Annex C-HIA
(normative)

Cyber Essentials mark for Health Information Act (HIA) entities – Requirements

C-HIA.1 Introduction

With increasing digitalisation, cyber-attacks and data breaches have become key risks for organisations and enterprises. In healthcare, such risks are heightened given that security breaches related to health information can potentially impact patient safety and care quality, beyond patient privacy and confidentiality. Furthermore, such breaches are also extremely costly to organisations, e.g. to recover lost data and indirectly from reputational damage.

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

The HIA will require HIA entities to meet the **Cybersecurity and Data Security Essentials (CS/DS Essentials)**[1], and to put in place security measures for proper storage, access, use and sharing of health information.

C-HIA.2 Additional terms and definitions

For the purposes of this annex, the following terms and definitions apply.

C-HIA.2.1 Health information

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 shall 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.

C-HIA.2.2 Entities under the scope of HIA

Entities within the scope of HIA include:

- All licensees under the Healthcare Services Act (HCSA);
- All contributors and users of the National Health Electronic Record (NEHR); and
- Prescribed entities that are enabled to share health information under the HIA.

C-HIA.3 Cyber Essentials mark for HIA entities

C-HIA.3.1 Boundary of scope and statement of scope

The scope of assessment and certification shall cover at least the following:

[1] Cyber and Data Security Essentials (CS/DS Essentials) was developed by MOH, in consultation with the Cyber Security Agency of Singapore (CSA), the Infocomm Media Development Authority (IMDA) and the Personal Data Protection Commission (PDPC).

COPYRIGHT

- HIA entities' computer and computer systems that are interconnected with NEHR or contain health information.

- HIA entities' electronic data (e.g. data in systems) and non-electronic data (e.g. data in hardcopy documents).

The statement of scope shall minimally include cybersecurity and data security requirements defined in C-HIA.3.4 and/or C-HIA.3.5, unless otherwise stated.[2]

C-HIA.3.2 Pre-certification preparation by HIA entity

Prior to engaging a certification body, the HIA entity shall complete the guided self-assessment template required for Cyber Essentials mark certification for HIA entities.

This consists of a list of requirements and recommendations that the HIA entity shall assess and indicate if these have been implemented in the organisation.

C-HIA.3.3 Independent assessment by certification body

Following the completion of its self-assessment, the HIA entity shall approach any of the certification bodies appointed by CSA for independent assessment and issuance of the Cyber Essentials mark certification for HIA entities.

For the organisation to be certified for Cyber Essentials mark for HIA entities, the organisation shall meet all the requirements for full scope of assessment and certification.

C-HIA.3.4 Provisions for Cyber Essentials for HIA entities

Following shows the provisions for Cyber Essentials for HIA entities.

Clause	Provisions in Cyber Essentials	Additional provisions for HIA entity
A.1 Assets: People – Equip employees with know-how to be the first line of defence		
A.1.4 (a)	Requirement	Requirement (CS/DS Essentials C.1, C1.1) NOTE: – The training may be conducted in-house or by external vendors; or conducted through self-help resources (e.g. official resources published by PDPC).
A.1.4 (b)	Requirement	Requirement (CS/DS Essentials C.2) NOTE: – The HIA entity shall 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.
A.1.4 (c)	Recommendation	Recommendation
A.1.4 (d)	Recommendation	Recommendation
A.1.4 (e)	Recommendation	Recommendation
A.2 Assets: Hardware and software – Know what hardware and software the organisation has and protect them		

[2] Refers to the "*Cyber and Data Security Essentials*" published by MOH

COPYRIGHT

Clause	Provisions in Cyber Essentials	Additional provisions for HIA entity
A.2.4 (a)	Requirement	Requirement (CS/DS Essentials A.16)
A.2.4 (b)	Recommendation	Recommendation
A.2.4 (c)	Recommendation	Recommendation
A.2.4 (d)	Recommendation	Recommendation
A.2.4 (e)	Recommendation	Recommendation
A.2.4 (f)	Requirement	Requirement (CS/DS Essentials A.17)
A.2.4 (g)	Requirement	Requirement (CS/DS Essentials A.18)
A.2.4 (h)	Requirement	Requirement (CS/DS Essentials A.15)
A.2.4 (i)	Requirement	Requirement (CS/DS Essentials A.15.1)
A.2.4 (j)	Requirement	Requirement (CS/DS Essentials A.15.2)
A.2.4 (k)	Requirement	Requirement (CS/DS Essentials C.9) NOTE: – Before disposing any hardware asset or data, the HIA entity shall ensure that all health information has been securely destroyed[3] (e.g. shredding physical documents, encrypting hard disk before reformatting, and overwriting electronic data in a storage medium completely[4]).
A.2.4 (l)	Recommendation	Recommendation
A.3 Assets: Data – Know what data the organisation has, where they are and secure the data		

A.3.4 (a)	Requirement	Requirement (CS/DS Essentials B.1, B.4, B.4.1, B.4.2)
		
		NOTE:
		– The HIA entity shall establish policies and processes to identify and protect its health information. Specifically, it shall 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.
		– The HIA entity shall set retention periods[5] for health information to ensure that such information is kept only where there is a business or legal purpose to do so.
		  – There shall be a proper rationale in the retention policy for the duration for which the health information is retained.
		  – The HIA entity shall consider applicable legislation (e.g. PDPA[6]), contractual requirements (e.g.

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

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

[5] 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.

[6] 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.

COPYRIGHT

Clause	Provisions in Cyber Essentials	Additional provisions for HIA entity
		funding or data sharing agreements), and national standards or guidelines[7].
A.3.4 (b)	Recommendation	Recommendation

A.3.4 (c)	Requirement	Requirement (CS/DS Essentials B.1, B.3, B.3.1, B.3.2, B.3.3)
		
		NOTE:
		– The HIA entity shall establish policies and processes to identify and protect its health information. Specifically, it shall 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.
		– The HIA entity shall have policies and practices to protect hardcopy documents containing health information that are stored in commercial storage facilities (outside office premises).
		  – The HIA entity shall check that the commercial storage facilities have adequate security measures, by checking on the service provider's credibility and security policies.
		  – The HIA entity shall maintain proper records of materials containing health information deposited in offsite storage.
		  – The HIA entity shall conduct stock-takes and audits to ensure its documents are intact or in order, and have not been subject to unauthorised access.

A.3.4 (d)	Requirement	Requirement (CS/DS Essentials B.1) NOTE: – The HIA entity shall establish policies and processes to identify and protect its health information. Specifically, it shall 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.
A.3.4 (e)	Requirement	Requirement (CS/DS Essentials C.9) NOTE: – Before disposing any hardware asset or data, the HIA entity shall ensure that all health information has been

[7] 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.

COPYRIGHT

Clause	Provisions in Cyber Essentials	Additional provisions for HIA entity
		securely destroyed[8] (e.g. shredding physical documents, encrypting hard disk before reformatting, and overwriting electronic data in a storage medium completely[9]).
A.4 Secure/Protect: Virus and malware protection – Protect from malicious software like viruses and malware		
A.4.4 (a)	Requirement	Requirement (CS/DS Essentials A.2)
A.4.4 (b)	Requirement	Requirement (CS/DS Essentials A.2.2, A.2.3) NOTE: – Virus and malware scans shall be carried out regularly to detect possible attacks.
A.4.4 (c)	Requirement	Requirement (CS/DS Essentials A.2.1)
A.4.4 (d)	Recommendation	Recommendation
A.4.4 (e)	Requirement	Requirement (CS/DS Essentials A.3)
A.4.4 (f)	Recommendation	Recommendation
A.4.4 (g)	Recommendation	Recommendation
A.4.4 (h)	Requirement	Requirement (CS/DS Essentials A.4.1) NOTE: – The HIA entity shall put in place policies and processes to ensure that its employees: – Install or access only authorised software or attachments from official or trusted sources.
A.4.4 (i)	Requirement	Requirement (CS/DS Essentials A.4.2) NOTE: – The HIA entity shall put in place policies and processes to ensure that its employees: – 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 shall also educate employees of the risks of using publicly available network connections, which are highly accessible and vulnerable against cyber-attacks.
A.4.4 (j)	Requirement	Requirement (CS/DS Essentials A.4.3) NOTE: – The HIA entity shall put in place policies and processes to ensure that its employees: – Are aware of the need to report any suspicious email or attachment to the IT team and / or senior management immediately.

[8] See Sample Sanitisation/Secure Disposal Standards from National Institute of Standards and Technology (NIST), Guidelines for Media Sanitisation from NIST.
[9] See PDPC Guide to Data Protection Practices for ICT Systems.

COPYRIGHT

Clause	Provisions in Cyber Essentials	Additional provisions for HIA entity
A.5 Secure/Protect: Access control – Control access to the organisation's data and services		
A.5.4 (a)	Requirement	Requirement (CS/DS Essentials A.5)
A.5.4 (b)	Requirement	Requirement (CS/DS Essentials A.5.1)
A.5.4 (c)	Requirement	Requirement (CS/DS Essentials A.7, A.7.1, A.7.2, A.7.4)

A.5.4 (d)	Requirement	Requirement (CS/DS Essentials A.7.3, B.10, B.10.1, B.10.2)
		
		NOTE:
		– The HIA entity shall have policies and processes to ensure that access to any health information is only granted to personnel who fulfil both the following conditions:
		  – The personnel (includes any third parties[10] 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).
		  – The personnel has been informed or made aware of, and has acknowledged[11] 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.

A.5.4 (e)	Requirement	Requirement (CS/DS Essentials A.6, A.6.1)
A.5.4 (f)	Requirement	Requirement (CS/DS Essentials A.6.2)
A.5.4 (g)	Requirement	Requirement (CS/DS Essentials A.9)
A.5.4 (h)	Requirement	Requirement (CS/DS Essentials A.9.1)
A.5.4 (i)	Recommendation	Recommendation
A.5.4 (j)	Requirement	Requirement (CS/DS Essentials A.10, B.2, B.2.1, B.2.2) NOTE: – The HIA entity shall secure health information from unauthorised access or loss where stored within office premises[12], as follows:

[10] Third parties shall consult the HIA entity (that engaged them) when uncertain about data disclosure permissions, while the HIA entity shall proactively establish and communicate clear restrictions for data requiring limited distribution. All third parties shall 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 shall 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.

[11] 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

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

COPYRIGHT

Clause	Provisions in Cyber Essentials	Additional provisions for HIA entity
		– Physical security measures shall include storing hardcopy documents in access-controlled locations within the office, such as storing these documents in locked file cabinet systems. – Laptops and portable storage media devices containing health information shall be locked and protected with a cable lock / attached to a fixture with a security cable when not in use[13].
A.5.4 (k)	Recommendation	Recommendation
A.5.4 (l)	Requirement	Requirement (CS/DS Essentials A.8)
A.5.4 (m)	Requirement	Requirement (CS/DS Essentials A.8.3)
A.5.4 (n)	Requirement	Requirement (CS/DS Essentials A.8.1)
A.5.4 (o)	Requirement	Requirement (CS/DS Essentials A.8.2)
A.5.4 (p)	Recommendation	Recommendation
A.6 Secure/Protect: Secure configuration – Use secure settings for the organisation's hardware and software		
A.6.4 (a)	Requirement	Requirement (CS/DS Essentials A.12, C.5) NOTE: – If the HIA entity is using cloud services (e.g. Amazon Web Services, Google Drive)[14], they shall ensure that they understand their responsibilities for setting security configurations.
A.6.4 (b)	Requirement	Requirement (CS/DS Essentials A.12.1)
A.6.4 (c)	Requirement	Requirement (CS/DS Essentials A.12.2)
A.6.4 (d)	Requirement	Requirement (CS/DS Essentials C.3, C.3.1, C.3.2, C.4, C.4.1, C.4.2, C.4.3) NOTE: – If the HIA entity is using an IT service provider[15] to manage its network, systems, and medical devices, it shall: – Clearly understand the services and security practices that the IT service provider will provide; and – 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. – When using third-party software and devices, the HIA entity shall ensure that it understands: – Where health information[16] is stored (whether in Singapore or overseas);

[13] Please refer to PDPC's Data Protection Practices for ICT Systems.
[14] 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
[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.
[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).

COPYRIGHT

Clause	Provisions in Cyber Essentials	Additional provisions for HIA entity
		– 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 vendors, audits); and – Its contractual arrangements with vendors, including responsibilities of each contractual party in the event of an incident or breach.
A.6.4 (e)	Recommendation	Recommendation
A.6.4 (f)	Requirement	Requirement (CS/DS Essentials A.12.3)
A.6.4 (g)	Requirement	Requirement (CS/DS Essentials A.11) NOTE: – The HIA entity shall maintain log-in rules (i.e. tracking of users logging[18] in and out of systems) properly and ensure that only authorised individuals have access to security logs.
A.6.4 (h)	Recommendation	Recommendation
A.6.4 (i)	Recommendation	Recommendation
A.6.4 (j)	Recommendation	Recommendation
A.7 Update: Software updates – Update software on devices and systems		
A.7.4 (a)	Requirement	Requirement (CS/DS Essentials A.1)
A.7.4 (b)	Recommendation	Recommendation
A.7.4 (c)	Recommendation	Recommendation
A.7.4 (d)	Recommendation	Recommendation
A.8 Backup: Back up essential data – Back up the organisation's essential data and store them separately and securely		
A.8.4 (a)	Requirement	Requirement (CS/DS Essentials A.13, A.14, A.14.1, A.14.2) NOTE: – If the scope includes cloud environment, the HIA entity shall: – Understand the role and responsibility between itself and the cloud service provider in terms of data backup; and – Ensure there are alternative forms of data backup being utilised to ensure business continuity.
A.8.4 (b)	Requirement	Requirement (CS/DS Essentials A.13.1)
A.8.4 (c)	Recommendation	Recommendation
A.8.4 (d)	Recommendation	Recommendation
A.8.4 (e)	Recommendation	Recommendation
A.8.4 (f)	Requirement	Requirement (CS/DS Essentials A.13.2)
A.8.4 (g)	Requirement	Requirement (CS/DS Essentials A.13.3)
A.8.4 (h)	Recommendation	Recommendation

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

[18] 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 shall also keep a manual log.

COPYRIGHT

Clause	Provisions in Cyber Essentials	Additional provisions for HIA entity
A.8.4 (i)	Recommendation	Recommendation
A.9 Respond: Incident response – Be ready to detect, respond to, and recover from cybersecurity incidents		
A.9.4 (a)	Requirement	Requirement (CS/DS Essentials C.11, C.12, C.12.1, C.12.2, C.12.3)
A.9.4 (b)	Requirement	Requirement (CS/DS Essentials C.13) NOTE: – The incident response plan[19] shall be made known to all employees in the organisation that have access to the organisation's IT assets and/or environment. All personnel shall also be aware of how to report suspicious activity and possible incidents based on the obligations under prevailing legislative or regulatory requirements.
A.9.4 (c)	Recommendation	Recommendation
A.9.4 (d)	Recommendation	Recommendation

C-HIA.3.5 Additional provisions for data security for HIA entity

Following shows the additional provisions for data security for HIA entity.

HIA Clause	Additional provisions for HIA entity
Additional HIA Data Security Requirements[20]	
B.5	Requirement (CS/DS Essentials B.5) The HIA entity shall 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	Requirement (CS/DS Essentials B.6) When making copies of health information using external devices (e.g. scanners, portable storage devices) or at external locations, the HIA entity shall have policies and practices to ensure that its personnel maintain possession of all copies made (e.g. personnel of a HIA entity shall not leave photocopied materials unattended at photocopiers outside the office premises).
B.7	Requirement (CS/DS Essentials B.7. B.7.1, B.7.2, B.7.3, B.7.4) The HIA entity shall have policies and practices to ensure that, when transferring any health information in public or transmitting electronically - – Its personnel only bring necessary health information out of the office, on a need-to-know basis and for appropriate work purposes;

[19] 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.

[20] The HIA entity's policies and processes have to take into account any legal and regulatory requirements (e.g. Personal Data Protection Act, Healthcare Services Act, Health Information Act).

COPYRIGHT

HIA Clause	Additional provisions for HIA entity
	– Materials containing health information remain in its personnel's possession or control at all times (e.g. documents shall not be left unattended); – Health information shall be protected from accidental exposure (e.g. use privacy filters or position computers to limit visibility); and – Files containing health information are protected from any unauthorised access. Electronic transmissions of files, e.g. by email, shall be password-protected (by setting strong passwords[21] 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).
B.8	Requirement (CS/DS Essentials B.8, B.8.1, B.8.2) The HIA entity shall have policies and practices[22] for marking health information to enable its personnel to recognise and properly manage the health information they are handling, such as: – Having an organisation-wide policy requiring all documents containing health information to be manually or electronically labelled when they are created (e.g. by inserting headers or footers in medical reports when they are created); – Where marking all documents and data is assessed to be impractical, the HIA entity shall clearly specify in its corporate policy what data shall be treated as health information (e.g. all information in medical reports) instead of marking the individual documents, and its personnel shall comply with the corresponding security measures for health information.
B.9	Requirement (CS/DS Essentials B.9, B.9.1, B.9.2, B.9.3, B.9.4) The HIA entity shall consider the following factors when assessing whether and how to mark its health information: – Format of the health information (e.g. hardcopy or in electronic format); – Practicality of marking (e.g. manual stamping of hard copies, cost of IT system enhancement if marking is done electronically); – 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 – Intent of the marking (i.e. to alert the recipient of the health information to protect the health information accordingly).
C.6	Requirement (CS/DS Essentials C.6) The HIA entity shall periodically review[23] its implementation of cybersecurity and data security safeguards for health information.
C.7	Requirement (CS/DS Essentials C.7) The HIA entity shall 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	Requirement (CS/DS Essentials C.8)

[21] Please refer to the CSA guidelines on how to set strong passwords.
[22] See PDPC Guide to Data Protection Practices for ICT Systems.
[23] See PDPC Guide on Data Protection Management Programme, PDPC Guide to Data Protection Impact Assessments

COPYRIGHT

<table>
<tr><th>HIA Clause</th><th>Additional provisions for HIA entity</th></tr>
<tr><td></td><td>The HIA entity shall 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).</td></tr>
<tr><td>C.10</td><td>Requirement (CS/DS Essentials C.10)

The HIA entity shall 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.</td></tr>
<tr><td>C.14</td><td>Requirement (CS/DS Essentials C.14)

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

<table>
<tr><th></th><th>Cybersecurity Incidents</th><th>Data Breaches</th></tr>
<tr><td>Reporting Thresholds</td><td>• A notifiable[24] 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.</td><td>• 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[25] to an affected individual; or
ii. is, or is likely to be, of a significant scale (i.e. 500 or more affected individuals).</td></tr>
<tr><td>Reporting Requirements</td><td colspan="2">• Initial notification to MOH within <u>2 hours</u> 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 <u>incident report within 14 days</u> of initial notification.
• The HIA entity shall 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.</td></tr>
</table>
</td></tr>
</table>

[24] 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.

[25] 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.

COPYRIGHT