information is collected in a manner consistent with that data sharing agreement; and
- (c) comply with any condition or restriction in relation to the collection of relevant information under this Part that may be prescribed. 10

(2) For the purposes of subsection (1)(c), different conditions or restrictions may be prescribed for —

- (a) different recipients or classes of recipients; 15
- (b) different use cases; and
- (c) different types of relevant information about any individual.

## Use of relevant information

**56.—**(1) This section applies in relation to the use of relevant information about any individual (*P*) that a recipient (*B*) collects from a discloser (*A*) pursuant to a data sharing agreement between *A* and *B*. 20

(2) The following persons must not use relevant information about *P* except to implement or facilitate a use case specified in the data sharing agreement between *A* and *B*: 25

- (a) *B*;
- (b) a health data intermediary of *B*;
- (c) a personnel of *B*;
- (d) a personnel of a health data intermediary of *B*.

(3) A health data intermediary of *B*, or any personnel of any health data intermediary of *B*, may process relevant information about *P* for 30

the purpose of enabling or facilitating *B*'s use of that relevant information for the use case mentioned in subsection (2).

(4) *B* must ensure that relevant information about *P* is made available to any personnel of *B* or a health data intermediary of *B* only to the extent that is necessary to enable the personnel or health data intermediary (as the case may be) to carry out any function or perform any duty relating to the implementation or facilitation of the use case mentioned in subsection (2).

(5) *B* must comply with any condition or restriction in relation to the use of relevant information under this Part that may be prescribed.

(6) For the purposes of subsection (5), different conditions or restrictions may be prescribed for —

(a) different recipients or classes of recipients;

(b) different use cases; and

(c) different types of relevant information about an individual.

### **Subsequent disclosure of relevant information by recipient**

**57.—**(1) A recipient (*B*) who collects, in relation to a use case, relevant information about any individual that is disclosed by a discloser (*A*) pursuant to a data sharing agreement between *A* and *B* must not disclose that relevant information to any other person unless —

(a) the disclosure of the relevant information is required or permitted by or under this Act or any other written law, or by an order of court; or

(b) the relevant information is disclosed to any person and in any circumstances that may be prescribed.

(2) For the purposes of subsection (1)(a), the disclosure of relevant information about an individual is not considered to be required or permitted under any written law merely because the individual has consented or has given his or her consent in accordance with Part 4 of the Personal Data Protection Act 2012, or such consent is not required under that Part.

(3) To avoid doubt, subsection (1) does not affect the processing of relevant information mentioned in that subsection by a health data intermediary of *B* or any personnel of a health data intermediary of *B* in accordance with section 56(3).

## Notification of data sharing agreements

5

**58.—(1)** The Minister may by regulations require —

(a) a discloser to provide to the Minister —

(i) a copy of any data sharing agreement between the discloser and any recipient; or

(ii) any document or information about any data sharing agreement between the discloser and any recipient that may be prescribed; or

10

(b) a recipient to provide to the Minister —

(i) a copy of any data sharing agreement between the recipient and any discloser; or

(ii) any document or information about any data sharing agreement between the recipient and any discloser that may be prescribed.

15

(2) For the purposes of subsection (1)(a)(ii) and (b)(ii), the document or information about any data sharing agreement between a discloser and a recipient mentioned in those provisions may relate to any of the following:

20

(a) the identity and particulars of the discloser or recipient;

(b) the type or types of relevant health information about any individual that have been disclosed, collected and used under the data sharing agreement;

25

(c) the use cases for which the type or types of relevant health information mentioned in paragraph (b) have been disclosed, collected and used;

(d) the identity and particulars of —

30

(i) any personnel of the discloser or a health data intermediary of the discloser who is authorised to

disclose relevant health information under the data sharing agreement; or

- (ii) any personnel of the recipient or a health data intermediary of the recipient who is authorised to collect or use relevant health information disclosed under the data sharing agreement.

(3) The discloser or recipient must provide the copy of the data sharing agreement or the document or information mentioned in subsection (1)(a) or (b), as the case may be —

(a) within the prescribed time; and

(b) in the form or manner prescribed, if prescribed.

(4) A person who contravenes subsection (3) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$20,000 or to imprisonment for a term not exceeding 12 months or to both.

### **Directions for purposes of this Part**

**59.—**(1) Subsections (2) and (3) apply if the Minister has reason to believe that —

(a) relevant information about any individual —

(i) has been or has purportedly been disclosed by a discloser (*A*); or

(ii) has been or has purportedly been collected or used by a recipient (*B*),

pursuant to a data sharing agreement between *A* and *B* (called in this section the DSA); and

(b) the disclosure, collection or use (as the case may be) of that relevant information is not in accordance with the DSA or the provisions of this Part.

(2) The Minister may, by written notice, direct *A* or *B* to take any one or more of the following actions:

(a) in the case of *A* —

(i) review and assess whether the disclosure or purported disclosure of relevant information about any individual is in accordance with the DSA and the provisions of this Part; or

5

(ii) identify any error, failure, inadequacy or shortcoming relating to the disclosure or purported disclosure of relevant information about any individual pursuant to the DSA, and take reasonable steps to remedy the error, failure, inadequacy or shortcoming and prevent its recurrence;

10

(b) in the case of *B* —

(i) review and assess whether the collection or use or purported collection or use of relevant information about any individual is in accordance with the DSA and the provisions of this Part; or

15

(ii) identify any error, failure, inadequacy or shortcoming in relation to the collection or use or purported collection or use (as the case may be) of relevant information about any individual pursuant to the DSA, and take reasonable steps to remedy the error, failure, inadequacy or shortcoming and prevent its recurrence;

20

## (c) provide to the Minister any document or information that the Minister may reasonably require relating to —

25

(i) the review and assessment conducted in accordance with paragraph (a)(i) or (b)(i), including information relating to the disclosure, collection or use (as the case may be) of relevant information about any individual pursuant to the DSA prior to the review and assessment;

30

(ii) any error, failure, inadequacy or shortcoming identified in accordance with paragraph (a)(ii) or (b)(ii); or

35

(iii) the steps taken to remedy any error, failure, inadequacy or shortcoming identified in accordance with paragraph (a)(ii) or (b)(ii);

(d) take any other action in relation to any matter mentioned in paragraph (a) or (b) that the Minister may reasonably require.

(3) In addition —

(a) where the Minister —

(i) directs *A* to take any action mentioned in subsection (2)(a)(i) or (ii); and

(ii) is of the opinion that *B*'s assistance is required or desirable to enable the proper and effective carrying out of that action by *A*,

the Minister may, by written notice, direct *B* to take all reasonable steps to assist *A*; and

(b) where the Minister —

(i) directs *B* to take any action mentioned in subsection (2)(b)(i) or (ii); and

(ii) is of the opinion that *A*'s assistance is required or desirable to ensure the proper and effective carrying out of that action by *B*,

the Minister may, by written notice, direct *A* to take all reasonable steps to assist *B*.

(4) If —

(a) both of the following apply:

(i) the Minister has reason to believe that *A* has contravened section 52(2) or 53(1), (2) or (3), or any condition or restriction imposed under section 53(4);

(ii) it is necessary for *A* to take any action mentioned in paragraph (c) or (d) in order to prevent or minimise any harm or damage to any individual pending the

outcome of any proceedings against *A* for an offence arising from that contravention; or

(*b*) *A* is convicted of an offence under section 60(1),

the Minister may, by written notice, direct *A* —

(*c*) to stop disclosing relevant information about any individual to any recipient under this Part; or 5

(*d*) to take any other specified action which the Minister reasonably considers to be necessary to bring the contravention to an end and prevent the recurrence of the contravention. 10

(5) If —

(*a*) both of the following apply:

(i) the Minister has reason to believe that *B* has contravened section 52(2), 54(1) or (3), 55(1), 56(2) or (4) or 57(1), or any condition or restriction imposed under section 54(5) or 56(5); 15

(ii) it is necessary for *B* to take any action mentioned in paragraph (*c*), (*d*) or (*e*) in order to prevent or minimise any harm or damage to any individual pending the outcome of any proceedings against *B* for an offence arising from that contravention; or 20

(*b*) *B* is convicted of an offence under section 60(2),

the Minister may, by written notice, direct *B* —

(*c*) to do either or both of the following:

(i) stop collecting relevant information about any individual from any discloser under this Part; 25

(ii) stop using relevant information about any individual collected from any discloser under this Part that is in the possession or under the control of *B*;

(*d*) to delete or destroy relevant information about any individual collected from any discloser under this Part; 30

(e) to take all reasonable steps —

(i) to retrieve all copies of the relevant information about any individual from any person to whom *B* has disclosed the relevant information; and

5 (ii) to delete or destroy all copies of the relevant information that are retrieved under sub-paragraph (i); or

10 (f) to take any other specified action which the Minister reasonably considers to be necessary to bring the contravention to an end and prevent the recurrence of the contravention.

15 (6) A person who, without reasonable excuse, refuses or fails to comply with a direction under subsection (2), (3), (4) or (5) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$50,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a continuing offence, to a further fine not exceeding \$1,000 for every day or part of a day during which the offence continues after conviction.

### Offences under this Part

20 **60.—**(1) A person who, without reasonable excuse, contravenes —

(a) section 52(2) or 53(1), (2) or (3); or

(b) any condition or restriction imposed under section 53(4), shall be guilty of an offence.

(2) A person who, without reasonable excuse, contravenes —

25 (a) section 52(2), 54(1) or (3), 55(1), 56(2) or (4) or 57(1); or

(b) any condition or restriction imposed under section 54(5) or 56(5),

shall be guilty of an offence.

30 (3) A person who is convicted of an offence under subsection (1) or (2) shall be liable on conviction —

(a) to a fine not exceeding \$50,000 or to imprisonment for a term not exceeding 2 years or to both, unless paragraph (b) applies; and

(b) if the person has a prior qualifying conviction — to a fine not exceeding \$100,000 or to imprisonment for a term not exceeding 4 years or to both.

(4) In subsection (3), “qualifying conviction” means a conviction for an offence under subsection (1) or (2).

## PART 4

### SECURITY OF HEALTH INFORMATION AND RELEVANT INFORMATION

#### *Division 1 — General*

#### **Interpretation of this Part**

**61.—(1)** In this Part —

“cybersecurity” means the state in which a computer or computer system is protected from unauthorised access or attack, and because of that state —

(a) the computer or computer system continues to be available and operational;

(b) the integrity of the computer or computer system is maintained; and

(c) the integrity and confidentiality of information stored in, processed by or transmitted through the computer or computer system is maintained;

“cybersecurity incident” means an act or activity carried out without lawful authority on or through a computer or computer system that jeopardises or adversely affects its cybersecurity or the cybersecurity of another computer or computer system;

“discloser” and “recipient” have the meanings given by section 45;

“relevant person” means a person mentioned in section 64(1);

“requestor” has the meaning given by section 6.

(2) For the purposes of this Part, a computer or computer system is taken to process health information or relevant information even though the computer or computer system also processes any information other than health information or relevant information, as the case may be.

### Meaning of “data breach”

**62.** For the purposes of this Part, “data breach”, in relation to health information or relevant information, means —

(a) the unauthorised access, collection, use, disclosure, copying, modification, disposal or destruction of that information; or

(b) the loss of any storage medium or device on which that information is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification, disposal or destruction of that information is likely to occur.

### Relevant computers or computer systems

**63.—(1)** For the purposes of this Part, “relevant computer or computer system” —

(a) means —

(i) a computer or computer system that is interconnected with the national electronic records system;

(ii) a computer or computer system that processes health information or relevant information, whether or not it is interconnected with the national electronic records system or a computer or computer system mentioned in sub-paragraph (i); or

- (iii) a computer or computer system that —
  - (A) processes information other than health information or relevant information; and
  - (B) is interconnected with a computer or computer system mentioned in sub-paragraph (i); but

5

(b) does not include —

- (i) the national electronic records system; or
- (ii) any computer or computer system mentioned in paragraph (a) that may be prescribed.

(2) A relevant computer system of a person includes the computer servers and network equipment operated or used by the person for the purposes of or in relation to the relevant computer system, whether or not the computer servers and network equipment are owned by that person.

10

### **Application of this Part**

15

**64.—**(1) Except as otherwise provided, this Part applies to the following persons (called in this Part a relevant person):

- (a) a contributor;
- (b) a user;
- (c) a requestor;
- (d) a System Operator;
- (e) a discloser;
- (f) a recipient.

20

(2) This Part does not apply to the Government or any public authority.

25

(3) This Part applies equally to and in relation to health information processed by a relevant HDI on behalf of and for the purposes of a contributor or user, and health information processed by a contributor or user directly.

(4) Unless otherwise expressly provided, this Part does not affect —

30

- (a) the operation of any other written law that applies to or in relation to the cybersecurity of any computer or computer system; or
- (b) the obligations of any person under any written law mentioned in paragraph (a).

### **Designated individual of relevant person**

**65.**—(1) A relevant person must designate one or more individuals to be responsible for ensuring that the relevant person complies with this Part and Part 5.

(2) An individual designated under subsection (1) may delegate to another individual the responsibility conferred by that designation.

(3) The designation of an individual by a relevant person under subsection (1) does not relieve the relevant person of any of the relevant person’s obligations under this Part or Part 5.

### *Division 2 — Data security requirements*

### **Data security and handling of health information and relevant information**

**66.**—(1) A relevant person must —

- (a) implement reasonable controls to ensure the secure processing of health information or relevant information, as the case may be;
- (b) implement reasonable safeguards to protect against the unauthorised access, collection, use, disclosure, copying, modification, disposal, destruction or loss of health information or relevant information, as the case may be; and
- (c) ensure that every personnel who accesses or handles health information or relevant information (as the case may be) is aware of his or her role and responsibility in ensuring that —
  - (i) the confidentiality and integrity of the information is protected; and

- (ii) the information is available for use by the relevant person (including individuals employed or engaged by the relevant person who are authorised to access or handle the information) in the ordinary course of the relevant person's activities. 5

(2) For the purposes of subsection (1)(a), the controls to ensure the secure processing of health information or relevant information include controls or requirements relating to the classification of the information, having regard to —

- (a) the nature of the information; and 10
- (b) the likely consequences that follow from the disclosure of the information.

(3) A relevant person must, in relation to any health information or relevant information that is in the form of or part of an extract or a compilation of de-identified or aggregated information, additionally ensure that — 15

- (a) the confidentiality and integrity of the extract or compilation is maintained at all times; and
- (b) the extract or compilation is available for use in the ordinary course of the relevant person's activities. 20

(4) If health information is processed by a relevant HDI (A) of a contributor or user (B) —

- (a) A must —
  - (i) implement reasonable controls to ensure the secure processing of health information; 25
  - (ii) implement reasonable safeguards to protect against the unauthorised access, collection, use, disclosure, copying, modification, disposal, destruction or loss of health information; and
  - (iii) ensure that every personnel who accesses or handles health information is aware of his or her role and responsibility in ensuring that — 30

(A) the confidentiality and integrity of the health information is protected; and

(B) the health information is available for use by *B* (including individuals employed or engaged by *B* who are authorised to access or handle the health information) in the ordinary course of *B*'s activities; and

(b) *B* must ensure that *A* complies with all the requirements under paragraph (a).

(5) A relevant person or a relevant HDI of a contributor or user must comply with any requirements that may be prescribed in relation to —

(a) the processing of health information or relevant information (as the case may be), including the controls mentioned in subsection (1)(a) or (4)(a)(i) that must be implemented, if any; and

(b) the protection of health information or relevant information (as the case may be) against unauthorised access, collection, use, disclosure, copying, modification, disposal, destruction or loss.

(6) A person who contravenes subsection (1), (3), (4) or (5) shall be guilty of an offence and shall be liable on conviction —

(a) in the case of an individual, to a fine not exceeding \$200,000 or to imprisonment for a term not exceeding 2 years or to both; or

(b) in any other case, to a fine not exceeding \$1 million.

## **Retention, disposal and destruction of health information and relevant information**

**67.—**(1) A relevant person must —

(a) cease to retain any health information or relevant information, or remove the means by which health information or relevant information can be associated

with any particular individual, as soon as it is reasonable to assume that —

(i) the purpose for which the information was collected is no longer being served by retention of the information; and

(ii) retention is no longer necessary for legal or business purposes; and

(b) take reasonable care, in relation to the disposal or destruction of any health information or relevant information, to prevent unauthorised access, disclosure or reproduction of the information.

(2) A relevant HDI of a contributor or user must —

(a) cease to retain any health information collected or processed on behalf of and for the purposes of the contributor or user (as the case may be), or remove the means by which the health information can be associated with any particular individual, as soon as it is reasonable to assume that —

(i) the purpose for which the health information was collected or processed is no longer being served by retention of the health information; and

(ii) retention is no longer necessary for legal or business purposes; and

(b) take reasonable care, in relation to the disposal or destruction of any health information, to prevent unauthorised access, disclosure or reproduction of the health information.

(3) A person who contravenes subsection (1) or (2) shall be guilty of an offence and shall be liable on conviction —

(a) in the case of an individual, to a fine not exceeding \$200,000 or to imprisonment for a term not exceeding 2 years or to both; or

(b) in any other case, to a fine not exceeding \$1 million.

### *Division 3 — Cybersecurity requirements*

#### **Cybersecurity of relevant computer or computer system**

5 **68.**—(1) A relevant person must implement reasonable safeguards, in relation to any relevant computer or computer system used by the relevant person to process health information or relevant information —

(a) to protect the confidentiality and integrity of the information;

10 (b) to ensure the availability of the information for use in the ordinary course of the relevant person’s activities; and

(c) to protect the relevant computer or computer system against unauthorised access, interference or tampering.

(2) If health information is processed by a relevant HDI of a contributor or user —

15 (a) the relevant HDI must implement reasonable safeguards —

(i) to protect the confidentiality and integrity of the health information processed by the relevant HDI;

20 (ii) to ensure the availability of the health information for use in the ordinary course of the activities of the contributor or user, as the case may be; and

(iii) to protect any relevant computer or computer system used by the relevant HDI to process the health information against unauthorised access, interference and tampering; and

25 (b) the contributor or user (as the case may be) must ensure that the relevant HDI implements the safeguards mentioned in paragraph (a).

30 (3) For the purposes of subsection (1), a relevant person must comply with any requirements that may be prescribed in respect of the safeguards mentioned in that subsection.

(4) For the purposes of subsection (2)(a), a relevant HDI of a contributor or user must comply with any requirements that may be prescribed in respect of the safeguards mentioned in that provision.

(5) A person who contravenes subsection (1), (2), (3) or (4) shall be guilty of an offence and shall be liable on conviction —

(a) in the case of an individual, to a fine not exceeding \$200,000 or to imprisonment for a term not exceeding 2 years or to both; or

(b) in any other case, to a fine not exceeding \$1 million.

5

#### *Division 4 — Miscellaneous*

### **Policies and practices for ensuring data security and cybersecurity**

**69.**—(1) A relevant person must establish and implement appropriate policies and practices in respect of the matters mentioned in sections 66(1), (3) and (4)(b), 67(1) and 68(1) and (2)(b).

10

(2) Without limiting subsection (1), a relevant person must ensure that the policies and practices mentioned in that subsection provide for any matter prescribed relating to those policies and practices.

15

(3) For the purposes of subsection (2), the Minister may prescribe different matters relating to the policies and practices mentioned in subsection (1) in relation to different relevant persons or classes of relevant persons.

20

(4) A relevant person must implement processes to ensure that every personnel of the relevant person adhere to the policies and practices mentioned in subsection (1).

(5) Additionally, a contributor or user must implement processes to ensure that any relevant HDI of the contributor or user and every personnel of that relevant HDI adhere to the policies and practices mentioned in subsection (1).

25

(6) A relevant person must, at the prescribed frequency, review and evaluate the policies and practices mentioned in subsection (1) to ensure that the policies and practices are effective.

30

(7) For the purposes of subsection (6), different frequencies may be prescribed for different relevant persons or classes of relevant persons.

(8) A person who contravenes subsection (1), (4), (5) or (6) shall be guilty of an offence and shall be liable on conviction —

(a) in the case of an individual, to a fine not exceeding \$200,000 or to imprisonment for a term not exceeding 2 years or to both; or

(b) in any other case, to a fine not exceeding \$1 million.

(9) In this section, “personnel” —

(a) in relation to a relevant person, means an individual who —

(i) is employed or engaged by the relevant person; or

(ii) provides, as a volunteer, any service to the relevant person or to any other person acting on behalf of the relevant person; or

(b) in relation to a relevant HDI of a contributor or user, means an individual who is employed or engaged by the relevant HDI.

### **Incident management framework**

**70.—**(1) A relevant person must establish and implement an incident management framework that provides for —

(a) mechanisms and processes to detect and respond to any cybersecurity incident or data breach; and

(b) processes to identify and resolve the cause or causes of any cybersecurity incident or data breach, and prevent the recurrence of the cybersecurity incident or data breach or the occurrence of a similar cybersecurity incident or data breach.

(2) Without limiting subsection (1), a relevant person must ensure that the incident management framework mentioned in that subsection provides for any prescribed matter relating to the mechanisms and processes mentioned in subsection (1)(a) or the processes in subsection (1)(b).

(3) For the purposes of subsection (2), the Minister may prescribe different matters relating to the mechanisms and processes mentioned in subsection (1)(a) or the processes in subsection (1)(b) for different relevant persons.

(4) A person who contravenes subsection (1) or (2) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$100,000 or to imprisonment for a term not exceeding 12 months or to both.

### **Directions relating to relevant persons**

**71.—**(1) If the Minister has reason to believe that a relevant person has contravened section 65(1), 66(1), (3) or (4)(b), 67(1), 68(1) or (2)(b), 69(1), (4), (5) or (6) or 70(1) or any requirement mentioned in section 66(5), the Minister may, by written notice, require the relevant person to take any action specified in the notice which the Minister reasonably considers to be necessary to bring the contravention to an end and prevent the recurrence of the contravention.

(2) If the Minister has reason to believe that a relevant HDI of a contributor or user has contravened section 66(4)(a), 67(2) or 68(2)(a) or any requirement mentioned in section 66(5) in relation to the processing of health information on behalf of and for the purposes of the contributor or user (as the case may be), the Minister may, by written notice, require the relevant HDI or the contributor or user (as the case may be) to take any action specified in the notice which the Minister reasonably considers to be necessary to bring the contravention to an end and prevent the recurrence of the contravention.

(3) A person who, without reasonable excuse, refuses or fails to comply with a direction under subsection (1) or (2) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$50,000 or to imprisonment for a term not exceeding 12 months or to both and, in the case of a continuing offence, to a further fine not exceeding \$1,000 for every day or part of a day during which the offence continues after conviction.

## PART 5

NOTIFICATION OF CYBERSECURITY INCIDENTS  
AND DATA BREACHES*Division 1 — General*5 **Interpretation of this Part**

72. In this Part —

“cybersecurity incident” has the meaning given by section 61(1);

“data breach” has the meaning given by section 62;

10 “notifiable data breach” has the meaning given by section 77(1);

“relevant computer or computer system” has the meaning given by section 63(1);

“relevant person” means a person mentioned in section 64(1).

**Application of this Part**

15 73. This Part applies to —

(a) in relation to any cybersecurity incident or data breach that affects —

(i) the national electronic records system; or

20 (ii) any relevant computer or computer system used by the relevant person to process health information or relevant information; and

(b) in relation to any data breach that affects health information or relevant information in the possession or under the control of the relevant person.

25 *Division 2 — Notification of cybersecurity incidents*

**Duty to conduct assessment of cybersecurity incident**

30 74.—(1) Where a relevant person has reason to believe that a cybersecurity incident in respect of the national electronic records system or any relevant computer or computer system used by the relevant person to process health information or relevant information

has occurred, the relevant person must conduct, in a reasonable and expeditious manner, an assessment of whether the cybersecurity incident is a notifiable cybersecurity incident.

(2) Where a relevant HDI of a contributor or user has reason to believe that a cybersecurity incident has occurred in respect of any relevant computer or computer system used by the relevant HDI to process health information on behalf of and for the purposes of the contributor or user (as the case may be) under this Act —

(a) the relevant HDI must, without undue delay, notify the contributor or user, as the case may be; and

(b) the contributor or user (as the case may be) must, upon notification by the relevant HDI, conduct an assessment of whether the cybersecurity incident is a notifiable cybersecurity incident.

(3) The relevant person must carry out the assessment mentioned in subsection (1) or (2)(b) in accordance with the prescribed requirements (if any).

### **Duty to notify occurrence of notifiable cybersecurity incident**

**75.**—(1) Where a relevant person assesses, in accordance with section 74, that a cybersecurity incident is a notifiable cybersecurity incident, the relevant person must notify the Minister as soon as is practicable, but in any case no later than the expiry of the period prescribed after the day the relevant person makes that assessment.

(2) For the purposes of subsection (1), different periods may be prescribed for different notifiable cybersecurity incidents.

(3) The notification under subsection (1) must contain, to the best of the knowledge and belief of the relevant person at the time the relevant person notifies the Minister, all the information that is prescribed for this purpose.

(4) The notification under subsection (1) must be made in the form and submitted in the manner required by the Minister.

(5) A relevant person is not, by reason only of notifying the Minister under subsection (1), to be regarded as being in breach of —

(a) any duty or obligation under any written law, rule of law or contract as to secrecy or other restriction on the disclosure of information; or

(b) any rule of professional conduct or ethics applicable to the relevant person.

(6) Subsection (1) applies concurrently with any obligation of the relevant person —

(a) under this Part to notify the Minister of the occurrence of a notifiable data breach arising from or relating to a cybersecurity incident; or

(b) under any other written law to notify any other person (including the Government or any public authority) of the occurrence of a cybersecurity incident, or to provide any information relating to a cybersecurity incident.

### *Division 3 — Notification of data breaches*

#### **Interpretation of this Division**

**76.** In this Division, “affected individual”, in relation to a data breach, means any individual to whom any health information or relevant information affected by the data breach relates.

#### **Notifiable data breaches**

**77.—(1)** Subject to subsection (4), a data breach in relation to health information or relevant information is a notifiable data breach under this Division if the data breach —

(a) results in, or is likely to result in, significant harm to an affected individual; or

(b) is, or is likely to be, of a significant scale.

(2) Without limiting subsection (1)(a), a data breach is deemed to result in significant harm to an individual —

(a) if the data breach is in relation to prescribed health information or relevant information or a prescribed class of health information or relevant information relating to the individual; or

(b) in other prescribed circumstances.

(3) Without limiting subsection (1)(b), a data breach is deemed to be of a significant scale —

(a) if the data breach affects not fewer than the prescribed number of affected individuals; or

(b) in other prescribed circumstances.

(4) Despite subsections (1), (2) and (3), a data breach is not a notifiable data breach if it is of a type or description that is prescribed as such for the purposes of this subsection.

### **Duty to conduct assessment of data breach**

**78.**—(1) Where a relevant person has reason to believe that a data breach affecting health information or relevant information in the possession or under the control of the relevant person has occurred, the relevant person must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a notifiable data breach.

(2) Where a relevant HDI of a contributor or user (other than a relevant HDI mentioned in section 81) has reason to believe that a data breach has occurred in relation to health information that the relevant HDI is processing on behalf of and for the purposes of the contributor or user, as the case may be —

(a) the relevant HDI must, without undue delay, notify the contributor or user (as the case may be) of the occurrence of the data breach; and

(b) the contributor or user (as the case may be) must, upon notification by the relevant HDI, conduct an assessment of whether the data breach is a notifiable data breach.

(3) The relevant person must carry out the assessment mentioned in subsection (1) or (2)(b) in accordance with any prescribed requirements.

## Duty to notify occurrence of notifiable data breach

79.—(1) Where a relevant person assesses, in accordance with section 78, that a data breach is a notifiable data breach, the relevant person must notify the Minister as soon as is practicable, but in any case no later than the expiry of the prescribed period after the day the relevant person makes that assessment.

(2) The notification under subsection (1) must contain, to the best of the knowledge and belief of the relevant person at the time the relevant person notifies the Minister, all the information that is prescribed for this purpose.

(3) The notification under subsection (1) must be made in the form and submitted in the manner required by the Minister.

(4) A relevant person is not, by reason only of notifying the Minister under subsection (1), to be regarded as being in breach of —

(a) any duty or obligation under any written law, rule of law or contract as to secrecy or other restriction on the disclosure of information; or

(b) any rule of professional conduct or ethics applicable to the relevant person.

(5) Subsection (1) applies concurrently with any obligation of the relevant person —

(a) under this Part to notify the Minister of the occurrence of a notifiable cybersecurity incident arising from or relating to a data breach; or

(b) under any other written law to notify any other person (including the Government or any public authority) of the occurrence of a data breach, or to provide any information relating to a data breach.

## **Duty to notify affected individuals of occurrence of notifiable data breach**

**80.**—(1) Subject to subsections (3), (4) and (5), a relevant person must, on or after notifying the Minister under section 79(1), notify each affected individual affected by a notifiable data breach mentioned in section 77(1)(a) in any manner that is reasonable in the circumstances. 5

(2) The notification under subsection (1) must contain, to the best of the knowledge and belief of the relevant person at the time the relevant person notifies the affected individual, all the information that is prescribed for this purpose. 10

(3) Subsection (1) does not apply to a System Operator in respect of a notifiable data breach mentioned in section 77(1)(a) that has occurred in relation to health information processed by or in the national electronic records system. 15

(4) Subsection (1) does not apply if the relevant person —

(a) upon or after assessing that a data breach is a notifiable data breach mentioned in section 77(1)(a), takes any action, in accordance with the prescribed requirements (if any), that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual; or 20

(b) had implemented, prior to the occurrence of the notifiable data breach mentioned in section 77(1)(a), any technological measure that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual. 25

(5) A relevant person must not notify any affected individual in accordance with subsection (1) if —

(a) a prescribed law enforcement agency so instructs; or

(b) the Minister so directs. 30

(6) The Minister may, on the written application of a relevant person, waive the requirement to notify an affected individual under subsection (1) subject to any conditions that the Minister thinks fit.

(7) A relevant person is not, by reason only of notifying an affected individual under subsection (1), to be regarded as being in breach of —

- (a) any duty or obligation under any written law, rule of law or contract as to secrecy or other restriction on the disclosure of information; or
- (b) any rule of professional conduct or ethics applicable to the relevant person.

### **Obligations of relevant HDI of public agency**

**81.** Where a relevant HDI —

- (a) processes health information on behalf of and for the purposes of a contributor or user that is a public agency; and
- (b) has reason to believe that a data breach has occurred in relation to that health information,

the relevant HDI must, without undue delay, notify the public agency of the occurrence of the data breach.

### *Division 4 — Miscellaneous*

#### **Offences under this Part**

**82.—**(1) A person who contravenes section 74(1) or (2)(a) or (b), 75(1) or (3), 78(1) or (2)(a) or (b), 79(1) or (2), 80(1) or (2) or 81 shall be guilty of an offence and shall be liable on conviction —

- (a) in the case of an individual, to a fine not exceeding \$200,000 or to imprisonment for a term not exceeding 2 years or to both; or
- (b) in any other case, to a fine not exceeding \$1 million.

(2) A person who contravenes section 75(4) or 79(3) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$20,000 or to imprisonment for a term not exceeding 12 months or to both.

## PART 6

RESPONSES TO THREATS AND INCIDENTS  
AFFECTING HEALTH INFORMATION AND  
RELEVANT INFORMATION

**Application of this Part**

5

**83.**—(1) This Part applies to the following persons:

- (a) a contributor;
- (b) a user;
- (c) a System Operator;
- (d) a discloser as defined in section 45;
- (e) a recipient as defined in section 45.

10

(2) To avoid doubt, this Part does not affect the operation of the Cybersecurity Act 2018 in relation to a cybersecurity incident or cybersecurity threat as defined in section 2(1) of that Act.

**Emergency measures and requirements**

15

**84.**—(1) Subsection (2) applies only if all of the following are satisfied:

- (a) an event (called in this section a critical event) has occurred or is likely to occur that involves or results in or is likely to involve or result in —
  - (i) the unauthorised disclosure, modification, transmission, conveyance or destruction of health information or relevant information in the possession or under the control of a person mentioned in section 83(1); or
  - (ii) the inability to access health information or relevant information in the possession or under the control of a person mentioned in section 83(1) in a timely manner or at all;
- (b) the occurrence or likely occurrence of a critical event, in the Minister’s opinion —

20

25

30

- (i) causes or is likely to cause serious and irreversible harm to the health, safety or welfare of a substantial number of individuals in Singapore;
- (ii) represents or is likely to represent a serious and imminent threat to public health; or
- (iii) causes or is likely to cause serious disruption to the safe, secure and efficient provision of any healthcare service or community health service in Singapore.

(2) If the Minister is satisfied that it is necessary for the purpose of preventing, detecting or countering any critical event, the Minister may, by a certificate under the Minister's hand, authorise or direct a person mentioned in section 83(1) that is specified in the certificate (called in this section the specified person) to take any measure, or comply with any requirements, as may be necessary —

(a) to prevent —

- (i) the loss of, or any damage to the accuracy, integrity or completeness of, health information or relevant information in the possession or under the control of the specified person; or
- (ii) the loss of, or any damage to, any computer, computer system, device or other equipment used by, in the possession of or under the control of the specified person that is used to process health information or relevant information; or

(b) to remedy or mitigate any loss or damage mentioned in paragraph (a) that has occurred.

(3) A measure or requirement mentioned in subsection (2) may additionally —

- (a) require or authorise the specified person to direct another person to take any measure in relation to the processing of health information or relevant information that is necessary to prevent, detect or counter the critical event; or
- (b) require the specified person to provide to the Minister any information relating to —

- (i) health information or relevant information that is or is likely to be affected by the critical event; or
- (ii) any computer, computer system, device or other equipment used by the specified person to process health information or relevant information.

5

(4) A measure or requirement mentioned in subsection (2), or a direction given by a specified person pursuant to subsection (3)(a) —

- (a) does not confer any right to the production of, or of access to, information subject to legal privilege; and
- (b) subject to paragraph (a), has effect despite any obligation or limitation imposed or any right, privilege or immunity conferred by or under any written law, rule of law, contract or rule of professional conduct or ethics, including any restriction on the disclosure of information imposed by any written law, rule of law, contract or rule of professional conduct or ethics.

10

15

(5) A specified person who, without reasonable excuse, fails to take any measure or comply with any requirement directed by the Minister under subsection (2) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$500,000 or to imprisonment for a term not exceeding 10 years or to both and, in the case of a continuing offence, to a further fine not exceeding \$5,000 for every day or part of a day during which the offence continues after conviction.

20

(6) A person who, without reasonable excuse —

25

- (a) obstructs a specified person in the taking of any measure or in complying with any requirement under subsection (2); or
- (b) fails to comply with any direction given by a specified person pursuant to subsection (3)(a),

30

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$500,000 or to imprisonment for a term not exceeding 10 years or to both and, in the case of a continuing offence, to a

further fine not exceeding \$5,000 for every day or part of a day during which the offence continues after conviction.

(7) No civil or criminal liability is incurred by —

5 (a) a specified person for doing or omitting to do any act if the specified person had done or omitted to do the act in good faith and for the purpose of or as a result of taking any measure or complying with any requirement under subsection (2); or

10 (b) a person for doing or omitting to do any act if the person had done or omitted to do the act in good faith and for the purpose of or as a result of complying with a direction given by a specified person for the purpose of taking any such measure or complying with any such requirement.

15 (8) The following persons are not considered to be in breach of any restriction upon the disclosure of information imposed by any written law, rule of law, contract or rule of professional conduct or ethics:

20 (a) a specified person who, in good faith, obtains any information for the purpose of taking any measure under subsection (2) or complying with any requirement under that subsection, or who discloses any information to the Minister in compliance with any requirement under that subsection;

25 (b) a person who, in good faith, obtains any information, or discloses any information to a specified person, in compliance with a direction given by the specified person for the purpose of taking any measure under subsection (2) or complying with any requirement under that subsection.

(9) The following persons, namely:

30 (a) a specified person to whom a person has provided information in compliance with a direction given by the specified person for the purpose of taking any measure or complying with any requirement under subsection (2);

- (b) a person to whom a specified person provides information in compliance with any requirement under subsection (2), must not use or disclose the information except —
- (c) with the written permission of the person from whom the information was obtained or, where the information is the confidential information of a third person, with the written permission of the third person; 5
  - (d) for the purpose mentioned in subsection (2)(a) or (b) in relation to which the specified person or the person mentioned in paragraph (b) (as the case may be) was provided the information; 10
  - (e) to disclose to any investigation officer, police officer or other law enforcement authority any information which discloses the commission of an offence under this Act or any other written law; or 15
  - (f) in compliance with the provisions of this Act or any other written law or an order of court.
- (10) A person who, without reasonable excuse, contravenes subsection (9) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$50,000 or to imprisonment for a term not exceeding 2 years or to both. 20
- (11) Where an offence is disclosed in the course of or pursuant to the exercise of any power under this section —
- (a) no information for that offence may be admitted in evidence in any civil or criminal proceedings; and 25
  - (b) no witness in any civil or criminal proceedings is obliged —
    - (i) to disclose the name, address or other particulars of any informer who has given information with respect to that offence; or 30
    - (ii) to answer any question if the answer would lead, or would tend to lead, to the discovery of the name, address or other particulars of the informer.

(12) If any book, document, data or computer output which is admitted in evidence or liable to inspection in any civil or criminal proceedings contains any entry in which any informer is named or described or which may lead to the informer's discovery, the court must cause those entries to be concealed from view or to be obliterated so far as may be necessary to protect the informer from discovery.

(13) In this section, "relevant information" has the meaning given by section 46(1).

### **Delegation by Minister of powers under this Part**

**85.**—(1) The Minister may delegate the exercise of his or her powers under this Part to any of the following office-holders in his or her Ministry by written notice to the person:

- (a) the Second Minister (if any) for his or her Ministry;
- (b) any Minister of State, including a Senior Minister of State, for his or her Ministry;
- (c) any Parliamentary Secretary, including a Senior Parliamentary Secretary, to his or her Ministry.

(2) A delegation by the Minister under subsection (1) may be general or for a particular case and is subject to any conditions or limitations that the Minister may specify.

## **PART 7**

### **PORTABILITY OF HEALTH INFORMATION IN ELECTRONIC FORM**

#### **Application of this Part**

**86.** This Part applies to a relevant HDI of a contributor or user in respect of health information in electronic form that the relevant HDI processes on behalf of and for the purposes of the contributor or user, as the case may be.

## Portability of health information

**87.—(1)** A relevant HDI of a contributor or user must establish and implement practices and processes in respect of the transfer, at the request of that contributor or user, of health information mentioned in section 86 to —

5

- (a) the contributor or user, as the case may be; or
- (b) another relevant HDI designated by the contributor or user, as the case may be.

(2) A relevant HDI of a contributor or user must, where the contributor or user requests that the relevant HDI transfer health information mentioned in section 86 to a person mentioned in subsection (1)(a) or (b), ensure that the health information is transferred in accordance with the relevant HDI's practices and processes mentioned in subsection (1).

10

(3) The relevant HDI must ensure that the practices and processes mentioned in subsection (1) contain measures or steps to ensure that —

15

- (a) the health information that is transferred is accurate and complete; and
- (b) the health information is transferred in a timely manner.

20

(4) Without limiting subsection (1), the practices and processes mentioned in that subsection include practices and processes relating to —

- (a) the selection, preparation, extraction and transformation of health information for the purposes of transfer; and
- (b) the identification and use of an appropriate format in which the health information is or is to be transferred.

25

(5) In addition to subsections (1), (2) and (3), a relevant HDI must comply with any requirements relating to the transfer of health information that may be prescribed.

30

(6) For the purposes of subsection (5), the Minister may prescribe different requirements for different relevant HDIs or classes of relevant HDIs.

(7) For the purposes of this section and section 88, the transfer of health information includes the preparation of copies of the health information and the provision of such copies to another person.

### **Directions under this Part**

5     **88.**—(1) The Minister may, by written notice, direct a relevant HDI of a contributor or user to take any one or more actions specified in subsection (2) if the Minister has reason to believe that the relevant HDI has contravened —

(a) section 87(1), (2) or (3);

10     (b) any requirement mentioned in section 87(5); or

(c) any provision of any code of practice issued or approved under section 90 in relation to the portability of health information under this Part.

(2) The actions mentioned in subsection (1) are the following:

15     (a) review the practices and processes of the relevant HDI mentioned in section 87(1);

(b) review whether any transfer of health information by the relevant HDI is in accordance with the practices and processes of the relevant HDI mentioned in section 87(1) and the provisions of this Part;

20     (c) identify any error, failure, inadequacy or shortcoming relating to the practices and processes of the relevant HDI or the transfer of health information, and take reasonable steps to remedy the error, failure, inadequacy or shortcoming and prevent its recurrence;

25     (d) any other action in relation to any matter in paragraph (a), (b) or (c) that the Minister may reasonably require.

(3) A person who, without reasonable excuse, refuses or fails to comply with a direction under subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$20,000 or to imprisonment for a term not exceeding 12 months or to both and, in the case of a continuing offence, to a further fine not

exceeding \$1,000 for every day or part of a day during which the offence continues after conviction.

## PART 8

### ADMINISTRATION AND ENFORCEMENT

#### Administration of Act

5

**89.—**(1) The Minister may —

- (a) appoint a public officer, an officer of a public authority, or any other individual who is suitably qualified, to be an authorised officer to exercise the powers conferred on authorised officers under this Part and Division 6 of Part 2; and 10
- (b) appoint a public officer or an officer of a public authority to be an investigation officer to exercise the powers conferred on investigation officers under this Part.

(2) Subject to subsection (3), the Minister may delegate the exercise of all or any of the powers conferred or duties imposed on the Minister under this Act to a public officer or an officer of a public authority; and any reference in the provision of this Act to the Minister includes a reference to that officer. 15

(3) Subsection (2) does not apply to the following powers and duties: 20

- (a) the power of appointment under subsection (1);
- (b) the power of delegation under subsection (2);
- (c) the Minister's powers and duties under section 36;
- (d) the Minister's powers under section 84; 25
- (e) the Minister's power to make subsidiary legislation.

(4) Any delegation under subsection (2) may be general or specific, and may be subject to any conditions or limitations that the Minister may specify.

(5) Every authorised officer or investigation officer in subsection (1) who is not otherwise a public servant under 30

section 21 of the Penal Code 1871, is taken to be one for the purposes of that Act.

## Codes of practice

**90.**—(1) The Minister may —

- 5           (a) issue one or more codes of practice;
- (b) approve as a code of practice any document prepared by a person other than the Minister if the Minister considers the document suitable for this purpose; or
- (c) amend or revoke any code of practice issued under
- 10           paragraph (a) or approved under paragraph (b),

with respect to all or any of the matters mentioned in subsection (2).

(2) The matters for the purposes of subsection (1) are the following:

- (a) the conduct of contributors, users, disclosers, recipients, relevant HDIs of contributors and users and health data intermediaries of disclosers and recipients;
- 15           (b) the measures to ensure the confidentiality, integrity and availability of health information and relevant information;
- (c) the portability of health information in electronic form that is processed by a relevant HDI of a contributor or user.

20       (3) If any provision in any code of practice is inconsistent with any provision of this Act, that provision, to the extent of the inconsistency —

- (a) is to have effect subject to this Act; or
- (b) having regard to this Act, is not to have effect.

25       (4) Where a code of practice is issued, approved, amended or revoked by the Minister under subsection (1), the Minister must —

- (a) publish a notice of the issue, approval, amendment or revocation (as the case may be) of the code of practice in a manner that will secure adequate publicity for the issue, approval, amendment or revocation;
- 30

- (b) specify in the notice the date of the issue, approval, amendment or revocation, as the case may be; and
- (c) ensure that, so long as the code of practice remains in force, copies of that code of practice, and of all amendments to it, are made available free of charge to the persons to whom the code of practice applies.

5

(5) No issued or approved code of practice, no amendment to any code of practice, and no revocation of any code of practice, has any force or effect until the notice mentioned in subsection (4) is published in accordance with that subsection.

10

(6) A code of practice issued or approved under this section does not have legislative effect.

(7) Subject to subsection (8), a person must comply with any code of practice that is applicable to that person.

(8) The Minister may, either generally or for any period that the Minister may specify, waive the application of any code of practice, or any part of a code of practice, issued or approved under this section to any person.

15

(9) A contravention or failure by a person to comply with a code of practice that applies to the person —

20

- (a) does not of itself render the person liable to criminal proceedings; but
- (b) in any proceedings (criminal or otherwise) may be relied on by any party to those proceedings as tending to establish or negate any liability which is in question in those proceedings.

25

### **Power to obtain documents and information — authorised officers**

**91.—**(1) An authorised officer may, by written notice, require any person to provide, within a reasonable period or at the time or frequency, and in the form or manner, specified in the notice, any document or information —

30

(a) that the authorised officer considers necessary to determine —

(i) the person's compliance with this Act, or any direction, notice or order issued under this Act;

5 (ii) whether the person's practices and procedures are in compliance with an applicable code of practice; or

(iii) whether information provided to the Minister or any authorised officer under a provision of this Act is correct; and

10 (b) that is —

(i) within the knowledge of that person; or

(ii) in the custody or under the control of that person.

(2) An authorised officer is entitled without payment to keep any document or information, or any copy or extract of any document or information, provided to the authorised officer under subsection (1).

### **Power to obtain documents and information — investigation officers**

92.—(1) An investigation officer may, by written notice, require any person to provide, within a reasonable period or at the time or frequency, and in the form or manner, specified in the notice, any document or information —

(a) that the investigation officer considers necessary —

25 (i) to determine the person's compliance with this Act, including whether an offence under this Act has been committed;

(ii) to determine the person's compliance with any direction, notice or order issued under this Act;

30 (iii) to determine whether information provided to the Minister or an authorised officer under a provision of this Act is correct; or

- (iv) to determine whether the person's practices and procedures are in compliance with an applicable code of practice; and
- (b) that is —
- (i) within the knowledge of that person; or 5
  - (ii) in the custody or under the control of that person.
- (2) The power under subsection (1) to require a person to provide any document or information includes the power —
- (a) to require that person, or any individual who is or was an officer or employee of the person, to provide an explanation of the document or information; 10
  - (b) if the document or information is not provided, to require that person to state, to the best of the knowledge and belief of that person, where it is;
  - (c) if the document or information is recorded otherwise than in legible form, to require the document or information to be made available to the authorised officer in legible form; and 15
  - (d) if the document or information is stored in a computer or other electronic device, and the person or individual is reasonably suspected to have knowledge of or access to any username, password or other authentication information required to gain access to the document or information, to require the person or individual to provide assistance (including but not limited to providing any username, password or other authentication information) to gain access to the computer or electronic device and the document or information in the computer or electronic device. 20 25
- (3) An investigation officer is entitled without payment to keep any document or information, or any copy or extract of any document or information, provided to the investigation officer under subsection (1). 30

## **Powers of entry and inspection — authorised officers**

**93.**—(1) An authorised officer may, during normal business hours, enter and inspect any premises or conveyance which the authorised officer reasonably believes to be —

- 5           (a) owned or occupied by a person; or
- (b) where any activity is being or has been conducted or carried on by a person,

for the purpose of —

- 10           (c) determining the person’s compliance with this Act, or any direction, notice or order issued under this Act; or
- (d) assessing whether the practices of the person are in compliance with an applicable code of practice.

(2) For the purposes of subsection (1), the authorised officer may do all or any of the following:

- 15           (a) inspect or examine any thing or observe any activity conducted in or on the premises or conveyance;
- (b) make a still or moving image or recording of the premises or conveyance and any thing in or on the premises or conveyance;
- 20           (c) inspect and make copies of or take extracts from, or require the occupier or any person having the management or control of the premises or conveyance to provide copies of or extracts from, any book, document, record or electronic material;
- 25           (d) inspect and make copies of or take extracts from, or require the occupier or any person having the management or control of the premises or conveyance to provide copies of or extracts from, health information about any individual in the possession or under the control of the occupier or person, even though the prior consent of that individual has
- 30           not been obtained;
- (e) take into or onto the premises or conveyance any equipment and material that the authorised officer

requires for the purpose of exercising any power under this Act in relation to the premises or conveyance;

(f) operate electronic equipment in or on the premises or conveyance.

(3) The power under subsection (2)(f) to operate electronic equipment in or on any premises or conveyance includes the power — 5

(a) to use a disk, tape or other storage device that is in or on the premises or conveyance and can be used with the equipment or in association with the equipment; 10

(b) to operate electronic equipment in or on the premises or conveyance to put the relevant data in documentary form and remove the documents so produced from the premises or conveyance; and

(c) to operate electronic equipment in or on the premises or conveyance to transfer the relevant data to a disk, tape or other storage device that — 15

(i) is brought to the premises or conveyance for the exercise of the power; or

(ii) is in or on the premises or conveyance and the use of which for that purpose has been agreed in writing by the occupier of the premises or conveyance, 20

and to remove the disk, tape or other storage device from those premises or that conveyance.

(4) Any individual who is present at any premises or conveyance mentioned in subsection (1) must render all assistance and cooperation to an authorised officer as are necessary for an entry or inspection or otherwise for the exercise of his or her powers under this Act in relation to those premises or that conveyance. 25

### **Powers of entry, inspection and search, etc. — investigation officers** 30

**94.—(1)** An investigation officer may, at any time and without notice and without warrant, enter, inspect and search any premises or

conveyance which the investigation officer reasonably believes to be —

- (a) owned or occupied by a person; or
- (b) where any activity is being or has been conducted or carried on by a person,

for the purpose of —

- (c) investigating an offence under this Act or a contravention of or non-compliance with a provision of this Act; or
- (d) assessing whether the practices of a person are in compliance with this Act or an applicable code of practice.

(2) For the purposes of subsection (1), the investigation officer may do all or any of the following:

- (a) inspect or examine any thing or observe any activity conducted in or on the premises or conveyance;
- (b) make a still or moving image or recording of the premises or conveyance and any thing in or on the premises or conveyance;
- (c) inspect and make copies of or take extracts from, or require the occupier or any person having the management or control of the premises or conveyance to provide copies of or extracts from, any book, document, record or electronic material;
- (d) inspect and make copies of or take extracts from, or require the occupier or any person having the management or control of the premises or conveyance to provide copies of or extracts from, health information about any individual in the possession or under the control of the occupier or person, even though the prior consent of that individual has not been obtained;
- (e) take into or onto the premises or conveyance any equipment and material that the investigation officer requires for the purpose of exercising any power under this Act in relation to the premises or conveyance;

- (f) operate electronic equipment in or on the premises or conveyance;
  - (g) seize any document or thing if all of the following are satisfied:
    - (i) the investigation officer has reasonable grounds to believe that the document or thing is —
      - (A) evidential material relevant to, or is intended to be used for the purpose of committing, an offence under this Act or a contravention of or non-compliance with a provision of this Act; or
      - (B) evidential material relevant to assessing a person’s compliance with this Act or an applicable code of practice;
    - (ii) it is necessary to seize the document or thing in order to prevent it from being concealed, lost or destroyed.
- (3) The power under subsection (2)(f) to operate electronic equipment in or on any premises or conveyance includes the power —
- (a) to use a disk, tape or other storage device that is in or on the premises or conveyance and can be used with the equipment or in association with the equipment;
  - (b) to operate electronic equipment in or on the premises or conveyance to put the relevant data in documentary form and remove the documents so produced from the premises or conveyance; and
  - (c) to operate electronic equipment in or on the premises or conveyance to transfer the relevant data to a disk, tape or other storage device that —
    - (i) is brought to the premises or conveyance for the exercise of the power; or

(ii) is in or on the premises or conveyance and the use of which for that purpose has been agreed in writing by the occupier of the premises or conveyance,

and to remove the disk, tape or other storage device from those premises or that conveyance.

(4) Any individual who is present at any premises or conveyance mentioned in subsection (1) must render all assistance and cooperation to an investigation officer as are necessary for an entry, inspection or investigation or otherwise for the exercise of his or her powers under this Act in relation to those premises or that conveyance.

(5) An investigation officer may for a purpose in subsection (1)(c) or (d) —

(a) require any person —

(i) to provide any information within the person's knowledge; or

(ii) to produce any book, document, record, electronic material, article or thing within the person's possession for inspection by the investigation officer and for him or her to make copies of the book, document or other record, or to provide the investigation officer with copies of the book, document or other record;

(b) orally examine any person who appears to be acquainted with the facts and circumstances of any contravention or suspected contravention of a provision under this Act, and must —

(i) reduce to writing any statement made by the person so examined;

(ii) read the statement over to the person so examined;

(iii) if the person does not understand English, interpret, or cause to be interpreted, the statement in a language that the person understands; and

- (iv) require the person so examined to sign the statement, after correction, if necessary; and
- (c) require, by written order, the attendance before the investigation officer of any person, being within the limits of Singapore, who, from information given or otherwise, appears to be acquainted with the facts and circumstances of any matter under this Act, and that person must attend as so required.

(6) A person examined under this section must state truly the facts and circumstances with which the person is acquainted, except only that the person need not say anything that might expose the person to a criminal charge, penalty or forfeiture.

### **Offence of obstructing, etc., authorised officer or investigation officer in exercise of powers, etc.**

95.—(1) A person who —

- (a) refuses to give access to, or obstructs, hinders, impedes or delays, an authorised officer or investigation officer in the exercise of any power under this Part;
- (b) without reasonable excuse, does not comply with a requirement under section 91(1), 92(1), 93(2)(c) or (d) or 94(2)(c) or (d) or (5)(a), or with section 93(4) or 94(4); or
- (c) refuses to be examined under section 94(5)(b) or does not attend before an investigation officer as required under section 94(5)(c),

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$20,000 or to imprisonment for a term not exceeding 12 months or to both.

(2) For the purposes of subsection (1)(b), it is a reasonable excuse for a person to refuse or fail to provide any information, produce any book, document, record, electronic material, article or thing or answer any question if doing so might tend to incriminate that person.

## False or misleading statements, documents or information

96. A person who, in relation to any matter under this Act —

- (a) makes any statement, or provides any document or information, that is false or misleading in a material particular; and
- (b) knows or ought reasonably to know that, or is reckless as to whether, the statement, document or information is false or misleading in a material particular,

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$20,000 or to imprisonment for a term not exceeding 12 months or to both.

## Disposal of things and documents

97.—(1) Any thing or document produced, detained or seized under this Act must —

- (a) where the thing or document is produced in any criminal trial, be dealt with in accordance with section 364(1) of the Criminal Procedure Code 2010; or
- (b) in any other case, be returned to the owner or reported to a Magistrate's Court.

(2) Where the report of any thing or document is made to a Magistrate's Court under subsection (1)(b), the Magistrate's Court may order the thing or document —

- (a) to be forfeited; or
- (b) to be disposed of in any manner that the Magistrate's Court thinks fit.

(3) This section does not affect any right to retain or dispose of property which may exist in law apart from this section.

## PART 9

## MISCELLANEOUS

**Legal protections — contributors**

**98.**—(1) This section applies to a contributor, or an authorised individual of a contributor, in relation to the contribution of health information about any individual under this Act by the contributor if, and only if, the health information is contributed — 5

(a) in good faith and with reasonable care; and

(b) in accordance with this Act.

(2) No liability shall lie against the contributor or the authorised individual of a contributor for anything done in relation to the contribution of the health information about the individual. 10

(3) Subject to subsection (4), the contribution of the health information by the contributor is not a breach of —

(a) any obligation of confidentiality; or 15

(b) any prohibition or restriction in respect of the disclosure or use of the health information,

that is imposed under any written law, rule of law, contract or rule of professional conduct or ethics.

(4) Subsection (3) does not apply in relation to any obligation of confidentiality, or any prohibition or restriction in respect of the disclosure or use of the health information, that is imposed under any prescribed written law. 20

(5) The contribution of the health information by the contributor is not an act of infringement of any copyright in the health information that is held by any person. 25

(6) In this section, “authorised individual” of a contributor means an individual who —

(a) is any of the following:

(i) an individual who is employed or engaged by the contributor; 30

(ii) an individual who provides, as a volunteer, any service to the contributor; and

(b) is authorised by the contributor to do any thing to enable or facilitate the contribution of health information by the contributor in accordance with this Act.

### Legal protections — users

**99.—**(1) This section applies in relation to the access, collection or disclosure of accessible health information about any individual under this Act —

(a) by a user if, and only if, the user accesses, collects or discloses the accessible health information —

(i) in good faith and with reasonable care; and

(ii) in accordance with this Act; and

(b) by an authorised individual of a user as defined in section 18(1) or (2) (as the case may be) if, and only if, the authorised individual accesses, collects or discloses the accessible health information —

(i) in good faith and with reasonable care;

(ii) in accordance with this Act; and

(iii) in the ordinary course of the duties of the authorised individual.

(2) No liability shall lie against the user or the authorised individual of a user for anything done in relation to the access, collection or disclosure of the accessible health information.

(3) The access, collection or disclosure of the accessible health information by the user or the authorised individual of a user is not a breach of —

(a) any obligation of confidentiality; or

- (b) any prohibition or restriction in respect of the access or collection (as the case may be) of the accessible health information,

that is imposed under any written law, rule of law, contract or rule of professional conduct or ethics. 5

(4) The access, collection or disclosure of the accessible health information by the user or the authorised individual of a user is not an act of infringement of any copyright in the health information that is held by any person.

### **Legal protections — requestors** 10

**100.**—(1) This section applies in relation to the access, collection, disclosure or use of derived information within the meaning given by section 6 —

- (a) by a requestor if, and only if, the requestor accesses, collects, discloses or uses the derived information — 15

- (i) in good faith and with reasonable care; and
- (ii) in accordance with this Act; and

- (b) by an authorised individual of a requestor if, and only if, the authorised individual accesses, collects, discloses or uses the derived information — 20

- (i) in good faith and with reasonable care;
- (ii) in accordance with this Act; and
- (iii) in the ordinary course of the duties of the authorised individual.

(2) No liability shall lie against the requestor or the authorised individual of a requestor for anything done in relation to the access, collection, disclosure or use of the derived information. 25

(3) The access, collection, disclosure or use of the derived information by the requestor or the authorised individual of a requestor is not a breach of — 30

- (a) any obligation of confidentiality; or

- (b) any prohibition or restriction in respect of the access, collection, disclosure or use (as the case may be) of the derived information,

5 that is imposed under any written law, rule of law, contract or rule of professional conduct or ethics.

(4) The access, collection, disclosure or use of the derived information by the requestor or the authorised individual of a requestor is not an act of infringement of any copyright in the derived information that is held by any person.

10 (5) In this section, “authorised individual” of a requestor means an individual who is, or who belongs to a class of individuals that is, specified in the approval granted by the Minister in accordance with section 25(10)(b).

### **Legal protections — System Operator, etc.**

15 **101.**—(1) This section applies, in relation to anything done or omitted to be done —

(a) by a System Operator if, and only if, the System Operator does or omits to do so —

(i) in good faith and with reasonable care; and

20 (ii) in accordance with this Act; and

(b) by any officer, employee or contractor of a System Operator if, and only if, the officer, employee or contractor (as the case may be) does so or omits to do so —

(i) in good faith and with reasonable care;

25 (ii) in accordance with this Act; and

(iii) in the ordinary course of the duties of the officer, employee or contractor (as the case may be) for the System Operator.

30 (2) No liability shall lie against the System Operator or the officer, employee or contractor of a System Operator for anything done or omitted to be done in relation to any specified matter.

(3) No liability shall lie against the System Operator or the officer, employee or contractor of a System Operator for any of the following:

- (a) any error or inaccuracy in —
  - (i) accessible health information about any individual that is made available to any user or any authorised individual of a user; or 5
  - (ii) derived information that is provided to a requestor in relation to an application approved under section 25(2) or (3);
- (b) any loss or damage arising from any error or inaccuracy in — 10
  - (i) accessible health information about any individual that is made available to any user or any authorised individual of a user; or
  - (ii) derived information that is provided to a requestor in relation to an application approved under section 25(2) or (3); 15
- (c) any loss or damage arising from —
  - (i) any failure or delay by any contributor to contribute health information about any individual; or 20
  - (ii) the inability of, or any interruption, suspension or restriction of the ability of, any contributor to contribute health information about any individual;
- (d) any loss or damage arising from —
  - (i) any failure or delay by any user or any authorised individual of a user to access or collect accessible health information about any individual; or 25
  - (ii) the inability of, or any interruption, suspension or restriction of the ability of, any user or any authorised individual of a user to access or collect accessible health information about any individual. 30

(4) No liability shall lie against the System Operator or the officer, employee or contractor of a System Operator for any loss or damage

that arises solely from or in relation to the imposition or operation of an access restriction in relation to accessible health information about any individual, or the revocation of any such access restriction.

(5) The System Operator or the officer, employee or contractor of a System Operator who does or omits to do anything in relation to any specified matter does not commit an act of infringement of any copyright in health information concerned that is held by any person.

(6) In this section, “specified matter” means any of the following matters:

(a) the processing of health information for the purposes of Part 2, including —

(i) the collection of health information about any individual that is contributed by any contributor;

(ii) the processing of health information stored in the national electronic records system for the purpose of making available accessible health information about any individual to any user or any authorised individual of a user;

(iii) the implementation of any request to impose an access restriction in relation to accessible health information about any individual, or to revoke any such access restriction; and

(iv) the provision of derived information to a requestor in accordance with an application approved under section 25(2) or (3);

(b) the operation, administration and maintenance of the national electronic records system, including the access and use of health information stored in the national electronic records system for that purpose.

## Legal protections — disclosers

**102.—**(1) This section applies in relation to the disclosure of relevant information, pursuant to a data sharing agreement —

(a) by a discloser if, and only if, the discloser discloses the relevant information —

(i) in good faith and with reasonable care; and

(ii) in accordance with this Act; and

(b) by an authorised personnel of a discloser if, and only if, the authorised personnel discloses the relevant information —

(i) in good faith and with reasonable care;

(ii) in accordance with this Act; and

(iii) in the ordinary course of the duties of the authorised personnel.

(2) No liability shall lie against the discloser or the authorised personnel of a discloser for anything done in relation to the disclosure of the relevant information.

(3) The disclosure of the relevant information by the discloser or the authorised individual of a discloser is not a breach of —

(a) any obligation of confidentiality; or

(b) any prohibition or restriction in respect of the disclosure of the relevant information,

that is imposed under any written law, rule of law, contract or rule of professional conduct or ethics.

(4) The disclosure of the relevant information by the discloser or the authorised individual of a discloser is not an act of infringement of any copyright in the relevant information that is held by any person.

(5) In this section, “authorised personnel” of a discloser means a personnel (as defined in section 45) of the discloser who is specified in a data sharing agreement in accordance with section 52(3)(d).

### **Legal protections — recipients**

**103.**—(1) This section applies in relation to the collection or use of relevant information, pursuant to a data sharing agreement —

(a) by a recipient if, and only if, the recipient collects or uses the relevant information —

- (i) in good faith and with reasonable care; and
- (ii) in accordance with this Act; and

(b) by an authorised personnel of a recipient if, and only if, the authorised personnel collects or uses the relevant information —

- (i) in good faith and with reasonable care;
- (ii) in accordance with this Act; and
- (iii) in the ordinary course of the duties of the authorised personnel.

(2) No liability shall lie against the recipient or the authorised personnel of a recipient for anything done in relation to the collection or use of the relevant information.

(3) The collection or use of the relevant information by the recipient or the authorised individual of a recipient is not a breach of —

- (a) any obligation of confidentiality; or
- (b) any prohibition or restriction in respect of the collection or use (as the case may be) of the relevant information,

that is imposed under any written law, rule of law, contract or rule of professional conduct or ethics.

(4) The collection or use of the relevant information by the recipient or the authorised individual of a recipient is not an act of infringement of any copyright in the relevant information that is held by any person.

(5) In this section, “authorised personnel” of a recipient means a personnel (as defined in section 45) of the recipient who is specified in a data sharing agreement in accordance with section 52(3)(e).

### **Legal protections — others**

**104.** No liability shall lie personally against any authorised officer or investigation officer who, acting in good faith and with reasonable care, does or omits to do anything in the execution or purported execution of this Act.

## Offences by corporations

**105.**—(1) Where, in a proceeding for an offence under this Act, it is necessary to prove the state of mind of a corporation in relation to a particular conduct, evidence that —

(a) an officer, employee or agent of the corporation engaged in that conduct within the scope of his or her actual or apparent authority; and 5

(b) the officer, employee or agent had that state of mind, is evidence that the corporation had that state of mind.

(2) Where a corporation commits an offence under this Act, a person — 10

(a) who is —

(i) an officer of the corporation; or

(ii) an individual involved in the management of the corporation and in a position to influence the conduct of the corporation in relation to the commission of the offence; and 15

(b) who —

(i) consented or connived, or conspired with others, to effect the commission of the offence; 20

(ii) is in any other way, whether by act or omission, knowingly concerned in, or is party to, the commission of the offence by the corporation; or

(iii) knew or ought reasonably to have known that the offence by the corporation (or an offence of the same type) would be or is being committed, and failed to take all reasonable steps to prevent or stop the commission of that offence, 25

shall be guilty of that same offence as is the corporation, and shall be liable on conviction to be punished accordingly. 30

(3) A person mentioned in subsection (2) may rely on a defence that would be available to the corporation if it were charged with the

offence with which the person is charged and, in doing so, the person bears the same burden of proof that the corporation would bear.

(4) To avoid doubt, this section does not affect the application of —

(a) Chapters 5 and 5A of the Penal Code 1871; or

5 (b) the Evidence Act 1893 or any other law or practice regarding the admissibility of evidence.

(5) To avoid doubt, subsection (2) also does not affect the liability of the corporation for an offence under this Act, and applies whether or not the corporation is convicted of the offence.

10 (6) In this section —

“corporation” includes a limited liability partnership within the meaning given by section 2(1) of the Limited Liability Partnerships Act 2005;

15 “officer”, in relation to a corporation, means any director, partner, chief executive, manager, secretary or other similar officer of the corporation, and includes —

(a) any person purporting to act in any such capacity; and

20 (b) for a corporation whose affairs are managed by its members, any of those members as if the member were a director of the corporation;

“state of mind” of a person includes —

(a) the knowledge, intention, opinion, belief or purpose of the person; and

25 (b) the person’s reasons for the intention, opinion, belief or purpose.

### **Offences by unincorporated associations or partnerships**

**106.**—(1) Where, in a proceeding for an offence under this Act, it is necessary to prove the state of mind of an unincorporated association or a partnership in relation to a particular conduct, evidence that —

30 (a) an employee or agent of the unincorporated association or partnership engaged in that conduct within the scope of his or her actual or apparent authority; and

(b) the employee or agent had that state of mind,  
is evidence that the unincorporated association or partnership (as the case may be) had that state of mind.

(2) Where an unincorporated association or a partnership commits an offence under this Act, a person —

5

(a) who is —

- (i) an officer of the unincorporated association or a member of its governing body;
- (ii) a partner in the partnership; or
- (iii) an individual involved in the management of the unincorporated association or partnership and in a position to influence the conduct of the unincorporated association or partnership (as the case may be) in relation to the commission of the offence; and

10

15

(b) who —

- (i) consented or connived, or conspired with others, to effect the commission of the offence;
- (ii) is in any other way, whether by act or omission, knowingly concerned in, or is party to, the commission of the offence by the unincorporated association or partnership; or
- (iii) knew or ought reasonably to have known that the offence by the unincorporated association or partnership (or an offence of the same type) would be or is being committed, and failed to take all reasonable steps to prevent or stop the commission of that offence,

20

25

shall be guilty of the same offence as is the unincorporated association or partnership (as the case may be), and shall be liable on conviction to be punished accordingly.

30

(3) A person mentioned in subsection (2) may rely on a defence that would be available to the unincorporated association or partnership if

it were charged with the offence with which the person is charged and, in doing so, the person bears the same burden of proof that the unincorporated association or partnership would bear.

(4) To avoid doubt, this section does not affect the application of —

(a) Chapters 5 and 5A of the Penal Code 1871; or

(b) the Evidence Act 1893 or any other law or practice regarding the admissibility of evidence.

(5) To avoid doubt, subsection (2) also does not affect the liability of an unincorporated association or a partnership for an offence under this Act, and applies whether or not the unincorporated association or partnership is convicted of the offence.

(6) In this section —

“officer”, in relation to an unincorporated association (other than a partnership), means the president, the secretary or any member of the committee of the unincorporated association, and includes —

(a) any person holding a position analogous to that of president, secretary or member of a committee of the unincorporated association; and

(b) any person purporting to act in any such capacity;

“partner” includes a person purporting to act as a partner;

“state of mind” of a person includes —

(a) the knowledge, intention, opinion, belief or purpose of the person; and

(b) the person’s reasons for the intention, opinion, belief or purpose.

## Service of documents

**107.**—(1) A document that is permitted or required by or under this Act to be served on a person may be served as described in this section.

(2) A document permitted or required by or under this Act to be served on an individual may be served —

- (a) by giving it to the individual personally;
- (b) by sending it by prepaid registered post to the address specified by the individual for the service of documents generally, or specifically for the document, or (if no address is so specified) the individual's residential address or business address; 5
- (c) by leaving it at the individual's residential address with an adult apparently resident there, or at the individual's business address with an adult apparently employed there;
- (d) by affixing a copy of the document in a conspicuous place at the individual's residential address or business address; 10
- (e) by sending it by fax to the fax number last known to the person giving or serving the document as the fax number for the service of documents on the individual; or
- (f) by sending it by email to the individual's last email address. 15

(3) A document permitted or required by or under this Act to be served on a partnership (other than a limited liability partnership) may be served —

- (a) by giving it to any partner or other similar officer, or an authorised representative, of the partnership; 20
- (b) by leaving it at, or by sending it by prepaid registered post to, the partnership's business address;
- (c) by sending it by fax to the fax number used at the partnership's business address; or 25
- (d) by sending it by email to the partnership's last email address.

(4) A document permitted or required by or under this Act to be served on a body corporate (including a limited liability partnership) or an unincorporated association may be served — 30

- (a) by giving it to the secretary or other similar officer of the body corporate or unincorporated association, or the limited liability partnership's manager;

(b) by leaving it at, or by sending it by prepaid registered post to, the registered office or principal office in Singapore of the body corporate or unincorporated association;

5 (c) by sending it by fax to the fax number used at the registered office or principal office in Singapore of the body corporate or unincorporated association; or

(d) by sending it by email to the last email address of the body corporate or unincorporated association.

(5) Service of a document under this section takes effect —

10 (a) if the document is sent by prepaid registered post, 2 days after the day the document was posted (even if it is returned undelivered);

15 (b) if the document is sent by fax and a notification of successful transmission is received, on the day of transmission; or

(c) if the document is sent by email, at the time that the email becomes capable of being retrieved by the person to whom it is sent.

20 (6) However, service of any document under this Act on a person by email may be effected only with the person’s prior written consent to service in that way.

(7) This section does not apply to documents to be served in proceedings in court.

(8) In this section —

25 “authorised representative”, in relation to a partnership (other than a limited liability partnership), means any person authorised to accept service of documents on behalf of the partnership;

“business address” means —

30 (a) in the case of an individual, the individual’s usual or last known place of business in Singapore; or

(b) in the case of a partnership (other than a limited liability partnership), the partnership’s principal or last known place of business in Singapore;

“document” includes an order or a notice permitted or required by or under this Act to be served; 5

“last email address” means the last email address given by the addressee concerned to the person giving or serving the document as the email address for the service of documents under this Act;

“residential address” means an individual’s usual or last known place of residence in Singapore. 10

### **Jurisdiction of court**

**108.** Despite the Criminal Procedure Code 2010, a District Court has jurisdiction to try any offence under this Act and has power to impose the full punishment for the offence. 15

### **Composition of offences**

**109.—**(1) The Minister may compound any offence under this Act (except an offence mentioned in subsection (2)) that is prescribed as a compoundable offence by collecting from a person reasonably suspected of having committed the offence a sum not exceeding the lower of the following: 20

(a) one half of the amount of the maximum fine that is prescribed for the offence;

(b) \$10,000.

(2) The Minister may compound any offence under Part 4 or 5 (other than an offence under section 70, 71 or 82(2)) that is prescribed as a compoundable offence by collecting from a person (*X*) reasonably suspected of having committed the offence — 25

(a) where *X* is an individual, a sum not exceeding the lower of the following: 30

(i) one half of the amount of the maximum fine prescribed for the offence that may be imposed on an individual who is convicted of that offence;

(ii) \$20,000; or

5 (b) in any other case, a sum not exceeding the lower of the following:

(i) one half of the amount of the maximum fine prescribed for the offence that may be imposed on a person (other than an individual) who is convicted of that offence;

10

(ii) \$200,000.

(3) On payment of the sum of money, no further proceedings are to be taken against that person in respect of the offence.

15

(4) All sums collected under this section must be paid into the Consolidated Fund.

## Exemption

20

**110.** The Minister may, by order in the *Gazette*, exempt any person or class of persons, or any health information or type of health information, from all or any of the provisions of this Act, either generally or in a particular case and subject to any conditions that the Minister may impose.

## Amendment of Schedules

**111.**—(1) The Minister may, by order in the *Gazette*, amend, add to or vary the Schedules.

25

(2) The Minister may, in an order under subsection (1), make provisions of a saving or transitional nature consequent on the enactment of the order that the Minister may consider necessary or expedient.

## Regulations

30

**112.**—(1) The Minister may make regulations necessary or convenient to be prescribed for carrying out or giving effect to this Act.

(2) Without limiting subsection (1), the Minister may make regulations for any of the following:

- (a) the form and manner in which an application to be approved as an approved contributor or approved user may be made; 5
- (b) the form and manner in which health information about any individual is to be contributed, including any other information that is to be provided to a System Operator together with that health information;
- (c) the requirements and standards applicable to health information about any individual that is contributed in accordance with this Act; 10
- (d) the form and manner in which an application in respect of an authorised individual of a user may be made to a System Operator; 15
- (e) the form and manner in which an application to obtain derived information may be made;
- (f) any matter that is required or permitted to be prescribed under this Act.

(3) The regulations made under this section may provide that any contravention of any provision of the regulations shall be an offence punishable with a fine not exceeding \$50,000 or with imprisonment for a term not exceeding 12 months or with both and, in the case of a continuing offence, with a further fine not exceeding \$1,000 for every day or part of a day during which the offence continues after conviction. 20 25

### **Related amendment to Human Organ Transplant Act 1987**

**113.** In the Human Organ Transplant Act 1987, in section 28(2), after paragraph (b), insert —

“(ba) as required or permitted under the Health Information Act 2025;”.

 30

## Saving and transitional provision

114. For a period of 2 years after the date of commencement of any provision of this Act, the Minister may, by regulations, prescribe any additional provisions of a saving or transitional nature consequent on the enactment of that provision that the Minister may consider necessary or expedient.

## FIRST SCHEDULE

Section 12

### CONTRIBUTION OF HEALTH INFORMATION BY SPECIFIED CONTRIBUTORS

#### PART 1

#### SPECIFIED CONTRIBUTORS AND TYPES OF HEALTH INFORMATION TO BE CONTRIBUTED

<i>First column</i>	<i>Second column</i>
<i>Specified contributor or class of specified contributors</i>	<i>Types of health information</i>
<p>1. An HCSA licensee licensed to provide an acute hospital service</p>	<p>(a) Visit event</p> <p>(b) Adverse drug event history</p> <p>(c) Ordered (prescribed) medications</p> <p>(d) Dispensed medications</p> <p>(e) Medication list</p> <p>(f) Vaccines administered</p> <p>(g) Cardiac report</p> <p>(h) Surgical procedure notes</p> <p>(i) Dental notes</p> <p>(j) Visit diagnoses/reasons for visit or patient problem list</p> <p>(k) Discharge summary</p> <p>(l) Emergency Department/Urgent Care summary</p> <p>(m) Referral memorandum</p>

FIRST SCHEDULE — *continued*

<i>First column</i>	<i>Second column</i>	
<i>Specified contributor or class of specified contributors</i>	<i>Types of health information</i>	
2. An HCSA licensee licensed to provide an ambulatory surgical centre service	(a) Visit event	5
	(b) Adverse drug event history	
	(c) Ordered (prescribed) medications	
	(d) Dispensed medications	10
	(e) Medication list	
	(f) Vaccines administered	
	(g) Cardiac report	
	(h) Surgical procedure notes	
	(i) Dental notes	15
	(j) Visit diagnoses/reasons for visit or patient problem list	
3. An HCSA licensee licensed to provide an assisted reproduction service	(k) Discharge summary	
	(l) Referral memorandum	
	(a) Visit event	20
	(b) Adverse drug event history	
	(c) Ordered (prescribed) medications	
	(d) Dispensed medications	
	(e) Medication list	25
	(f) Cardiac report	
	(g) Surgical procedure notes	
	(h) Visit diagnoses/reasons for visit or patient problem list	
(i) Discharge summary	30	
(j) Referral memorandum		

FIRST SCHEDULE — *continued*

	<i>First column</i>	<i>Second column</i>
	<i>Specified contributor or class of specified contributors</i>	<i>Types of health information</i>
5	4. An HCSA licensee licensed to provide a clinical laboratory service	(a) Laboratory test reports
10	5. An HCSA licensee licensed to provide a community hospital service	(a) Visit event (b) Adverse drug event history (c) Ordered (prescribed) medications (d) Dispensed medications (e) Medication list (f) Vaccines administered (g) Cardiac report (h) Surgical procedure notes (i) Visit diagnoses/reasons for visit or patient problem list
15		(j) Discharge summary
20		(k) Referral memorandum
25	6. An HCSA licensee licensed to provide a contingency care service	(a) Visit event (b) Adverse drug event history (c) Ordered (prescribed) medications (d) Dispensed medications (e) Medication list (f) Vaccines administered (g) Cardiac report (h) Surgical procedure notes (i) Visit diagnoses/reasons for visit or patient problem list (j) Discharge summary
30		

FIRST SCHEDULE — *continued*

<i>First column</i>	<i>Second column</i>	
<i>Specified contributor or class of specified contributors</i>	<i>Types of health information</i>	
	(k) Referral memorandum	5
7. An HCSA licensee licensed to provide a nuclear medicine service	(a) Adverse drug event history	
	(b) Ordered (prescribed) medications	
	(c) Dispensed medications	
	(d) Laboratory test reports	10
	(e) Radiology/imaging reports	
	(f) Cardiac report	
	(g) Surgical procedure notes	
8. An HCSA licensee licensed to provide a nursing home service	(a) Visit event	
	(b) Adverse drug event history	15
	(c) Ordered (prescribed) medications	
	(d) Dispensed medications	
	(e) Medication list	
	(f) Vaccines administered	20
	(g) Cardiac report	
	(h) Surgical procedure notes	
9. An HCSA licensee licensed to provide an outpatient dental service	(i) Visit diagnoses/reasons for visit or patient problem list	
	(j) Discharge summary	25
	(k) Referral memorandum	
	(a) Visit event	
	(b) Adverse drug event history	
	(c) Ordered (prescribed) medications	30
	(d) Dispensed medications	

FIRST SCHEDULE — *continued*

<i>First column</i>	<i>Second column</i>
<i>Specified contributor or class of specified contributors</i>	<i>Types of health information</i>
5	<ul style="list-style-type: none"> <li>(e) Medication list</li> <li>(f) Vaccines administered</li> <li>(g) Cardiac report</li> <li>(h) Surgical procedure notes</li> <li>(i) Dental notes</li> </ul>
10	<ul style="list-style-type: none"> <li>(j) Visit diagnoses/reasons for visit or patient problem list</li> <li>(k) Referral memorandum</li> </ul>
15	<p>10. An HCSA licensee licensed to provide an outpatient medical service</p> <ul style="list-style-type: none"> <li>(a) Visit event</li> <li>(b) Adverse drug event history</li> <li>(c) Ordered (prescribed) medications</li> <li>(d) Dispensed medications</li> <li>(e) Medication list</li> <li>(f) Vaccines administered</li> <li>(g) Cardiac report</li> <li>(h) Surgical procedure notes</li> <li>(i) Visit diagnoses/reasons for visit or patient problem list</li> </ul>
20	<ul style="list-style-type: none"> <li>(j) Referral memorandum</li> </ul>
25	<p>11. An HCSA licensee licensed to provide an outpatient renal dialysis service</p> <ul style="list-style-type: none"> <li>(a) Visit event</li> <li>(b) Adverse drug event history</li> <li>(c) Ordered (prescribed) medications</li> <li>(d) Dispensed medications</li> <li>(e) Medication list</li> <li>(f) Vaccines administered</li> </ul>
30	<ul style="list-style-type: none"> <li>(f) Vaccines administered</li> </ul>

FIRST SCHEDULE — *continued*

<i>First column</i>	<i>Second column</i>	
<i>Specified contributor or class of specified contributors</i>	<i>Types of health information</i>	
	(g) Cardiac report	5
	(h) Surgical procedure notes	
	(i) Visit diagnoses/reasons for visit or patient problem list	
	(j) Referral memorandum	
12. An HCSA licensee licensed to provide a radiological service	(a) Adverse drug event history	10
	(b) Ordered (prescribed) medications	
	(c) Dispensed medications	
	(d) Radiology/imaging reports	
	(e) Cardiac report	15
	(f) Surgical procedure notes	
13. A retail pharmacy licensee	(a) Adverse drug event history	
	(b) Ordered (prescribed) medications	
	(c) Dispensed medications	20
	(d) Medication list	
	(e) Vaccines administered	

## PART 2

## DEFINITIONS

1. In this Schedule —	25
“acute hospital service”, “ambulatory surgical centre service”, “assisted reproduction service”, “clinical laboratory service”, “community hospital service”, “contingency care service”, “inpatient”, “nuclear medicine service”, “nursing home service”, “outpatient dental service”, “outpatient medical service”, “outpatient renal dialysis service” and “radiological service” have the meanings given by paragraph 2 of the First Schedule to the Healthcare Services Act 2020;	30

FIRST SCHEDULE — *continued*

5 “adverse drug event history” means health information about an individual regarding any event where the administration to the individual of a medication has or is likely to have any debilitating, harmful, toxic or detrimental effect on the individual’s body or health;

“cardiac report” means health information relating to the condition of an individual’s cardiovascular system that is generated by any medical device used for the purpose of assessing or diagnosing the individual’s condition;

10 “dispensed medication” means —

(a) in relation to an HCSA licensee — health information about any medication prescribed for an individual that is dispensed to the individual at the conclusion of a visit event; or

15 (b) in relation to a retail pharmacy licensee — health information about any medication sold or dispensed to an individual by a qualified pharmacist engaged or employed by the retail pharmacy licensee;

“medical device” means a health product categorised as a medical device in the First Schedule to the Health Products Act 2007;

20 “medication” means —

(a) a health product categorised as a therapeutic product in the First Schedule to the Health Products Act 2007; or

(b) a medicinal product within the meaning given by section 3 of the Medicines Act 1975;

25 “ordered (prescribed) medication” —

(a) in relation to an HCSA licensee that is licensed to provide an acute hospital service, a community hospital service, a contingency care service or a nursing home service —

30 (i) means health information about any medication prescribed for an individual (*P*) who is a patient of the HCSA licensee that is to be dispensed to *P* at the conclusion of a visit event; but

35 (ii) does not include health information about any medication prescribed for *P* for administration while *P* is an inpatient, whether or not the medication is dispensed to *P*; or

FIRST SCHEDULE — *continued*

(b) in relation to an HCSA licensee that is licensed to provide an ambulatory surgical centre service, an assisted reproduction service, a nuclear medicine service, an outpatient dental service, an outpatient medical service, an outpatient renal dialysis service or a radiological service — 5

(i) means health information about any medication prescribed for *P* that is to be dispensed to *P* at the conclusion of a visit event; but

(ii) does not include health information about any medication prescribed for *P* for administration during the visit event, whether or not the medication is dispensed to *P*; 10

“referral memorandum” means a document or information in respect of an individual that is issued by a specified contributor for the purpose of enabling or facilitating the provision of a healthcare service or community health service to the individual by another person, but excludes an individual employed or engaged by the specified contributor; 15

“surgical procedure notes” means health information about any surgical procedure performed on an individual that is listed in the Table of Surgical Procedures, other than a surgical procedure with table ranking “MSP”; 20

“Table of Surgical Procedures” means the Table of Surgical Procedures issued by the Ministry of Health and accessible at the website at <https://www.moh.gov.sg/managing-expenses/schemes-and-subsidies/medisave/inpatient-care>; 25

“visit event”, in relation to a specified contributor, means health information about any occasion on which an individual consults the specified contributor or receives a service provided by the specified contributor, whether by attending at the premises or conveyance of the specified contributor or by electronic or other means. 30

## SECOND SCHEDULE

Sections 18(1)(a)(i) and 19(1)(c)

ACCESS AND COLLECTION OF  
ACCESSIBLE HEALTH INFORMATION

5

## PART 1

SPECIFIED USERS AND  
AUTHORISED INDIVIDUALS

	<i>First column</i>	<i>Second column</i>
	<i>Specified user or class of specified users</i>	<i>Authorised individual or class of authorised individuals</i>
10	1. An HCSA licensee licensed to provide an acute hospital service	<p>(a) Registered allied health professionals</p> <p>(b) Registered dentists</p> <p>(c) Registered medical practitioners</p> <p>(d) Registered midwives</p> <p>(e) Registered nurses</p> <p>(f) Registered optometrists</p> <p>(g) Registered oral health therapists</p> <p>(h) Registered pharmacists</p> <p>(i) Audiologists</p> <p>(j) Clinical psychologists</p> <p>(k) Dietitians</p> <p>(l) Medical technologists</p> <p>(m) Pharmacy technicians</p> <p>(n) Podiatrists</p> <p>(o) Pre-registration pharmacists</p>
15		
20		
25	2. An HCSA licensee licensed to provide an ambulatory surgical centre service	<p>(a) Registered medical practitioners</p> <p>(b) Registered nurses</p>
30	3. An HCSA licensee licensed to provide an assisted reproduction service	<p>(a) Registered medical practitioners</p> <p>(b) Registered nurses</p>



SECOND SCHEDULE — *continued*

	<i>First column</i>	<i>Second column</i>
	<i>Specified user or class of specified users</i>	<i>Authorised individual or class of authorised individuals</i>
5	10. An HCSA licensee licensed to provide a medical transport service	(a) Registered medical practitioners (b) Registered nurses
10	11. An HCSA licensee licensed to provide a nuclear medicine service	(a) Registered medical practitioners (b) Registered nurses
15	12. An HCSA licensee licensed to provide a nursing home service	(a) Registered allied health professionals (b) Registered medical practitioners (c) Registered nurses (d) Registered pharmacists (e) Audiologists (f) Clinical psychologists (g) Dietitians (h) Medical technologists (i) Podiatrists
20	13. An HCSA licensee licensed to provide an outpatient dental service	(a) Registered dentists (b) Registered medical practitioners (c) Registered nurses (d) Registered oral health therapists
25	14. An HCSA licensee licensed to provide an outpatient medical service	(a) Registered allied health professionals (b) Registered medical practitioners (c) Registered nurses (d) Registered optometrists (e) Registered pharmacists (f) Audiologists (g) Clinical psychologists
30		

SECOND SCHEDULE — *continued*

<i>First column</i>	<i>Second column</i>	
<i>Specified user or class of specified users</i>	<i>Authorised individual or class of authorised individuals</i>	
	(h) Dietitians	5
	(i) Podiatrists	
15. An HCSA licensee licensed to provide an outpatient renal dialysis service	(a) Registered medical practitioners (b) Registered nurses	
16. An HCSA licensee licensed to provide a radiological service	(a) Registered medical practitioners (b) Registered nurses	10
17. A retail pharmacy licensee	(a) Registered pharmacists (b) Pre-registration pharmacists (c) Pharmacy technicians	
18. Ministry of Defence	(a) Registered allied health professionals (b) Registered dentists (c) Registered medical practitioners (d) Registered nurses (e) Registered optometrists (f) Registered oral health therapists (g) Registered pharmacists (h) Paramedics (i) Pharmacy technicians	15
19. Ministry of Home Affairs	Registered medical practitioners	
20. Singapore Armed Forces	(a) Registered allied health professionals (b) Registered dentists (c) Registered medical practitioners (d) Registered nurses (e) Registered optometrists	25
		30

SECOND SCHEDULE — *continued*

<i>First column</i>	<i>Second column</i>
<i>Specified user or class of specified users</i>	<i>Authorised individual or class of authorised individuals</i>
5	(f) Registered oral health therapists (g) Registered pharmacists (h) Paramedics (i) Pharmacy technicians
21. Singapore Civil Defence Force 10	(a) Registered medical practitioners (b) Registered nurses (c) Paramedics
22. Singapore Prison Service 15	(a) Registered allied health professionals (b) Registered dentists (c) Registered medical practitioners (d) Registered nurses (e) Registered pharmacists (f) Clinical psychologists (g) Pharmacy technicians

20

## PART 2

## DEFINITIONS

## 1. In this Schedule —

“enlisted personnel” has the meaning given by section 6;

“paramedic” means an individual who —

25

(a) is employed or engaged by a specified user to perform the functions of a paramedic; or

(b) is an enlisted personnel of a specified user and is appointed or authorised by the specified user to perform the functions of a paramedic;

SECOND SCHEDULE — *continued*

- “pre-registration pharmacist” means an individual who, for the purpose of the individual satisfying the requirements for registration as a registered pharmacist under the Pharmacists Registration Act 2007, is approved by the Singapore Pharmacy Council to undergo pre-registration training with an HCSA licensee licensed to provide an acute hospital service or a community hospital service or a retail pharmacy licensee that is approved by the Council; 5
- “registered allied health professional” means an individual who is an allied health professional registered under the Allied Health Professions Act 2011 and holds a valid practising certificate under that Act; 10
- “registered dentist” means an individual who is registered under the Dental Registration Act 1999 as a registered dentist and holds a valid practising certificate under that Act;
- “registered medical practitioner” means an individual who is registered under the Medical Registration Act 1997 and holds a valid practising certificate under that Act; 15
- “registered midwife” means an individual who is registered under the Nurses and Midwives Act 1999 as a registered midwife and holds a valid practising certificate under that Act; 20
- “registered nurse” means an individual who is registered under the Nurses and Midwives Act 1999 as a registered nurse and holds a valid practising certificate under that Act;
- “registered optometrist” means an individual who is registered under the Optometrists and Opticians Act 2007 for the carrying out of any practice of optometry and holds a valid practising certificate under that Act; 25
- “registered oral health therapist” means an individual who is registered under the Dental Registration Act 1999 as a registered oral health therapist and holds a valid practising certificate under that Act;
- “registered pharmacist” means an individual who is registered under the Pharmacists Registration Act 2007 as a registered pharmacist and holds a valid practising certificate under that Act. 30

## THIRD SCHEDULE

Section 19(3)

WRITTEN LAWS UNDER WHICH  
SPECIFIED EXAMINATIONS CARRIED OUT FOR  
PURPOSES OF SECTION 19(3)

5

**Protection of public health**

## 1. Biological Agents and Toxins Act 2005

10

- (a) Medical examination of an individual under section 6(6)(e)(i), 7(3)(b)(v)(A), 15(5)(e)(i), 16(2)(b)(v)(A), 23(2)(e)(i), 27(3)(e)(i), 31(4)(b)(v)(A), 45(1)(b)(v)(A), 50(7)(e)(v)(A), 51(6)(h)(i), 52(1)(f) or 53(1)(i)(i)

## 2. Control of Vectors and Pesticides Act 1998

- (a) Medical examination of an individual under section 20 or 35(2)(a)  
(b) Post-mortem examination of a corpse under section 35(2)(c)

15

## 3. Coroners Act 2010

- (a) Post-mortem examination under section 18(1) or (2)  
(b) Special examination by a person appointed by a pathologist under section 19(2)(b)

## 4. Environmental Public Health Act 1987

20

- (a) Medical examination of an individual under section 37(1)

## 5. Immigration Act 1959

- (a) Medical examination of an individual under section 29(1)

## 6. Immigration Regulations (Rg 1)

- (a) Medical surveillance of an individual under regulation 8(2A)

25

## 7. Infectious Diseases Act 1976

- (a) Medical examination of an individual under section 7(2)(b), 8(1), 17(3)(d), 29(1)(b), 45A(1), 45B(1) or 55(1)(f)  
(b) Post-mortem examination of the body of a deceased person under section 9

30

## 8. Infectious Diseases (Quarantine) Regulations (Rg 1)

- (a) Medical examination of an individual under regulation 21(1)

THIRD SCHEDULE — *continued*

9. Registration of Births and Deaths Act 2021
- (a) Examination of the body of a deceased person by a medical practitioner under section 23(1)(a)
  - (b) Ascertainment of relevant information about a deceased person's medical history and the circumstances of the deceased person's death by a medical practitioner under section 23(1)(b) 5
10. Sale of Food Act 1973
- (a) Medical examination of an individual under section 22(1)
11. Wholesome Meat and Fish (Processing Establishments and Cold Stores) Rules (R 3) 10
- (a) Medical examination of an individual for the purposes of rule 7(2)
  - (b) Medical examination or medical test of an individual for the purposes of rule 7(4)
12. Wholesome Meat and Fish (Slaughter-houses) Rules (R 4) 15
- (a) Medical examination of an individual for the purposes of rule 7(2)
  - (b) Medical examination or medical test of an individual for the purposes of rule 7(4)
- Individuals involved in hazardous work**
13. Hydrogen Cyanide (Fumigation) Regulations 1989 20
- (a) Medical examination of an individual for the purposes of obtaining a certificate under regulation 12(a)
  - (b) Medical examination of an individual under regulation 12(b)
14. Radiation Protection (Ionising Radiation) Regulations 2023
- (a) Medical examination of an individual under regulation 16(2)(a) 25
  - (b) Medical examination of an individual for the purposes of regulation 30(6)(b) or (7)(c) or 35(9)(c) or (11)(d)
  - (c) Medical examination of an individual affected by any radiation accident occurring in a non-medical application of ionising radiation or radioactive materials in relation to the preparation of a preliminary written report or final full written report mentioned in regulation 72(2) 30
15. Radiation Protection (Non-Ionising Radiation) Regulations (Rg 1)
- (a) Medical examination of an individual for the purposes of regulation 8

THIRD SCHEDULE — *continued*

(b) Medical examination of an individual under regulation 20(c)

## 16. Workplace Safety and Health (Construction) Regulations 2007

(a) Medical examination of an individual for the purposes of regulation 102(6)

## 17. Workplace Safety and Health (Medical Examinations) Regulations 2011

(a) Medical examination of an individual for the purposes of regulation 4(1) or (2), 5(1) or 6(1)

## 18. Workplace Safety and Health (Operation of Cranes) Regulations 2011

(a) Medical examination of an individual for the purpose of obtaining a medical certificate mentioned in regulation 7(2) or 12(2)(c)

**Licensing of drivers**

## 19. Road Traffic Act 1961

(a) Carrying out a prescribed medical examination of an individual mentioned in section 35(10A)(a)

(b) Carrying out a prescribed test of an individual mentioned in section 37(5) or (8)

## 20. Road Traffic (Motor Vehicles, Driving Licences) Rules (R 27)

(a) Medical examination of an individual for the purposes of rule 4A(1)(a) or 5(2)(a)

**Uniformed and related services and enlistment**

## 21. Civil Defence Act 1986

(a) Medical or dental examination or test of an individual under section 32A(a)

(b) Medical examination of an individual under section 101A(1)(f)

## 22. Enlistment Act 1970

(a) Examination of an individual required to report for a fitness examination within the meaning given by section 2

(b) Medical examination of an individual under section 8(6) or (7)

## 23. Home Team Corps Regulations 2018

(a) Medical examination of an individual for the purposes of regulation 15 or 36

THIRD SCHEDULE — *continued*

24. National Cadet Corps Regulations (Rg 1)
- (a) Medical examination of an individual for the purposes of regulation 10
25. Police Force Act 2004
- (a) Medical or dental examination or test of a police officer that is required under any lawful order (whether given orally or in writing) or under the Police General Orders, any Force Orders or any Standing Orders made under the Act 5
26. Police (Special Constabulary) Regulations (Rg 3)
- (a) Medical examination of an individual for the purposes of regulation 6A(1) or (2) 10
27. Singapore Armed Forces (Volunteers) Regulations (Rg 7)
- (a) Medical examination of an individual for the purposes of regulation 6(1)
- Individuals providing healthcare services** 15
28. Allied Health Professions Act 2011
- (a) Medical examination of an individual for the purposes of section 21(2)
29. Allied Health Professions (Professional Conduct and Discipline) Regulations 2013
- (a) Medical examination of a registered allied health professional mentioned in regulation 26(1)(a) 20
30. Dental Registration Act 1999
- (a) Medical examination of an individual for the purposes of section 15(2) or 22(2)
31. Dental Registration Regulations (Rg 1) 25
- (a) Medical examination of a registered person mentioned in regulation 29(1)(a) or 37(4)
32. Medical Registration Act 1997
- (a) Medical examination of an individual mentioned in section 29(4)(b)
33. Medical Registration Regulations 2010 30
- (a) Medical examination of a practitioner pursuant to a direction of the Health Committee under regulation 50(1) or 57(4)

THIRD SCHEDULE — *continued*

## 34. Nurses and Midwives Act 1999

(a) Medical examination of an individual for the purposes of section 15(1)

## 35. Nurses and Midwives Regulations 2012

5 (a) Medical examination of a registered nurse, an enrolled nurse, a registered midwife or an Advanced Practice Nurse mentioned in regulation 34(1)(a) or 41(2)

## 36. Pharmacists Registration Act 2007

(a) Medical examination of an individual for the purposes of section 21(2)

## 10 37. Pharmacists Registration (Registration of Pharmacists) Regulations 2013

(a) Medical examination of an individual for the purposes of a medical report mentioned in regulation 7(3)(a)(ii)

(b) Medical examination of an individual required by the Singapore Pharmacy Council under regulation 8(3)

15 **Court proceedings**

## 38. Criminal Procedure Code 2010

(a) Medical examination of an individual for the purposes of section 247(3) or (6), 252(3), 253(2), 254(1) or 256(1) or (2)

## 39. State Courts Act 1970

20 (a) Medical examination of an individual pursuant to section 31(2)(c), 50(1)(b), 51(1)(b) or 52(1B)(b)(iii)

## 40. Supreme Court of Judicature Act 1969

(a) Medical examination of an individual pursuant to paragraph 19 or 20 of the First Schedule to the Act

25 **Sentencing in criminal matters and implementation of sentences imposed**

## 41. Criminal Procedure Code 2010

(a) Medical examination of an individual for the purposes of a report mentioned in section 304(3), 305(3) or 339(2)

30 (b) Medical examination of an offender for the purposes of a medical officer's certificate mentioned in section 331(1)

THIRD SCHEDULE — *continued***Arrest and detention of individuals**

42. Civil Defence (Detention) Regulations (Rg 3)
- (a) Medical examination of an individual for the purposes of regulation 8(1) or 34(1) 5
  - (b) Medical examination of an arrested person or a person serving detention in relation to an approval by a medical officer under regulation 17(5)
  - (c) Medical examination of an arrested person or a person serving detention for the purposes of regulation 27(4) or 28A(1) 10
  - (d) Periodic medical observation of an arrested person or a person serving detention for the purposes of regulation 28
43. Criminal Procedure Code (Corrective Training and Preventive Detention) Regulations 2010
- (a) Medical examination of a prisoner in relation to a certification by a medical officer under regulation 13(3) 15
44. Internal Security (Detained Persons) Rules (R 1)
- (a) Medical examination of a detained person for the purposes of rule 17A(2)(a), 53(b) or 61(1)
  - (b) Medical examination of a detained person in relation to a certification by a medical officer under rule 53(a) or 75 20
45. Intoxicating Substances (Discipline in Approved Centres) Regulations (Rg 2)
- (a) Medical examination of an inmate for the purposes of regulation 5(2)
46. Intoxicating Substances (Treatment and Rehabilitation) Regulations (Rg 3) 25
- (a) Medical examination of an inmate for the purposes of regulation 4 or 5(1)
47. Mental Health (Care and Treatment) Act 2008
- (a) Examination of an individual by a medical practitioner under section 7(1)(a) 30
  - (b) Examination of an individual by a designated medical practitioner at a psychiatric institution under section 10(1)
48. Misuse of Drugs (Approved Institutions) (Discipline) Regulations (Rg 5)
- (a) Medical examination of an inmate for the purposes of regulation 5(2)

THIRD SCHEDULE — *continued*

- (b) Medical examination of an inmate in relation to a certification by a medical officer under regulation 12(c)
- 5 49. Misuse of Drugs (Approved Institutions, Medical Observation and Treatment and Rehabilitation) Regulations (Rg 3)
- (a) Medical examination of a suspected drug addict or an inmate for the purposes of regulation 4 or 8(1)
- 10 50. Police Force (Special Constabulary — Detention) Regulations 2016
- (a) Medical examination of an individual for the purposes of regulation 8(1)
- (b) Medical examination of a detainee in relation to an approval by a medical officer under regulation 17(5)
- (c) Medical examination of a detainee for the purposes of regulation 26(4)(a), 28(1) or 35(1)
- 15 (d) Periodic medical observation of a detainee for the purposes of regulation 27
51. Prisons Act 1933
- (a) Medical examination of a prisoner in relation to a certification by a medical officer under section 67 or 77(4)
- 20 52. Prisons (Lock-ups in Specified Court Houses) Regulations 2011
- (a) Medical examination of a lock-up prisoner for the purposes of regulation 16(3)(a)
53. Prisons (Police Lock-ups) Regulations 2013
- (a) Examination of a lock-up prisoner for the purposes of regulation 17(3)(a)
- 25 54. Prisons Regulations (Rg 2)
- (a) Medical examination of a prisoner for the purposes of regulation 38(2)(a), 74A, 75(1), 94(1) or 142
- (b) Medical examination of a vagrant for the purposes of regulation 94(2)
- 30 55. Singapore Armed Forces (Detention and Imprisonment) Regulations (Rg 3)
- (a) Medical examination of a detainee or military prisoner for the purposes of regulation 6(3)(b), 13(d), 21(1), 39(4), 47(3) or 50(1)

THIRD SCHEDULE — *continued*

## 56. Singapore Armed Forces (Disciplinary Barracks) Regulations (Rg 8)

- (a) Medical examination of an individual for the purposes of regulation 8(c) or 28

**Medical examinations relating to making of mandatory treatment orders under written law**

5

## 57. Protection from Harassment Act 2014

- (a) Medical examination of an individual in relation to a formal assessment report mentioned in section 13B(3)(b)
- (b) Medical examination of an individual in relation to a preliminary assessment report mentioned in section 13B(4)(a)

10

## 58. Women's Charter 1961

- (a) Medical examination of an individual in relation to a preliminary assessment report mentioned in section 60F(6)(a)
- (b) Medical examination of an individual in relation to a formal assessment report mentioned in section 60F(9)(a)

15

**Vulnerable individuals**

## 59. Adoption of Children Act 2022

- (a) Medical, psychiatric or psychological assessment of any joint applicant or sole applicant for or issued with an Adoption Suitability Assessment pursuant to a direction of an authorised adoption agency or the Guardian-in-Adoption under section 19(2)(a)(i)
- (b) Medical, psychiatric or psychological assessment of any joint applicant or sole applicant, or any relevant person of a child before the court, pursuant to a direction of the Guardian-in-Adoption under section 29(1)(a)(i)
- (c) Medical, psychiatric or psychological assessment of a child pursuant to a direction of the Guardian-in-Adoption under section 29(1)(c)
- (d) Medical, psychiatric or psychological assessment of any joint applicant or sole applicant of an adoption application, or any relevant person of the child before the court, pursuant to an order of the court under section 34(1)(b)(i)
- (e) Medical, psychiatric or psychological assessment of a child before the court pursuant to an order of the court under section 34(1)(b)(ii)

20

25

30

THIRD SCHEDULE — *continued*

## 60. Children and Young Persons Act 1993

(a) Assessment of a child or young person by a registered medical practitioner or psychologist under section 10(1)(b)

5 (b) Assessment of a child or young person by a registered medical practitioner mentioned in section 13(2) that is authorised by a warrant issued by a Magistrate's Court under section 13

10 (c) Medical or psychological assessment of a child or young person, or the parent or guardian of a child or young person, required by the Youth Court under section 47(11)(b)

(d) Assessment of a child or young person by a registered medical practitioner ordered by the Youth Court under section 54(14)(c)

15 (e) Medical, psychiatric or psychological assessment of the parent or guardian of a child or young person ordered by the Youth Court under section 54(14)(d)

## 61. Children and Young Persons (Government Homes) Regulations 2011

(a) Medical examination of a resident under regulation 11

## 62. Children and Young Persons (Licensing of Homes) Regulations 2011

(a) Medical examination of a resident under regulation 14

## 20 63. Destitute Persons (Welfare Homes) Rules (R 1)

(a) Medical examination of a destitute person admitted into a welfare home under rule 24(1)

## 64. Vulnerable Adults Act 2018

25 (a) Assessment (within the meaning given by section 2(1)) of an individual or a vulnerable adult under section 6(1)(a) or (b)

(b) Assessment (within the meaning given by section 2(1)) of an individual pursuant to a court order under section 14(4)(c)

## 65. Women's Charter 1961

30 (a) Assessment (within the meaning given by section 59(6)) of an individual by a protector or a qualified assessor under section 59(1)

## 66. Women's Charter (Protection of Women and Girls) Rules (R 2)

(a) Medical examination of a girl under rule 55(a), (b) or (e)

(b) Examination of the teeth of a girl under rule 57(1)

FOURTH SCHEDULE

Sections 47 and 51(1)(a) and (2)(c)

DISCLOSURE, COLLECTION AND  
USE OF RELEVANT INFORMATION

PART 1

5

<i>First column</i>	<i>Second column</i>	<i>Third column</i>
<i>Discloser or class of discloser</i>	<i>Recipient or class of recipient</i>	<i>Use case</i>
Continuity of care for national health initiatives		
1. Any of the following persons: (a) a public healthcare institution; (b) a cluster HQ	AIC	(a) Identifying individuals who may require a community health service; and (b) contacting and engaging the individuals mentioned in paragraph (a), as part of the Healthier SG programme or the Age Well SG programme established by the Government — (i) to encourage those individuals to make behavioural changes to reduce or eliminate the risk of developing or aggravating their health conditions; or (ii) to refer those individuals to providers of any healthcare service or community health service to enable them to better manage or address their health conditions.

10

15

20

25

30

35

FOURTH SCHEDULE — *continued*

	<i>First column</i>	<i>Second column</i>	<i>Third column</i>
	<i>Discloser or class of discloser</i>	<i>Recipient or class of recipient</i>	<i>Use case</i>
5	2. AIC	Any of the following persons: (a) a public healthcare institution;	(a) Identifying individuals who may require a community health service; and
10		(b) a cluster HQ	(b) contacting and engaging the individuals mentioned in paragraph (a), as part of the Healthier SG programme or the Age Well SG programme established by the Government —
15			(i) to encourage those individuals to make behavioural changes to reduce or eliminate the risk of developing or aggravating their health conditions; or
20			(ii) to refer those individuals to providers of any healthcare service or community health service to enable them to better manage or address their health conditions.
25			
30			

FOURTH SCHEDULE — *continued*

<i>First column</i>	<i>Second column</i>	<i>Third column</i>	
<i>Discloser or class of discloser</i>	<i>Recipient or class of recipient</i>	<i>Use case</i>	
Outreach for national health initiatives			5
3. Any public agency	AIC	<p>(a) Identifying individuals above 60 years of age who reside at a place other than the place of residence registered under the National Registration Act 1965; and</p> <p>(b) contacting and engaging the individuals mentioned in paragraph (a) —</p> <p style="padding-left: 40px;">(i) to check on the physical or mental wellbeing of those individuals; and</p> <p style="padding-left: 40px;">(ii) if necessary, to refer those individuals to providers of any healthcare service or community health service that are participating in the Age Well SG programme established by the Government.</p>	<p>10</p> <p>15</p> <p>20</p> <p>25</p> <p>30</p>

FOURTH SCHEDULE — *continued*

<i>First column</i>	<i>Second column</i>	<i>Third column</i>
<i>Discloser or class of discloser</i>	<i>Recipient or class of recipient</i>	<i>Use case</i>
5 4. Any public agency	Any of the following persons: (a) a public healthcare institution; 10 (b) a cluster HQ; 15 (c) AIC	As part of the Healthier SG programme established by the Government — (a) identifying and engaging individuals who may benefit from taking up, continuing or completing any action or measure to monitor, maintain or improve their health; and (b) to engage and encourage those individuals to take up, continue or complete any action or measure mentioned in paragraph (a).

## PART 2

## DEFINITIONS

## 1. In this Schedule —

“AIC” means the Agency for Integrated Care Pte Ltd;

“cluster HQ” means any of the following:

- 25 (a) National Healthcare Group Pte Ltd;
- (b) National University Health System Pte Ltd;
- (c) Singapore Health Services Pte Ltd;

“public healthcare institution” means a person that —

- 30 (a) is or is controlled by a cluster HQ or its subsidiary; and
- (b) is licensed under the Healthcare Services Act 2020 to provide any licensable healthcare service.

## EXPLANATORY STATEMENT

This Bill seeks to —

- (a) introduce a statutory framework governing —
  - (i) the contribution of health information about individuals to the national electronic records system;
  - (ii) the access, collection and disclosure of accessible health information made available on the national electronic records system; and
  - (iii) the access, collection, disclosure and use of information derived from health information contributed to the national electronic records system;
- (b) introduce a statutory framework under which individually-identifiable information about individuals may be shared by specified persons and public agencies for the implementation of Government programmes and schemes to maintain or improve the physical or mental health and wellbeing of individuals; and
- (c) impose cybersecurity and data security requirements on persons subject to or using the statutory frameworks under the Bill.

The Bill also makes a related amendment to the Human Organ Transplant Act 1987.

Clause 1 relates to the short title and commencement.

### PART 1

#### GENERAL

Part 1 (clauses 2 to 5) introduces the fundamental concepts used in the Bill.

Clause 2 is a general interpretation provision. It contains definitions of terms used in the Bill, including key terms such as “community health service”, “contribute”, “contributor”, “health data intermediary”, “process”, “relevant HDI” and “user”. “Contributor” means a specified contributor or an approved contributor. “User” means a specified user or an approved user.

Clause 3 defines key terms relating to information about individuals in the Bill, such as “health information” and “accessible health information”. “Health information” about an individual means administrative information or clinical information about the individual.

Clause 4 sets out the purposes of the Bill.

Clause 5 sets out the provisions of the Bill that apply to the Government. The clause further provides that unless the Bill provides otherwise, nothing in the Bill affects any authority, right, privilege or immunity conferred, or any obligation or limitation imposed, by or under any other written law or any rule of law, contract or rule of professional conduct or ethics.

## PART 2

### NATIONAL ELECTRONIC RECORDS SYSTEM

Part 2 (clauses 6 to 44) provides for —

- (a) the contribution of health information about individuals to the national electronic records system;
- (b) the access, collection and disclosure of accessible health information about individuals that is made available on the national electronic records system; and
- (c) the access, collection, disclosure and use of derived information derived from accessible health information about individuals.

Division 1 of Part 2 contains general provisions for the purposes of the Part.

Clause 6 sets out definitions for the purposes of Part 2, including the key definitions of “excluded purpose”, “derived information” and “requestor”.

Clause 7 defines “national electronic records system” for the purposes of the Bill.

Clause 8 provides that the Minister may, by order in the *Gazette*, designate any person as a System Operator to operate, administer and maintain the national electronic records system. A System Operator must perform those functions in accordance with the Minister’s directions.

Clause 9 provides that Part 2 applies equally to a contributor, user or requestor who does anything under Part 2 through a relevant HDI and to one who acts directly.

Clause 10 provides that Part 2 applies to and in relation to health information about any individual who —

- (a) is a citizen or permanent resident of Singapore;
- (b) is issued with a foreign identification number; or
- (c) belongs to any other class of individuals that may be prescribed.

Clause 11 provides that the consent of an individual (*P*) is not required for —

- (a) the contribution of health information about *P*;

- (b) the access, collection and disclosure of accessible health information about *P*; or
- (c) the access, collection, disclosure and use of derived information derived from accessible health information about *P*,

where the contribution, access, collection, disclosure or use (as the case may be) takes place in accordance with Part 2.

Additionally, nothing in Part 2 allows a person to access, collect or disclose accessible health information about *P* on the basis that *P* consents or has consented to the person doing so.

Division 2 of Part 2 contains provisions relating to the contribution of health information about individuals to the national electronic records system.

Clause 12 provides that the following persons (specified contributors) must contribute health information about any individual in accordance with Part 2:

- (a) a person to whom a licence is granted under the Healthcare Services Act 2020 to provide a licensable healthcare service (HCSA licensee), where the HCSA licensee is specified in, or belongs to a class of HCSA licensees specified in, the first column of Part 1 of the First Schedule;
- (b) a person who holds a licence issued under the Health Products Act 2007 to carry on a retail pharmacy business at or from the retail pharmacy specified in the licence (retail pharmacy licensee), where the retail pharmacy licensee is specified in, or belongs to a class of retail pharmacy licensees specified in the first column of Part 1 of the First Schedule;
- (c) a person (other than an HCSA licensee or retail pharmacy licensee) or public agency specified in, or belonging to a class of persons or public agencies specified in, the first column of Part 1 of the First Schedule.

A specified contributor must contribute the types of health information specified opposite the specified contributor in the second column of Part 1 of the First Schedule about any individual mentioned in clause 12(2), (3) or (4), as the case may be.

Under clause 13, the Minister may approve any person or public agency (approved contributor) to contribute health information about any individual. The Minister must, as soon as is practicable after approving an approved contributor, publish a notification in the *Gazette* specifying —

- (a) the class or classes of individuals whose health information the approved contributor may contribute;
- (b) the types of health information that the approved contributor may contribute; and

- (c) the conditions and restrictions (if any) that the approved contributor must comply with in relation to the contribution of health information.

Under clause 14, a contributor must comply with all requirements, conditions and restrictions relating to the contribution of health information that may be prescribed. In relation to an approved contributor, this obligation is in addition to the obligation to comply with the conditions and restrictions mentioned in clause 13(2)(c). Also, a contributor must comply with the administrative instructions and technical requirements of a System Operator in relation to the contribution of health information.

Clause 15 allows the Minister to direct a specified contributor to contribute health information about any individual if the specified contributor fails or neglects to do so.

Also, the Minister may by written notice direct —

- (a) a specified contributor who fails or neglects to comply with any requirement, condition or restriction mentioned in clause 14(1) or any administrative instruction or technical requirement of a System Operator mentioned in clause 14(4); or
- (b) an approved contributor who fails or neglects to comply with any condition or restriction mentioned in clause 13(2)(c), any condition or requirement mentioned in clause 14(1) or any administrative instruction or technical requirement of a System Operator mentioned in clause 14(4),

to comply with the requirement, condition, restriction, administrative instruction or technical requirement, as the case may be.

Non-compliance with the Minister's direction under clause 15 is an offence.

Division 3 of Part 2 pertains to the access, collection and disclosure of accessible health information about individuals that is made available on the national electronic records system.

Clause 16 provides that a person may access, collect or disclose accessible health information about an individual only if it is carried out in accordance with Part 2 or is required or permitted under any other written law. The access, collection or disclosure of accessible health information about an individual is not considered to be required or permitted under any written law merely because the individual has consented or has given his or her consent in accordance with Part 4 of the Personal Data Protection Act 2012 (PDPA), or such consent is not required under Part 4 of the PDPA.

Clause 17 provides that an individual (*P*), or *P*'s authorised representative as defined in clause 17(2), may access and collect accessible health information about *P* in any manner prescribed. A System Operator must comply with the

Minister's directions in relation to the type or types of accessible health information about *P* that *P* or *P*'s authorised representative may access and collect.

Clause 18 defines “authorised individual” in relation to a specified user or an approved user.

Clause 19 provides that certain persons specified in the Second Schedule (specified users) may access and collect accessible health information about an individual (*P*) but only for a purpose specified in clause 19(2) (specified purpose).

The specified purposes are the following:

- (a) the provision of a healthcare service to *P* but excluding the provision of a healthcare service for an excluded purpose;
- (b) the carrying out of any medical, dental, psychiatric or psychological examination, test or assessment of *P* that is required or authorised by or under, or is necessary for the purpose of complying with, any written law specified in the Third Schedule or any order made under any such written law, and any purpose relating to the carrying out of the examination.

The excluded purposes relate to matters concerning —

- (a) *P*'s employment or appointment to office, engagement under a contract for services or entering or continuing under a platform work agreement with any platform operator; and
- (b) the insurance of *P* or any other individual, and the making and processing of insurance claims.

An authorised individual (*X*) of a specified user may access and collect accessible health information about *P* if, and only if —

- (a) the access and collection of that information is necessary to enable *X* to perform or discharge his or her duties for the specified user; and
- (b) those duties relate to the specified user carrying out a specified purpose.

Clause 20 allows the Minister to approve any person or public agency to access and collect accessible health information about any individual (*P*) for any of the following purposes:

- (a) the provision of any healthcare service to *P* by that person or public agency or any individual employed or engaged by that person or public agency, but not the provision of any such service for an excluded purpose;
- (b) the provision of any community health service to *P* by that person or public agency or any individual employed or engaged by that person or

public agency, but not the provision of any such service for an excluded purpose;

(c) any public health purpose.

The excluded purposes are the same as those that apply in relation to clause 19.

The Minister must, as soon as is practicable after approving an approved user under clause 20, publish a notification in the *Gazette* specifying —

- (a) the class or classes of individuals whose accessible health information the approved user may access and collect;
- (b) the purpose or purposes for which the approved user may access and collect accessible health information;
- (c) the types of accessible health information that the approved user may access and collect;
- (d) the authorised individuals (by name or description), or the class or classes of authorised individuals, of the approved user who may access those types of accessible health information; and
- (e) the conditions and restrictions (if any) that the approved user must comply with.

Clause 21 sets out the circumstances in which a specified user or an authorised individual of a specified user, or an approved user or an authorised individual of an approved user, may disclose accessible health information. The clause also sets out the conditions that must be satisfied for such disclosure.

Clause 22 sets out the obligations of a user. The clause provides that a user must —

- (a) comply with all requirements, conditions and restrictions relating to the access, collection, retention and disclosure of accessible health information as may be prescribed. In the case of an approved user, this obligation is in addition to the obligation to comply with the conditions and restrictions mentioned in clause 20(2)(e);
- (b) establish and implement appropriate policies and practices (including policies and practices in respect of any matters relating to the access, collection, retention and disclosure of accessible health information that may be prescribed) to ensure that the user's authorised individuals access, collect, retain and disclose accessible health information in accordance with Part 2; and
- (c) ensure that every authorised individual of the user complies with all such requirements, conditions and restrictions and policies and practices.

A user who contravenes any of these obligations commits an offence.

Further, a user and every authorised individual of a user must comply with every administrative instruction or technical requirement of a System Operator in relation to the access and collection of accessible health information.

Finally, a user must notify a System Operator, within the prescribed time and in the form and manner prescribed (if any), of the cessation for any reason of any individual as an authorised individual of the user, or any change in an authorised individual's designation or role in the user's organisation. A user who fails to notify the cessation or change commits an offence.

Clause 23 allows the Minister, by written notice, to direct any person defined in clause 23(4) (person concerned) to —

- (a) stop accessing or collecting accessible health information about any individual;
- (b) delete or destroy all copies of accessible health information about any individual that are in the possession or under the control of the person concerned; or
- (c) take all reasonable steps to retrieve all copies of accessible health information about any individual from any person to whom the person concerned has disclosed the accessible health information, and delete or destroy all such copies.

If the Minister directs the person concerned to delete or destroy all copies of accessible health information, the Minister may additionally direct the person concerned to delete or destroy the copies in the manner specified by the Minister, and certify that the copies have been so deleted or destroyed.

A person concerned who, without reasonable excuse, fails to comply with the Minister's direction under clause 23 commits an offence.

Division 4 of Part 2 contains provisions relating to derived information and the access, collection, disclosure and use of derived information.

Clause 24 sets out definitions for the purposes of Division 4. "Type 1 derived information" means derived information that is in the form of individually-identifiable health information. "Type 2 derived information" means derived information that is in the form of aggregated or anonymised health information.

Clause 25 provides that a person who satisfies the prescribed criteria and requirements or a public agency may apply to the Minister to obtain derived information. An application to obtain derived information must satisfy the requirements set out in the clause. The Minister may, having regard to and giving appropriate weight to a non-exhaustive list of matters specified and any other matter and evidence that may be relevant, approve —

- (a) an application to obtain type 1 derived information if the application is made for a purpose that relates to or promotes public health; or
- (b) an application to obtain type 2 derived information if the Minister is satisfied, having regard to the purpose for which the application is made, that it is in the public interest to do so.

Further, if the application is an application to obtain type 1 derived information, the Minister may provide the applicant with type 2 derived information instead, if the Minister is of the opinion that the purpose specified in the application can be satisfied by the provision of type 2 derived information.

A requestor who contravenes any condition or restriction imposed on the Minister's approval under clause 25 granted to the requestor commits an offence.

Clause 26 provides that a requestor may, subject to any condition or restriction imposed on the Minister's approval under clause 25 granted to the requestor, access, collect, disclose and use derived information obtained under the Minister's approval for any purpose specified in that approval without the prior consent of any individual to whom the derived information relates.

Clause 27 sets out the obligations of a requestor. Under the clause, a requestor must establish and implement policies and practices to ensure that derived information is accessed, collected, disclosed and used in accordance with the provisions of the Bill. A requestor who fails to establish and implement such policies and practices commits an offence.

The clause also sets out prohibitions against the disclosure, use and retention of derived information by requestors. A requestor who contravenes any of these prohibitions commits an offence.

Clause 28 allows the Minister to direct a requestor —

- (a) to delete or destroy the derived information that the requestor obtained under the Minister's approval granted under clause 25, and all copies of the derived information in the possession or under the control of the requestor; or
- (b) take all reasonable steps to retrieve all copies of the derived information from any person to whom the requestor disclosed the derived information, and delete or destroy all such copies.

If the Minister directs the requestor to delete or destroy all copies of derived information, the Minister may additionally direct the requestor to delete or destroy the copies in the manner specified by the Minister, and certify that the copies have been deleted or destroyed.

A requestor who fails to comply with the Minister's direction under clause 28 commits an offence.

Division 5 of Part 2 contains provisions relating to access restrictions.

Clause 29 defines access restrictions for the purposes of the Bill. There are 2 types of access restrictions:

- (a) a class 1 access restriction prevents the access, collection and disclosure of accessible health information about an individual (*P*);
- (b) a class 2 access restriction restricts the access, collection or disclosure of accessible health information about *P* in respect of one or more of the following matters:
  - (i) the type or types of accessible health information about *P* that may be accessed, collected or disclosed;
  - (ii) any attribute of or relating to any type of accessible health information about *P* that may be prescribed;
  - (iii) the specified user, or the approved user approved to access and collect accessible health information about any individual for a purpose mentioned in clause 20(1)(a) or (b), or the class of such users, who may access, collect or disclose accessible health information about *P*;
  - (iv) the purpose or purposes for which accessible health information about *P* may be accessed, collected or disclosed;
  - (v) the time or times at which, or the period or periods during which, accessible health information about *P* may be accessed, collected or disclosed.

Different types of class 2 access restrictions may be prescribed.

Clause 30 provides that, subject to the specified exceptions —

- (a) a class 1 access restriction that is in force prevents the access, collection and disclosure of accessible health information about an individual; and
- (b) a class 2 access restriction that is in force allows the access, collection and disclosure of accessible health information about an individual only to the extent permitted under that access restriction.

The exceptions specified in the clause are the following:

- (a) the access, collection or disclosure by a user of any type of accessible health information about an individual as may be prescribed;
- (b) the access, collection or disclosure of accessible health information about an individual by a user, if the access, collection or disclosure is necessary to respond to an emergency that threatens the individual's life or health;

- (c) the provision of derived information to a requestor in relation to an approval granted by the Minister under clause 25(2) or (3);
- (d) the access, collection or disclosure of accessible health information about an individual that is required or permitted under any other Act or by an order of court. However, access, collection or disclosure of accessible health information is not considered to be required or permitted under any Act merely because the individual has consented or has given his or her consent in accordance with Part 4 of the PDPA, or such consent is not required under Part 4 of the PDPA.

Clause 31 provides for how an access restriction may be imposed or revoked.

Clause 32 provides that an access restriction may not be revoked under clause 31 in respect of accessible health information about a deceased individual, where the access restriction is in force immediately before the date of death of the deceased individual.

Clause 33 sets out a transitional provision for administrative measures to prevent or restrict access to accessible health information about an individual imposed under the current governance framework for the national electronic records system, where the measures are in force immediately before the date of commencement of clause 31. These administrative measures correspond to access restrictions under the Bill.

Division 6 of Part 2 concerns the actions that may be taken against a contributor, a user or an authorised individual of a user.

Clause 34 empowers an authorised officer to direct a System Operator to take any action described in clause 34(2) against a contributor or user or an authorised individual of a user if any of the following applies:

- (a) the authorised officer is satisfied that the contributor, user or authorised individual of a user is contravening or has contravened any requirement under Part 2, the contravention of which is not an offence;
- (b) the authorised officer —
  - (i) has reason to believe that the contributor, user or authorised individual of a user is contravening or has contravened any provision of the Bill, the contravention of which is an offence; and
  - (ii) is satisfied that it is necessary to take the action in order to prevent or minimise any harm or damage to the national electronic records system pending the outcome of any proceedings against the contributor, user or authorised

individual of a user for an offence arising from the contravention;

- (c) the contributor, user or authorised individual of a user has been convicted of an offence under the Bill;
- (d) the authorised officer is satisfied that the public interest so requires.

Clause 35 sets out the procedure that an authorised officer must comply with before giving a direction under clause 34.

Clause 36 provides that a contributor or user or an authorised individual of a user aggrieved by an authorised officer's decision to give a direction under clause 34 to take action against the contributor, user or authorised individual of a user has a right of appeal to the Minister.

Clause 37 provides that the Minister may designate a Second Minister, any Minister of State or any Parliamentary Secretary to hear and determine any appeal or a specific appeal under clause 36 in the Minister's place.

Division 7 of Part 2 sets out offences relating to accessible health information and derived information.

Clause 38 provides for offences relating to the improper access or collection of accessible health information. In particular, the clause provides for the following prohibitions:

- (a) a specified user or an authorised individual of a specified user must not access or collect accessible health information about any individual except for a specified purpose mentioned in clause 19(2), or as otherwise required or permitted under the Bill;
- (b) an approved user or an authorised individual of an approved user must not —
  - (i) access or collect any type of accessible health information that is not specified in the notification published in respect of that approved user under clause 20(2); or
  - (ii) access or collect accessible health information about any individual except for a purpose specified in that notification, or as otherwise required or permitted under the Bill; and
- (c) a user or an authorised individual of a user must not access or collect accessible health information about any individual in a manner that is contrary to any access restriction imposed in respect of that accessible health information that is in force and where the access or collection is not otherwise permitted under clause 30(3), (4) or (5).

A person who contravenes clause 38 commits an offence. A person who contravenes the clause by accessing or collecting accessible health information

about any individual for an excluded purpose faces enhanced punishment upon conviction. The excluded purposes for the purposes of clause 38 are the same as those that apply in relation to clause 19.

Clause 39 makes it an offence for a person who is not a user or an authorised individual of a user to access or collect accessible health information about any individual for any purpose, unless the access or collection is required or permitted under the Bill or another written law, or by an order of court. Such access or collection is not considered to be required or permitted under any written law merely because the individual has consented or has given his or her consent in accordance with Part 4 of the PDPA, or such consent is not required under Part 4 of the PDPA.

Clause 40 makes it an offence —

- (a) for a user or an authorised individual of a user to disclose accessible health information about any individual, or any document that reproduces (fully or substantially) accessible health information about any individual, to any other person except in specified circumstances; and
- (b) for a person who is not a user or an authorised individual of a user to disclose accessible health information about any individual, or any document that reproduces (fully or substantially) accessible health information about any individual, unless the disclosure is required or permitted under the Bill or another written law, or by an order of court.

For the purposes of clause 40, disclosure of accessible health information about an individual is not considered to be required or permitted under any written law merely because the individual has consented or has given his or her consent in accordance with Part 4 of the PDPA, or such consent is not required under Part 4 of the PDPA. The clause also sets out a defence for the accused to prove, on a balance of probabilities, that the accused did not know, and had no reason to believe, that the accused had disclosed accessible health information or a document reproducing accessible health information.

Clause 41 makes it an offence for a requestor or an authorised individual of a requestor to disclose or use derived information in contravention of clause 27. It is also an offence for a requestor who obtains type 2 derived information, or an authorised individual of any such requestor, to do any act or take any step to identify or cause the identification of any individual from the type 2 derived information.

Clause 42 makes it an offence for any such person who is not a requestor —

- (a) to access, collect, disclose or use any information that the person knows or has reason to believe is derived information; or

- (b) to do any act or take any step to identify or cause the identification of any individual from aggregated or anonymised health information, where the person knows or has reason to believe that the aggregated or anonymised health information in question is type 2 derived information.

Division 8 of Part 2 sets out miscellaneous provisions for the purposes of the Part.

Clause 43 applies to a person (*X*) who is not a user or an authorised individual of a user. The Minister may, by written notice, direct *X* to stop accessing or collecting accessible health information about any individual and delete or destroy all copies of any such accessible health information that is in the possession or under the control of *X*, if —

- (a) the Minister has reason to believe that *X* is contravening or has contravened clause 39(1), and it is necessary for *X* to take any such action in order to prevent or minimise any harm or damage to any individual pending the outcome of any proceedings against *X* for an offence arising from that contravention; or
- (b) *X* is convicted of an offence arising from a contravention of clause 39(1).

The Minister may also direct *X* to delete or destroy all copies of accessible health information about any individual that is in the possession or under the control of *X*, if the Minister has reason to believe that *X*'s possession or control of the accessible health information is not required or permitted under the Bill or another written law, or by an order of court.

*X* commits an offence if *X*, without reasonable excuse, fails to comply with the Minister's direction under clause 43. The possession or control of accessible health information about an individual is not considered to be required or permitted under any written law merely because the individual has consented or has given his or her consent in accordance with Part 4 of the PDPA, or such consent is not required under Part 4 of the PDPA.

Clause 44 sets out transitional provisions relating to existing contracts or agreements entered into between a person and the Government under the current governance framework for the national electronic records system, under which the person —

- (a) contributes or agrees to contribute health information about any individual to the national electronic records system; or
- (b) is allowed to access and collect health information about any individual that is made available on the national electronic records system. The transitional provisions also allow the continued retention

and use of any such health information that was so accessed and collected.

### PART 3

#### SHARING OF RELEVANT INFORMATION FOR SPECIFIED USE CASES

Part 3 (clauses 45 to 60) provides a statutory framework for the sharing of relevant information about individuals in relation to specified use cases.

Clause 45 sets out definitions for the purposes of Part 3, including the key definitions of “data request”, “data sharing agreement”, “discloser” and “recipient”.

Clause 46 sets out the definition of “relevant information” for the purposes of Part 3.

Clause 47 sets out the definition of “use case” for the purposes of Part 3.

Clause 48 provides that —

- (a) Part 3 does not apply to the disclosure, collection and use of accessible health information about any individual;
- (b) Part 3 does not prevent or restrict the disclosure, collection or use of relevant information about any individual in accordance with any other provision of the Bill or any other written law or rule of law or by an order of court;
- (c) a person is not to be taken to be a discloser or recipient on the basis that the person is a contributor, user or requestor under the Bill; and
- (d) nothing in Part 3 imposes an obligation on a discloser to collect any relevant information for the purpose of enabling the discloser to disclose that information to any recipient under this Part.

Clause 49 provides that a discloser or recipient who does anything under Part 3 through a health data intermediary has the same obligations under the Part as one who acted directly.

Clause 50 provides that despite any other written law or rule of law or any obligation of confidentiality imposed by contract, the consent of an individual (*P*) is not required for —

- (a) the disclosure by a discloser of relevant information about *P* to a recipient;
- (b) the recipient’s collection of relevant information about *P* disclosed by the discloser; and

(c) the recipient's use of such relevant information,

where the disclosure, collection or use is in accordance with Part 3.

Clause 51 sets out, in relation to a use case —

- (a) when a discloser may disclose relevant information about an individual to a recipient; and
- (b) when the recipient may collect the relevant information from the discloser, and use that relevant information.

Clause 52 provides that a person or public agency who intends to disclose, and a person or public agency who intends to collect and use, relevant information about any individual in relation to a use case must enter into an agreement (data sharing agreement) that satisfies the requirements set out in the clause. These persons or public agencies must enter into the data sharing agreement before the discloser discloses any relevant information to the recipient. The type or types of relevant information about any individual that may be disclosed, collected and used must be specified in the data sharing agreement. They must be no more than the minimum necessary to implement or facilitate the use case in question. An agreement that does not satisfy the requirements in this clause is not considered a data sharing agreement for the purposes of Part 3.

Clause 53 sets out a discloser's obligations. The discloser may, in relation to a use case, disclose relevant information about an individual to a recipient only if —

- (a) the recipient makes a data request to the discloser pursuant to a data sharing agreement that relates to that use case;
- (b) the purpose for which the recipient makes the data request comes within the scope of that use case; and
- (c) at the time the discloser discloses the relevant information to the recipient in response to the recipient's data request, the data sharing agreement in question is in force.

Further, the discloser must —

- (a) ensure, before disclosing the relevant information to the recipient, that every type of relevant information to be disclosed is a type that is specified in the data sharing agreement;
- (b) ensure that the relevant information —
  - (i) is disclosed only by a personnel of the discloser, or of a health data intermediary of the discloser, who is specified in the data sharing agreement; and

- (ii) is disclosed only to a personnel of the recipient, or of a health data intermediary of the recipient, who is specified in the data sharing agreement;
- (c) make reasonable efforts to ensure that the relevant information that is disclosed —
  - (i) is no more than the minimum that is necessary to implement or facilitate the use case in question; and
  - (ii) is accurate and complete; and
- (d) make reasonable efforts to ensure that the relevant information is disclosed in a manner consistent with the data sharing agreement.

Clause 54 sets out a recipient's obligations. The recipient must not, in relation to a use case, make a data request to a discloser for the disclosure of relevant information about any individual unless —

- (a) the data request is pursuant to a data sharing agreement between the recipient and the discloser;
- (b) the purpose for which the recipient makes the data request comes within the scope of the use case in question; and
- (c) the recipient, having regard to all the circumstances of the case, genuinely requires the relevant information for the purpose for which the data request is made.

In relation to a data request, the recipient may disclose to the discloser any information about any individual to whom the data request relates if the disclosure of that information is necessary to identify the individual concerned, or to substantiate, or explain or elaborate on the purpose or scope of, the data request. However, the information that the recipient discloses must be no more than the minimum that is relevant to, and is necessary for, either of those purposes.

Clause 55 provides that a recipient that collects, in relation to a use case, relevant information about any individual that is disclosed by a discloser pursuant to a data sharing agreement must ensure that the relevant information is collected only by a personnel of the recipient, or of a health data intermediary of the recipient, who is specified in the data sharing agreement between the recipient and the discloser. The recipient must also make reasonable efforts to ensure that the relevant information is collected in a manner consistent with the data sharing agreement.

Under clause 56 —

- (a) a recipient, a health data intermediary of a recipient or any personnel of the recipient or the recipient's health data intermediary must not use relevant information about any individual collected from a discloser

pursuant to a data sharing agreement, except to implement or facilitate a use case specified in that data sharing agreement;

- (b) a health data intermediary of a recipient or any personnel of any such health data intermediary may process relevant information about any individual for the purpose of enabling or facilitating the recipient's use of that relevant information; and
- (c) the recipient must ensure that relevant information about any individual is made available to any personnel of the recipient or the recipient's health data intermediary only to the extent that is necessary to enable the personnel or health data intermediary to carry out any function or perform any duty relating to the implementation or facilitation of the use case in question.

Clause 57 provides that a recipient who collects, in relation to a use case, relevant information about any individual that is disclosed by a discloser pursuant to a data sharing agreement must not disclose that relevant information to any other person, unless —

- (a) the disclosure is required or permitted by or under the Bill or another written law, or by an order of court; or
- (b) the relevant information is disclosed to any person and in any circumstances that may be prescribed.

The disclosure of relevant information about an individual is not considered to be required or permitted under any written law merely because the individual has consented or has given his or her consent in accordance with Part 4 of the PDPA, or such consent is not required under Part 4 of the PDPA.

Clause 58 provides that the Minister may, by regulations, require —

- (a) a discloser to provide a copy of any data sharing agreement between the discloser and any recipient, or any document or information about any such data sharing agreement that may be prescribed; or
- (b) a recipient to provide a copy of any data sharing agreement between the recipient and any discloser, or any document or information about any such data sharing agreement that may be prescribed.

The discloser or recipient must provide the copy of the data sharing agreement, or document or information, within the prescribed time and in the form or manner prescribed, if any. Non-compliance with any such requirement is an offence.

Clause 59 empowers the Minister to issue directions to a discloser or recipient if the Minister has reason to believe that —

- (a) relevant information about any individual has been disclosed or purportedly disclosed by a discloser, or collected or used or

purportedly collected or used by a recipient, pursuant to a data sharing agreement between the discloser and recipient; and

- (b) the disclosure, collection or use of that relevant information is not in accordance with that data sharing agreement or the provisions of Part 3.

The Minister's direction may require the discloser or recipient to take any one or more of the following actions:

- (a) review and assess whether the disclosure or purported disclosure, or the collection or use or purported collection or use, of the relevant information is in accordance with the data sharing agreement between the discloser and recipient and the provisions of Part 3;
- (b) identify any error, failure, inadequacy or shortcoming relating to the disclosure or purported disclosure, or collection or use or purported collection or use, of the relevant information, and take reasonable steps to remedy and prevent the recurrence of the error, failure, inadequacy or shortcoming;
- (c) provide to the Minister any document or information that the Minister may reasonably require relating to any of those matters;
- (d) take any other action in relation to any of those matters that the Minister may reasonably require.

The Minister may additionally direct a recipient to take all reasonable steps to assist a discloser where the Minister is of the opinion that the recipient's assistance is required or desirable to enable the discloser to properly and effectively carry out any action mentioned in clause 59(2)(a)(i) or (ii) that the Minister directs the discloser to take. Similarly, the Minister may direct a discloser to take all reasonable steps to assist a recipient where the Minister is of the opinion that the discloser's assistance is required or desirable to enable the recipient to properly and effectively carry out any action that the Minister directs the recipient to take.

Further, under clause 59, the Minister may direct a discloser to stop disclosing relevant information about any individual to any recipient, or take any other specified action which the Minister reasonably considers to be necessary to bring a contravention to an end and prevents its recurrence, if —

- (a) the Minister has reason to believe that the discloser has contravened clause 52(2) or 53(1), (2) or (3), or any condition or restriction imposed under clause 53(4), and it is necessary for the discloser to take any such action in order to prevent or minimise any harm or damage to any individual pending the outcome of any proceedings against the discloser for an offence arising from that contravention; or
- (b) the discloser is convicted of an offence under clause 60(1).

Similarly, if —

- (a) the Minister has reason to believe that the recipient has contravened clause 52(2), 54(1) or (3), 55(1), 56(2) or (4) or 57(1), or any condition or restriction imposed under clause 54(5) or 56(5), and it is necessary for the recipient to take a certain action in order to prevent or minimise any harm or damage to any individual pending the outcome of any proceedings against the recipient for an offence arising from that contravention; or
- (b) the recipient is convicted of an offence under clause 60(2),

the Minister may direct a recipient —

- (c) to stop collecting relevant information about any individual collected from any discloser, or stop using relevant information about any individual collected from any discloser that is in the possession or under the control of the recipient;
- (d) to delete or destroy relevant information about any individual collected from any discloser;
- (e) to take all reasonable steps —
  - (i) to retrieve all copies of relevant information about any individual from any person to whom the recipient has disclosed the relevant information; and
  - (ii) to delete or destroy all copies of the relevant information that are retrieved; or
- (f) to take any other specified action which the Minister reasonably considers to be necessary to bring the contravention to an end and prevents its recurrence.

A person who, without reasonable excuse, refuses or fails to comply with the Minister's direction under clause 59 commits an offence.

Under clause 60, it is an offence for —

- (a) any person, without reasonable excuse, to contravene clause 52(2) or 53(1), (2) or (3), or any condition or restriction imposed under clause 53(4); or
- (b) any person, without reasonable excuse, to contravene clause 52(2), 54(1) or (3), 55(1), 56(2) or (4) or 57(1), or any condition or restriction imposed under clause 54(5) or 56(5).

## PART 4

SECURITY OF HEALTH INFORMATION AND  
RELEVANT INFORMATION

Part 4 (clauses 61 to 71) provides for data security and cybersecurity obligations to ensure the security of health information and relevant information.

Division 1 of Part 4 sets out provisions of general application for the purposes of Part 4.

Clause 61 sets out definitions for the purposes of Part 4, including the key definition of “cybersecurity incident”.

Clause 62 defines “data breach” for the purposes of Part 4.

Clause 63 defines “relevant computer or computer system” for the purposes of Part 4.

Clause 64 provides that except as otherwise provided, Part 4 applies to a contributor, user, requestor, System Operator, discloser or recipient under the Bill (relevant person). Further, Part 4 applies equally to and in relation to health information processed by a relevant HDI on behalf of and for the purposes of a contributor or user and health information processed by a contributor or user directly.

Under clause 65, a relevant person must designate one or more individuals to be responsible for ensuring that the relevant person complies with Parts 4 and 5. The designation of any such individual does not relieve the relevant person of the relevant person’s obligations under those Parts.

Division 2 of Part 4 sets out data security requirements in respect of health information and relevant information.

Clause 66 provides that a relevant person must —

- (a) implement reasonable controls to ensure the secure processing of health information or relevant information;
- (b) implement reasonable safeguards to protect against the unauthorised access, collection, use, disclosure, copying, modification, disposal, destruction or loss of health information or relevant information; and
- (c) ensure that every personnel who accesses or handles health information or relevant information is aware of his or her role and responsibility in ensuring that —
  - (i) the confidentiality and integrity of the information is protected; and
  - (ii) the information is available for use by the relevant person (including individuals employed or engaged by the relevant

person who are authorised to access or handle that information) in the ordinary course of the relevant person's activities.

A relevant person who contravenes any of these requirements commits an offence.

Clause 66 also sets out —

- (a) a relevant person's obligations in relation to health information or relevant information that is in the form of or part of an extract or a compilation of de-identified or aggregated information; and
- (b) where health information is processed by a relevant HDI of a contributor or user, the obligations of the relevant HDI and the contributor or user.

A person who contravenes any such obligation commits an offence.

Clause 67 provides that a relevant person —

- (a) must cease to retain any health information or relevant information, or remove the means by which the information can be associated with any particular individual, as soon as it is reasonable to assume that the purpose for which that information was collected is no longer being served by its retention, and retention of that information is no longer necessary for legal or business purposes; and
- (b) must take reasonable care, in relation to the disposal or destruction of any health information or relevant information, to prevent its unauthorised access, disclosure or reproduction.

Similar obligations apply to a relevant HDI of a contributor or user in respect of health information collected or processed on behalf of and for the purposes of the contributor or user.

A person who contravenes any obligation under clause 67 commits an offence.

Division 3 of Part 4 sets out cybersecurity requirements in relation to any relevant computer or computer system used by a relevant person to process health information or relevant information.

Clause 68 provides that the relevant person must implement reasonable safeguards, in relation to any such relevant computer or computer system —

- (a) to protect the confidentiality and integrity of health information or relevant information;
- (b) to ensure the availability of the health information or relevant information for use in the ordinary course of the relevant person's activities; and
- (c) to protect the relevant computer or computer system against unauthorised access, interference or tampering.

If health information is processed by a relevant HDI of a contributor or user, the relevant HDI must similarly implement reasonable safeguards and comply with any requirements prescribed in respect of those safeguards. The contributor or user must ensure that the relevant HDI implements the safeguards.

A person who contravenes any obligation under clause 68 commits an offence.

Division 4 of Part 4 sets out further obligations relating to data security and cybersecurity.

Clause 69 provides that a relevant person must —

- (a) establish and implement appropriate policies and practices in respect of the matters mentioned in clauses 66(1), (3) and (4)(b), 67(1) and 68(1) and (2)(b);
- (b) implement processes to ensure that every personnel of the relevant person adheres to those policies and practices; and
- (c) at the prescribed frequency, review and evaluate those policies and practices to ensure their effectiveness.

Additionally, a contributor or user must implement processes to ensure that any relevant HDI and every personnel of the relevant HDI adheres to the policies and practices established by the contributor or user, as the case may be.

A person who contravenes the obligations under the clause commits an offence.

Clause 70 provides that a relevant person must establish and implement an incident management framework that provides for —

- (a) mechanisms and processes to detect and respond to any cybersecurity incident or data breach; and
- (b) processes to identify and resolve the cause or causes of any cybersecurity incident or data breach, and prevent its recurrence or the occurrence of a similar cybersecurity incident or data breach.

The relevant person must ensure that the incident management framework provides for any matter relating to those mechanisms and processes that may be prescribed. A person who contravenes any obligation under clause 70 commits an offence.

Clause 71 provides that the Minister may direct a relevant person or a relevant HDI of a contributor or user to take any specified action in the direction to bring a contravention of any provision or requirement of Part 4 specified in the clause to an end and prevent its recurrence. A person who, without reasonable excuse, refuses or fails to comply with the Minister's direction commits an offence.

## PART 5

NOTIFICATION OF CYBERSECURITY INCIDENTS  
AND DATA BREACHES

Part 5 (clauses 72 to 82) sets out obligations in respect of —

- (a) the assessment of cybersecurity incidents affecting any relevant computer or computer system used by a relevant person to process health information or relevant information and the notification of the Minister of notifiable cybersecurity incidents; and
- (b) the assessment of data breaches affecting health information or relevant information and the notification of the Minister of notifiable data breaches.

Division 1 of Part 5 sets out provisions of general application for the purposes of the Part.

Clause 72 sets out definitions for the purposes of Part 5, including the key definition of “notifiable cybersecurity incident”.

Clause 73 provides that Part 5 applies in relation to any cybersecurity incident or data breach that affects the national electronic records system or any relevant computer or computer system used by the relevant person to process health information or relevant information.

Division 2 of Part 5 pertains to the assessment of cybersecurity incidents affecting any relevant computer or computer system used by a relevant person to process health information or relevant information, and the notification of notifiable cybersecurity incidents.

Clause 74 provides that where a relevant person has reason to believe that a cybersecurity incident in respect of the national electronic records system or any relevant computer or computer system used by the relevant person to process health information or relevant information has occurred, the relevant person must conduct, in a reasonable and expeditious manner, an assessment of whether the cybersecurity incident is a notifiable cybersecurity incident.

Further, where a relevant HDI of a contributor or user has reason to believe that a cybersecurity incident has occurred in respect of any relevant computer or computer system used by the relevant HDI to process health information on behalf of and for the purposes of the contributor or user —

- (a) the relevant HDI must, without undue delay, notify the contributor or user; and

- (b) the contributor or user must, upon notification by the relevant HDI, conduct an assessment of whether the cybersecurity incident is a notifiable cybersecurity incident.

The relevant person must carry out the assessment under clause 74 in accordance with the prescribed requirements, if any.

Clause 75 applies where a relevant person assesses, in accordance with clause 74, that a cybersecurity incident is a notifiable cybersecurity incident. The relevant person must notify the Minister as soon as is practicable, but in any case no later than the expiry of the prescribed period after the day the relevant person makes that assessment. The notification by the relevant person under clause 75 must contain all information that is prescribed for the purpose, to the best of the relevant person's knowledge and belief at the time the relevant person notifies the Minister. It must also be made in the form and submitted in the manner required by the Minister.

The relevant person is not, by reason only of notifying the Minister, to be regarded as being in breach of any duty or obligation under any written law, rule of law or contract as to secrecy or other restriction on the disclosure of information, or any rule of professional conduct or ethics applicable to the relevant person. The obligation under clause 75 applies concurrently with any other obligation of the relevant person under Part 5, or any obligation of the relevant person under any other written law to notify any other person (including the Government or any public authority) of the occurrence of a cybersecurity incident, or to provide any information relating to a cybersecurity incident.

Division 3 of Part 5 pertains to the assessment of data breaches and the notification of notifiable data breaches.

Clause 76 defines “affected individual” for the purposes of Division 3.

Clause 77 defines “notifiable data breach” for the purposes of Division 3. A notifiable data breach is a data breach in relation to health information or relevant information that —

- (a) results in, or is likely to result in, significant harm to an affected individual; or
- (b) is, or is likely to be, of a significant scale.

Under clause 78, a relevant person that has reason to believe that a data breach affecting health information or relevant information in the possession or under the control of the relevant person has occurred must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a notifiable data breach.

Where a relevant HDI of a contributor or user (other than a relevant HDI mentioned in clause 81) has reason to believe that a data breach has occurred in

relation to health information that the relevant HDI is processing on behalf of and for the purposes of the contributor or user, as the case may be —

- (a) the relevant HDI must, without undue delay, notify the contributor or user of the occurrence of the data breach; and
- (b) the contributor or user must, upon notification by the relevant HDI, conduct an assessment of whether the data breach is a notifiable data breach.

The relevant person must carry out the assessment under clause 78 in accordance with any prescribed requirements.

Clause 79 applies where a relevant person assesses, in accordance with clause 78, that a data breach is a notifiable data breach. The relevant person must notify the Minister as soon as is practicable, but in any case no later than the expiry of the prescribed period after the day the relevant person makes that assessment. The notification by the relevant person must contain all information that is prescribed for the purpose, to the best of the relevant person's knowledge and belief at the time the relevant person notifies the Minister. It must be made in the form and submitted in the manner required by the Minister.

The relevant person is not, by reason only of notifying the Minister under clause 79, to be regarded as being in breach of any duty or obligation under any written law, rule of law or contract as to secrecy or other restriction on the disclosure of information, or any rule of professional conduct or ethics applicable to the relevant person. The obligation under clause 79 applies concurrently with any other obligation of the relevant person under Part 5, or any obligation of the relevant person under any other written law to notify any other person (including the Government or any public authority) of the occurrence of a data breach, or to provide any information relating to a data breach.

Under clause 80, a relevant person must, on or after notifying the Minister under clause 79(1), notify each individual affected by a notifiable data breach mentioned in clause 77(1)(a) in any manner that is reasonable in the circumstances. The notification must contain, to the best of the relevant person's knowledge and belief at the time the relevant person notifies the affected individual, all the information that is prescribed for this purpose.

The relevant person is not, by reason only of notifying the affected individual, to be regarded as being in breach of any duty or obligation under any written law, rule of law or contract as to secrecy or other restriction on the disclosure of information, or any rule of professional conduct or ethics applicable to the relevant person. However, the obligation to notify the affected individual does not apply in certain circumstances specified in clause 80.

Clause 81 provides that where a relevant HDI of a contributor or user that is a public agency has reason to believe that a data breach has occurred in relation to

health information that the relevant HDI processes on behalf of and for the purposes of the public agency, the relevant HDI must, without undue delay, notify the public agency.

Division 4 of Part 5 sets out offences under the Part.

Clause 82 provides that a person who contravenes any of the specified provisions of Part 5 commits an offence.

## PART 6

### RESPONSES TO THREATS AND INCIDENTS AFFECTING HEALTH INFORMATION AND RELEVANT INFORMATION

Part 6 (clauses 83, 84 and 85) pertains to measures that must be taken in response to threats and incidents that affect health information and relevant information.

Clause 83 provides that Part 6 applies to a contributor, user, System Operator, discloser or recipient. Part 6 does not affect the operation of the Cybersecurity Act 2018 in relation to a cybersecurity incident or cybersecurity threat as defined in that Act.

Clause 84 empowers the Minister to authorise or direct any person mentioned in clause 83(1) to take emergency measures and comply with the necessary requirements on the occurrence or likely occurrence of certain critical events.

Clause 85 allows the Minister to delegate to any of the specified office-holders the exercise of the Minister's powers under clause 84.

## PART 7

### PORTABILITY OF HEALTH INFORMATION IN ELECTRONIC FORM

Part 7 (clauses 86, 87 and 88) seeks to ensure that health information in electronic form that is processed by a relevant HDI of a contributor or user remains accessible to the contributor or user if the contributor or user decides to engage a different relevant HDI to process the health information or to process the health information itself.

Clause 86 provides that Part 7 applies to a relevant HDI of a contributor or user in respect of health information in electronic form that the relevant HDI processes on behalf of and for the purposes of the contributor or user, as the case may be.

Under clause 87 —

- (a) the relevant HDI must establish and implement practices and processes in respect of the transfer, at the request of the contributor or user, of

health information in electronic form to the contributor or user, or another relevant HDI designated by the contributor or user, as the case may be. Those practices and processes must ensure that the health information that is transferred is accurate and complete, and that the health information is transferred in a timely manner; and

- (b) where the contributor or user requests the transfer of such health information, the relevant HDI must ensure that the health information is transferred in accordance with those practices and processes.

Clause 88 empowers the Minister to direct the relevant HDI to take any of the following actions if the Minister has reason to believe that the relevant HDI has contravened its obligations under Part 7:

- (a) review the practices and processes established and implemented;
- (b) review whether any transfer of health information by the relevant HDI is in accordance with its practices and processes and the provisions of Part 7;
- (c) identify any error, failure, inadequacy or shortcoming relating to its practices and processes or the transfer of health information, and take reasonable steps to remedy and prevent the recurrence of the error, failure, inadequacy or shortcoming;
- (d) take any other action that the Minister may reasonably require.

A person who, without reasonable excuse, refuses or fails to comply with the Minister's direction commits an offence.

## PART 8

### ADMINISTRATION AND ENFORCEMENT

Part 8 (clauses 89 to 97) sets out provisions relating to the administration and enforcement of the Bill.

Clause 89 empowers the Minister to appoint authorised officers and investigation officers to exercise the respective enforcement powers conferred on such officers under Part 8, and to appoint authorised officers for the purpose of directing a System Operator to take actions under Division 6 of Part 8. An authorised officer may be a public officer, an officer of a public authority or any other individual who is suitably qualified. An investigation officer may be a public officer or an officer of a public authority. Also, the Minister may delegate the exercise of the powers conferred or duties imposed on the Minister under the Bill (except certain specified powers and duties) to a public officer or an officer of a public authority.

Clause 90 empowers the Minister to issue codes of practice, or approve as a code of practice any document prepared by another person that the Minister considers suitable for this purpose, that relate to the matters specified in the clause. The Minister may also amend or revoke any such code of practice issued or approved. Codes of practice do not have legislative effect.

Clause 91 deals with the powers of authorised officers to obtain information and documents.

Clause 92 deals with the powers of investigation officers to obtain information and documents.

Clause 93 deals with the powers of authorised officers to enter into and inspect premises or conveyances.

Clause 94 deals with the powers of investigation officers to enter into and inspect premises or conveyances, and of search and seizure. An investigation officer is also empowered to require any person to provide information within the person's knowledge, or produce any book, document, record, electronic material, article or thing in the person's possession for the investigation officer's inspection and making of copies, or provide the investigation officer with copies.

Clauses 95 and 96 criminalise various acts in support of the powers of enforcement under this Part.

Clause 97 deals with the disposal of any thing or document produced, detained or seized under the Bill.

## PART 9

### MISCELLANEOUS

Part 9 (clauses 98 to 114) sets out miscellaneous provisions.

Clause 98 provides for legal protections for a contributor or an authorised individual of a contributor in relation to the contribution of health information about any individual in accordance with the Bill.

Clause 99 provides for legal protections for a user or an authorised individual of a user in relation to the access, collection and disclosure of accessible health information about any individual in accordance with the Bill.

Clause 100 provides for legal protections for a requestor or an authorised individual of a requestor in relation to the access, collection, disclosure or use of derived information in accordance with the Bill.

Clause 101 provides for legal protections for a System Operator in relation to the processing of health information for the purposes of Part 2, and the operation, administration and maintenance of the national electronic records system, in accordance with the Bill, among other protections.

Clause 102 provides for legal protections for a discloser or an authorised personnel of a discloser in relation to the disclosure of relevant information about any individual in accordance with the Bill.

Clause 103 provides for legal protections for a recipient or an authorised personnel of a recipient in relation to the collection or use of relevant information about any individual in accordance with the Bill.

Clause 104 provides that no personal liability lies personally against an authorised officer or an investigation officer, who, acting in good faith and with reasonable care, does or omits to do anything in the execution or purported execution of the Bill.

Clauses 105 and 106 are standard provisions concerning corporate criminal liability.

Clause 107 deals with the service of documents permitted or required by the Bill to be served on a person. The clause does not deal with service of court documents like summonses.

Clause 108 confers on a District Court jurisdiction to try any offence under the Bill and to punish accordingly despite any limits set under the Criminal Procedure Code 2010.

Clause 109 allows the Minister to compound any offence under the Bill that is prescribed as a compoundable offence.

Clause 110 confers on the Minister the power to exempt any person or class of persons or any health information or type of health information from the provisions of the Bill.

Clause 111 allows the Minister to amend any Schedule to the Bill by order in the *Gazette*, and to make any saving and transitional provisions that may be necessary or expedient.

Clause 112 allows for regulations to be made for carrying out or giving effect to the Bill.

Clause 113 makes a related amendment relating to the disclosure of information under section 28 of the Human Organ Transplant Act 1987.

Clause 114 empowers the Minister to prescribe additional provisions of a saving or transitional nature consequent on the coming into force of different clauses in the Bill that the Minister considers necessary or expedient. The additional saving or transitional provisions may be made by regulations only within 2 years after the date of commencement of the provisions in question.

The First Schedule sets out the specified contributors required to contribute health information about any individual under clause 12 and the types of health information they are required to contribute.

The Second Schedule sets out the specified users, and the authorised individuals of those specified users, that may access and collect accessible health information about any individual under clause 19.

The Third Schedule sets out the specified examinations for the purposes of clause 19(3).

The Fourth Schedule sets out, in relation to the sharing of relevant information under Part 3, the disclosers and recipients who may share such information and the use cases for which they may do so.

## EXPENDITURE OF PUBLIC MONEY

This Bill will involve the Government in extra financial expenditure, the exact amount of which cannot at present be ascertained.

---