MINISTRY OF HEALTH
SINGAPORE

CYBERSECURITY AND DATA SECURITY ESSENTIALS

Date of Publication: 03-2026 (First edition)

Security measures for the proper storage, access, use, and sharing of health information.

In consultation with:

CSA SINGAPORE

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

Please email HIA Enquiries for further clarification on the Essentials. For more information on the Health Information Act, please visit the MOH HIA website.

1. Introduction

1.1 The Ministry of Health (MOH) has introduced the Health Information Act (HIA) to govern the safe and secure collection, access, use and sharing of health information to enhance quality and continuity of care for patients.

1.2 This document sets out new Cybersecurity and Data Security (CS/DS) guidelines, known as the CS/DS Essentials, to provide guidance on the security measures to be put in place for proper storage, access, use and sharing of health information[1]. This document is developed by MOH in consultation with the Cyber Security Agency of Singapore (CSA), Infocomm Media Development Authority (IMDA) and Personal Data Protection Commission (PDPC).

Who Do the CS/DS Essentials Apply To

1.3 The CS/DS Essentials apply to entities within the scope of the HIA, or "HIA entitles". They are:

1.3.1 all licensees under the Healthcare Services Act (HCSA);

1.3.2 all contributors and users of the National Health Electronic Record (NEHR); and

1.3.3 prescribed entities that are enabled to share health information under the HIA.

Scope of Information Covered under CS/DS Essentials

1.4 Health information refers to administrative and clinical information, including information that may be prescribed under the HIA for sharing in relation to specified use cases. HIA entities must identify the range of health information that they own and access (e.g. medical records, laboratory test results) and implement appropriate safeguards for this information.

[1] Information on other aspects of the HIA is set out separately at MOH HIA website.

Summary of the CS/DS Essentials

1.5 The CS/DS Essentials are summarised in **Table 1**.

Table 1: Cybersecurity & Data Security Essentials

A. Cybersecurity (IT and Software-Related Measures)
1. Updates ☑ Install software updates on your devices and systems promptly.
2. Secure/Protect ☑ Use anti-malware and anti-virus solutions to protect against malicious software. ☑ Implement IT access control measures to control access to your data and services. ☑ Use secure settings for your organisation's procured hardware & software.
3. Backup ☑ Back up essential data and store them separately.
4. Asset ☑ Identify the hardware and software used in your organisation and secure them.
B. Data Security (Data-Related Practices)
5. Secure ☑ Identify the type of data your organisation has, where they are stored, and secure them. ☑ Reproduce health information only when necessary for a specified purpose. ☑ Transfer health information properly to avoid unwanted data exposure.
6. Identify ☑ Differentiate and mark your health information.
7. Access ☑ Restrict access to health information for valid and relevant purposes.
C. Common Cybersecurity & Data Security Practices (Personnel Training, Vendor Management and Organisation Protocols)
8. Training and education ☑ Equip personnel with cybersecurity and data security hygiene practices as the first line of defence.
9. Outsourcing and Vendor Management ☑ Understand the responsibilities set between your organisation and vendor.
10. Security Reviews and Internal Audit Measures ☑ Regular checks on corporate policies and processes to ensure compliance and identify gaps.
11. Disposal

☑ Proper disposal of health information reduces the risk of unauthorised access.
12. Emergency Planning for Contingency ☑ Supports ability to withstand service disruptions to ensure business continuity.
13. Incident Response ☑ Prepared to detect, respond, and recover from incidents.

Resources And Support

1.6 MOH has developed a guidebook, templates and self-help resources to help HIA entities implement the measures; these will be progressively issued over the course of 2026. These resources should help HIA entities implement the majority of the measures in these CS/DS Essentials, especially the corporate protocols, vendor management policies and personnel training measures.

1.7 On Category (A), MOH has worked with Health Information Management Systems (HIMS)[2] vendors to embed key controls into their systems, namely, timely software updates, use of two-factor authentication to change system configurations, implementation of security configurations, protecting against unauthorised access to backup data, and securing backup storage. Those that do so would be Cyber Essentials certified, or CE certified. Other systems and applications that contain health information (e.g. hardware and billing applications) used by HIA entities should also have the same security measures.

1.8 If necessary, HIA entities can also consider engaging services support[3] (e.g. CISO-as-a-service) to implement these measures.

[2] For example, vendors of Clinic Management Systems.

[3] Please refer to Business Grants Portal, CSA (CISO as-a-Service), IMDA (SMEs Go Digital)

A. Cybersecurity (IT and Software Measures)

Note: *All cybersecurity measures apply to computer and computer systems that are interconnected with NEHR or contain health information.*

* Implemented by Cyber Essentials (CE) certified HIMS vendors (implementation in other IT solutions is still required)

1. Update: Install software updates on your devices and systems promptly

A.1 When software updates for operating systems and applications become available from the software companies or other legitimate sources, HIA entities should prioritise critical or important ones.

2. Secure/Protect – Use anti-malware and anti-virus solutions to protect against malicious software

A.2 Anti-malware solutions should be used and installed in endpoints (e.g. laptops, desktops, servers) to detect attacks on the HIA entity's environment.

A.2.1 Anti-malware solutions should be configured to auto-update signature files or equivalent, to detect new malware.

A.2.2 Virus and malware scans should be carried out regularly to detect possible attacks.

A.2.3 Anti-malware solutions should be configured to automatically scan the files upon access. This includes files and attachments downloaded from the internet through the web browser or email, and external sources such as portable USB drives.

A.3 Firewalls should be configured and deployed to protect the network, systems, and endpoints and virtual environments. Depending on the organisation's network setup, the firewall functionality may be integrated with other networking devices or deployed as a standalone device.

In a simple organisation setup, comprising just endpoints connecting to the internet and/or cloud-based applications, firewalls that are built-in/included in operating systems (e.g. software firewall or host-based firewall), and firewalls integrated with the organisation's router or wireless access point, should be configured and deployed.

In a network setup, a network perimeter firewall (e.g. Domain Name System (DNS) firewall and application-level gateway firewall) should be configured and deployed to accept only authorised network traffic.

A.4 The HIA entity should put in place policies and processes to ensure that its employees:

A.4.1 Install or access only authorised software or attachments from official or trusted sources.

A.4.2 Use only trusted network connections (e.g. mobile hotspot, personal Wi-Fi, corporate Wi-Fi, and Virtual Private Network) to access the organisation's data or business email rather than publicly available network connections. The HIA entity should also educate employees of the risks of using publicly available network connections, which are highly accessible and vulnerable against cyber-attacks.

A.4.3 Are aware of the need to report any suspicious email or attachment to the IT team and / or senior management immediately.

Secure/Protect: Implement access control measures to control access to your data and services

A.5 The HIA entity should maintain and manage an inventory of user, administrator, third-party, and service accounts.

A.5.1 It should have minimally the following details for each account:

(a) Name;
(b) Username;
(c) Department;
(d) Role/Account Type;
(e) Date of access created; and
(f) Last log-on date

A.6 The HIA entity should ensure that each personnel is provided with unique user accounts.

A.6.1 Accounts with unnecessary or expired access rights should be disabled or removed from the system. Shared, duplicate, obsolete, dormant and inactive accounts (e.g. inactive for more than 60 days) should be removed. Disabled accounts that cannot be removed should have their access rights revoked.

A.6.2 The administrator account should only be accessed to perform administrator functions with approval from the senior management.

A.7 The HIA entity should have a process to grant and revoke access only when the appropriate approvals are granted.

A.7.1 Approval may be documented in different ways (e.g. email, through access request form).

A.7.2 Approvals for any change in access to devices or applications should be sought when there are personnel changes such as onboarding of new personnel or change of role for personnel.

A.7.3 Access should be managed to ensure that personnel can access only the information and systems required for their job role.

A.7.4 The following fields should be captured for personnel who are granted access to accounts:

(a) Name;
(b) System to access;
(c) Department;
(d) Role/Account type;
(e) From [date]; and
(f) To [date] (if applicable)

A.8 The HIA entity should ensure that all default passwords are replaced with a strong passphrase[4]. In setting passwords, publicly known information, or predictable character combinations should be avoided.

A.8.1 Account passwords should be changed in the event of any suspected compromise or lost tokens.

A.8.2 Two-factor authentication (2FA) should be used for administrative access (including remote access) to important systems, such as an internet-facing system containing sensitive or business-critical data (will be in-built in CE-certified HIMS).

A.8.3 User account should be disabled and/or locked out after multiple failed login attempts, e.g. after 10 failed login attempts.

A.9 Access should be managed to ensure third parties / contractors can access only the information and systems required for their job role. Such access should be removed once they no longer require them.

A.9.1 Third-party or contractors working with health information in the organisation should sign a Non-Disclosure Agreement (NDA) form.

[4] A strong passphrase should be at least 12 characters long and include upper case, lower case, and/or special characters. Avoid using common words, obvious patterns, or easily guessed information such as "password" or "qwerty".

A.10 The HIA entity should implement physical access controls to allow only authorised employees or contractors to access the HIA entity's IT assets and/or environment.

A.11 The HIA entity should maintain log-in rules (i.e. tracking of users logging[5] in and out of systems) properly and ensure that only authorised individuals have access to security logs.

Secure/Protect: Secure Configuration – Use secure settings for your organisation's procured hardware & software

A.12 Security configurations should be implemented for assets, including desktops, servers, and routers.

A.12.1 Insecure configurations and weak protocols should be replaced or upgraded before assets are used.

A.12.2 Features, services, or applications that are not in use should be disabled or removed.

A.12.3 Automatic connection to open networks and auto-run feature of non-essential programmes (other than backup or anti-malware solution etc.) should be disabled.

3. Back up: Back up essential data and store them separately

A.13 The HIA entity should identify business-critical systems and those containing essential business information and perform backup. What needs to be backed up should be based on what is needed for business recovery and continuity in the event of a cybersecurity incident.

A.13.1 The backups should be performed on a regular basis, with the backup frequency aligned to the business requirements.

A.13.2 All backups should be protected from unauthorised access and restricted to authorised personnel only.

A.13.3 Backups should be stored separately and isolated from the operating environment.

A.14 If the scope includes cloud environment, the HIA entity should:

A.14.1 Understand the role and responsibility between itself and the cloud service provider in terms of data backup; and

[5] Security and audit logs serve as records of who have accessed the IT network or systems and what operations they have performed. Having such logs is useful to establish baseline, identify suspicious trends, and critical for understanding the nature of security incidents (i.e. during an active investigation and postmortem analysis). If it is impossible to enable logging on all systems or devices, the HIA entity should also keep a manual log.

A.14.2 Ensure there are alternative forms of data backup being utilised to ensure business continuity.

4. Asset: Hardware & Software – Identify the hardware and software used in your organisation, and protect them

A.15 The HIA entity should develop a protocol to authorise new hardware and software into the organisation.

A.15.1 The date of authorisation of any software and hardware should be keyed into the asset inventory list after obtaining the relevant approvals.

A.15.2 Software and hardware without an approval date should be removed.

A.16 The HIA entity should maintain an up-to-date inventory of assets used in the organisation for all IT hardware and software.

A.17 Hardware and software assets that are unauthorised or have reached the End-of-Support (EOS) should be replaced. End-of-Support (EOS) refers to the point when a company ceases technical servicing for a product e.g. limited tech support, software updates, or repairs.

A.18 In the event of any continued use of EOS assets, the HIA entity should assess the risk, obtain approval from the senior management, and monitor its use until the asset is replaced.

B. Data Security (Data-Related Practices)

Note: *All data security measures are applicable to both electronic data (e.g. data in systems) and non-electronic data (e.g. data in hardcopy documents).*

5. Secure: Identify the types of data your organisation has, where they are stored, and secure them

B1 The HIA entity should establish policies and processes to identify and protect its health information. Specifically, it should implement policies and processes to prevent employees, third parties and contractors from disclosing or leaking confidential and/or sensitive data outside the organisation, by including clauses prohibiting unauthorised disclosure of information in employment contracts and contractual agreements with third parties or contractors.

B.2 The HIA entity should secure health information from unauthorised access or loss where stored within office premises[6], as follows:

B.2.1 Physical security measures should include storing hardcopy documents in access-controlled locations within the office, such as storing these documents in locked file cabinet systems.

B.2.2 Laptops and portable storage media devices containing health information should be locked and protected with a cable lock / attached to a fixture with a security cable when not in use[7].

B.3 The HIA entity should have policies and practices to protect hardcopy documents containing health information that are stored in commercial storage facilities (outside office premises).

B.3.1 The HIA entity should check that the commercial storage facilities have adequate security measures, by checking on the service provider's credibility and security policies.

B.3.2 The HIA entity should maintain proper records of materials containing health information deposited in offsite storage.

B.3.3 The HIA entity should conduct stock-takes and audits to ensure its documents are intact or in order, and have not been subject to unauthorised access.

B.4 The HIA entity should set retention periods[8] for health information to ensure that such information is kept only where there is a business or legal purpose to do so.

B.4.1 There should be a proper rationale in the retention policy for the duration for which the health information is retained.

B.4.2 The HIA entity should consider applicable legislation (e.g. PDPA[9]), contractual requirements (e.g. funding or data sharing agreements), and national standards or guidelines[10].

---

[6] See PDPC Advisory Guidelines on Key Concepts in the PDPA (Chapter 17 on the Protection Obligation).

[7] Please refer to PDPC's Data Protection Practices for ICT Systems.

[8] Please refer to the latest Licence Conditions (LCs) on the Retention Periods of Patient Health Records and FAQs for HCSA licensees, and note that these may be amended from time to time. For example, the LCs state that inpatient paper records of adults have to be retained for 15 years from the last day of (i) stay in the facility, or (ii) consultation of treatment (if applicable), whichever is later.

[9] An organisation shall cease to retain any personal data when there is no business or legal purpose to do so. The PDPA does not prescribe specific retention period for personal data, organisations need to comply with any legal or specific industry-standard requirements that may apply.

[10] See PDPC Data Protection Practices for ICT Systems, PDPC Guide to Printing Processes for Organisations, and PDPC Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data.

Secure: Reproduce health information only where necessary for an official purpose

B.5 The HIA entity should have policies and processes to ensure that copies of health information are only made by authorised parties on a need-to-know basis, and where necessary for an official purpose.

B.6 When making copies of health information using external devices (e.g. scanners, portable storage devices) or at external locations, the HIA entity should have policies and practices to ensure that its personnel maintain possession of all copies made (e.g. personnel of a HIA entity should not leave photocopied materials unattended at photocopiers outside the office premises).

Secure: Transfer health information properly to avoid unwanted data exposure

B.7 The HIA entity should have policies and practices to ensure that, when transferring any health information in public or transmitting electronically -

B.7.1 Its personnel only bring necessary health information out of the office, on a need-to-know basis and for appropriate work purposes;

B.7.2 Materials containing health information remain in its personnel's possession or control at all times (e.g. documents should not be left unattended);

B.7.3 Health information should be protected from accidental exposure (e.g. use privacy filters or position computers to limit visibility); and

B.7.4 Files containing health information are protected from any unauthorised access. Electronic transmissions of files, e.g. by email, should be password-protected (by setting strong passwords[11] and sending the password to the recipient to unlock the file through a different channel from the channel used to send the file) and sent to the right recipients (e.g. check the email addresses before sending).

6. Identify: Differentiate and mark your health information

B.8 The HIA entity should have policies and practices[12] for marking health information to enable its personnel to recognise and properly manage the health information they are handling, such as:

B.8.1 Having an organisation-wide policy requiring all documents containing health information to be manually or electronically labelled when they are

[11] Please refer to the CSA guidelines on how to set strong passwords.
[12] See PDPC Guide to Data Protection Practices for ICT Systems .

created (e.g. by inserting headers or footers in medical reports when they are created);

B.8.2 Where marking all documents and data is assessed to be impractical, the HIA entity should clearly specify in its corporate policy what data should be treated as health information (e.g. all information in medical reports) instead of marking the individual documents, and its personnel should comply with the corresponding security measures for health information.

B.9 The HIA entity should consider the following factors when assessing whether and how to mark its health information:

B.9.1 Format of the health information (e.g. hardcopy or in electronic format);

B.9.2 Practicality of marking (e.g. manual stamping of hard copies, cost of IT system enhancement if marking is done electronically);

B.9.3 Party/user that is handling the health information (e.g. personnel of HIA entity that handles health information on a day-to-day basis, or a third-party vendor managing or delivering documents containing health information on behalf of a HIA entity); and

B.9.4 Intent of the marking (i.e. to alert the recipient of the health information to protect the health information accordingly).

7. Access: Restrict access to health information for valid and relevant purposes

B.10 The HIA entity should have policies and processes to ensure that access to any health information is only granted to personnel who fulfil both the following conditions:

B.10.1 The personnel (includes any third parties[13] engaged by the HIA entity, which the health information has been shared with) has a legitimate need to know and access the individual's health information to carry out their work functions as determined by an appropriate authority within the HIA entity (e.g. a clinician is granted access rights to the HIA entity's EMR to access a patient's healthcare record to understand the patient's medical condition(s) and carry out appropriate patient care).

[13] Third parties should consult the HIA entity (that engaged them) when uncertain about data disclosure permissions, while the HIA entity should proactively establish and communicate clear restrictions for data requiring limited distribution. All third parties should protect health information from unauthorised disclosure by maintaining secure custody, implementing reasonable processing safeguards, and ensuring contractors do not unnecessarily access or retain health information. Additionally, third parties should use health information solely for its intended purpose and cannot disclose it to other organisations or parties for different purposes without explicit consent from the HIA entity, unless authorised by law.

B.10.2 The personnel has been informed or made aware of, and has acknowledged[14] the data protection and security measures in these CS/DS Essentials, relevant prevailing laws e.g. PDPA, the HIA entity's corporate policies and/or professional ethics/policies.

C. Common Cybersecurity and Data Security Measures Practices (Personnel Training, Vendor Management and Organisation Protocols)

8. Training and Education: Equip personnel with security hygiene practices as the first line of defence

C.1 The HIA entity should ensure its personnel attend cybersecurity and data security-related awareness training periodically (e.g. ideally, personnel should attend such training at least once annually) so that they are aware and kept up-to-date on the security measures and what their roles and responsibilities are.

C.1.1 The training may be conducted in-house or by external vendors; or conducted through self-help resources (e.g. official resources published by PDPC).

C.2 The HIA entity should develop cybersecurity and data security-related hygiene policies and practices for their personnel to adopt in their daily operations, to ensure that they are familiar with the security practices and behaviours expected of them.

9. Outsourcing and Vendor Management: Understand the responsibilities set between your organisation and vendor

C.3 If the HIA entity is using an IT service provider[15] to manage its network, systems, and medical devices, it should:

C.3.1 Clearly understand the services and security practices that the IT service provider will provide; and

C.3.2 Ask the IT service provider to provide regular vulnerability reports and updates about security issues for the systems they are managing on behalf of the HIA entity.

[14] Examples of acknowledgement include sending an email on data security with email recipients responding "I understand the data security measures", or records of attendance at briefing sessions.

[15] See PDPC Advisory Guidelines on Key Concepts in the PDPA (Chapter 6 on Organisations) for information on obligations of data intermediaries (e.g. vendors acting on behalf of a HIA entity), Guide to Managing Data Intermediaries.

C.4 When using third-party software and devices, the HIA entity should ensure that it understands:

C.4.1 Where health information[16] is stored (whether in Singapore or overseas);

C.4.2 The safeguards[17] that vendors have in place to secure the third-party software and devices they provide, including any audits and certifications carried out (e.g. CSA Cyber Essentials certification for HIMS, audits); and

C.4.3 Its contractual arrangements with vendors, including responsibilities of each contractual party in the event of an incident or breach.

C.5 If the HIA entity is using cloud services (e.g. Amazon Web Services, Google Drive)[18], they should ensure that they understand their responsibilities for setting security configurations.

10. Security Reviews and Internal Audit: Regular checks on corporate policies and processes to ensure compliance and identify gaps

C.6 The HIA entity should periodically review[19] its implementation of cybersecurity and data security safeguards for health information.

C.7 The HIA entity should conduct checks (e.g. self-assessments, or audits conducted by external auditors, as determined by the HIA entity's business or operational considerations) to review established corporate policies, its personnel's compliance with its corporate policies.

C.8 The HIA entity should take action in a timely manner, if it discovers any lapse in compliance (e.g. rectifying the lapses, conduct further training for personnel to prevent similar occurrences and strengthen security measures where necessary).

11. Disposal: Proper disposal of health information reduces the risk of unauthorised access

C.9 Before disposing any hardware asset or data, the HIA entity should ensure that all health information has been securely destroyed[20] (e.g. shredding physical

---

[16] See Personal Data Protection Act 2012: Section 26 Transfer of Personal Data Outside Singapore, Personal Data Protection Regulations 2021: Part 3 Transfer of Personal Data Outside Singapore, Advisory Guidelines on Key Concepts in the PDPA (Chapter 19 on Transfer Limitation Obligation).

[17] See PDPC Guide to Data Protection Practices for ICT Systems.

[18] See CSA Cloud Security for Organisations programme, PDPC Advisory Guidelines on Selected Topics (Chapter 9 on Cloud Services), PDPC Guide to Data Protection Practices for ICT Systems.

[19] See PDPC Guide on Data Protection Management Programme, PDPC Guide to Data Protection Impact Assessments

[20] See Sample Sanitisation/Secure Disposal Standards from National Institute of Standards and Technology (NIST), Guidelines for Media Sanitisation from NIST.

documents, encrypting hard disk before reformatting, and overwriting electronic data in a storage medium completely[21]).

12. Emergency Planning for Contingency: Supports ability to withstand service disruptions to ensure business continuity

C.10 The HIA entity should establish a business continuity plan to ensure organisational resilience (e.g. identifying critical assets that require high availability and putting in place redundancies) against the common business disruption scenarios, including those caused by cybersecurity incidents and data breaches, and execute it when needed.

13. Incident Response: Prepared to detect, respond, and recover from incidents

C.11 The HIA entity should establish an up-to-date basic incident response plan to guide the organisation on how to respond, manage and mitigate the impact of cybersecurity incidents (e.g. phishing and ransomware) or data breaches.

C.12 The plan should contain the following details:

C.12.1 Clear roles and responsibilities of key personnel in the HIA entity involved in the incident response process;

C.12.2 Procedures to detect, respond to, and recover from the common cybersecurity/data threat scenarios, e.g. phishing and ransomware; and

C.12.3 Communication plan and timeline to escalate and report the incident to internal and external stakeholders (such as regulators, customers, and senior management).

C.13 The incident response plan[22] should be made known to all employees in the organisation that have access to the organisation's IT assets and/or environment. All personnel should also be aware of how to report suspicious activity and possible incidents based on the obligations under prevailing legislative or regulatory requirements.

C.14 The incident reporting thresholds and timelines for cybersecurity incidents or data breaches under the HIA are summarised in **Table 2**. Specific details of how HIA entities can report the incidents to MOH will be shared shortly.

---

[21] See PDPC Guide to Data Protection Practices for ICT Systems.

[22] For more information on the key components and steps in an incident response plan, please refer to CSA's resource on Incident Response Checklist, CIS's sample on Incident Response Policy. MOH will also issue templates that HIA entities can adopt.

Table 2: Incident Reporting Thresholds & Timelines under the HIA

	Cybersecurity Incidents	Data Breaches
Reporting Thresholds	• A notifiable[23] cybersecurity incident involves: i. a computer or computer system containing health information or interconnected with a computer or computer system containing health information; and ii. The computer or computer systems are under the HIA entity's control.	• Aligned to PDPA's data breach notification threshold. • In the context of health information, a notifiable data breach is one that: i. results in, or is likely to result in, significant harm[24] to an affected individual; or ii. is, or is likely to be, of a significant scale (i.e. 500 or more affected individuals).
Reporting Requirements	• Initial notification to MOH within 2 hours after the HIA entity assesses that the incident is a notifiable cybersecurity incident or data breach meeting the reporting thresholds. • Affected HIA entity to provide an incident report within 14 days of initial notification. • The HIA entity must notify affected individuals at the same time, or as soon as practicable after notifying MOH, if the incident causes, or is likely to cause significant harm to an individual.	

END OF DOCUMENT

[23] Notifiable cybersecurity incidents include but are not limited to e.g. unauthorised hacking of computer or computer systems, installation or execution of unauthorised software or computer codes of malicious nature, attempts to prevent the availability of computer information or services to its intended users (i.e. denial of service attacks), attempts to intercept the traffic between two computer or computer systems to steal or alter information (i.e. man-in-the-middle attack), etc.

[24] For example, data breaches involving certain health information deemed to be more sensitive, such as those relating to sexually transmitted infections. Details of data breaches that would be deemed as being likely to result in significant harm will be set out in subsidiary legislation to be issued.