Annex B-HIMS
(normative)

Cyber Essentials mark for Health Information Management System (HIMS) vendors – Requirements

B-HIMS.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 MOH's **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. The Health Information Management System (HIMS) vendors will also be required to meet the additional cybersecurity requirements described in the MOH's **HIA-compliant HIMS Certification Framework**, for software-as-a-service (SaaS) and non-SaaS implementations.

B-HIMS.2 Additional terms and definitions

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

B-HIMS.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. HIMS vendors 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.

B-HIMS.2.2 HIMS vendor implemented as software-as-a-service (SaaS)

HIMS applications and product features are provided as a service.

B-HIMS.2.3 HIMS vendor implemented as non-SaaS

HIMS applications and product features are deployed as a standalone application installed on a workstation/desktop/laptop.

B-HIMS.3 Cyber Essentials mark for HIMS vendors

B-HIMS.3.1 Boundary of scope and statement of scope

[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).

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

- The production and development environment for HIMS vendor providing SaaS solution; or
- The development environment for HIMS vendor providing non-SaaS solution.

The statement of scope shall apply to all devices, systems[2] and software that are within this boundary of scope; and shall minimally include classical cybersecurity requirements defined in B-HIMS.3.4 and B-HIMS 3.5.[3]

B-HIMS.3.2 Pre-certification preparation by HIMS vendor

Prior to engaging a certification body, the HIMS vendor shall complete the guided self-assessment template required for Cyber Essentials mark certification for HIMS vendors.

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

B-HIMS.3.3 Independent assessment by certification body

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

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

B-HIMS.3.4 Provisions for Cyber Essentials for HIMS vendors

Following shows the provisions for Cyber Essentials for HIMS vendors.

Clause	Provisions in Cyber Essentials	Additional provisions for HIMS vendor
A.1 Assets: People – Equip employees with know-how to be the first line of defence		
A.1.4 (a)	Requirement	Requirement
A.1.4 (b)	Requirement	Requirement NOTE: – The HIMS vendor 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		
A.2.4 (a)	Requirement	Requirement NOTE: – The asset inventory shall include: – 3rd party software and tools deployed, and

[2] For HIMS vendor that adopts cloud-based software, the scope of assessment and certification shall include such cloud-based services.

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

Clause	Provisions in Cyber Essentials	Additional provisions for HIMS vendor
		– what is hosted on the cloud instances, e.g., software and Operating System (OS). – The asset inventory shall track expiry of all digital assets, such as certificates, software licenses, software renewal, etc. – The asset inventory shall be reviewed at least once a year.
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
A.2.4 (g)	Requirement	Requirement NOTE: – No EOS asset shall be allowed for HIMS vendor.
A.2.4 (h)	Requirement	Requirement
A.2.4 (i)	Requirement	Requirement
A.2.4 (j)	Requirement	Requirement
A.2.4 (k)	Requirement	Requirement NOTE: – Before disposing any hardware asset or data, the HIMS vendor shall ensure that all health information has been securely destroyed[4] (e.g. shredding physical documents, encrypting hard disk before reformatting, and overwriting electronic data in a storage medium completely[5]).
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 NOTE: – The HIMS vendor 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.

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

Clause	Provisions in Cyber Essentials	Additional provisions for HIMS vendor

		– The HIMS vendor shall set retention periods[6] 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 HIMS vendor shall consider applicable legislation (e.g. PDPA[7]), contractual requirements (e.g. funding or data sharing agreements), and national standards or guidelines[8].

A.3.4 (b)	Recommendation	Recommendation

A.3.4 (c)	Requirement	Requirement
		
		NOTE:
		– HIMS vendor shall establish process(es) to protect data-in-motion, such as backup or migration.
		– The HIMS vendor 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 HIMS vendor shall have policies and practices to protect hardcopy documents containing health information that are stored in commercial storage facilities (outside office premises).
		  – The HIMS vendor shall check that the commercial storage facilities have adequate security measures, by checking on the service provider's credibility and security policies.
		  – The HIMS vendor shall maintain proper records of materials containing health information deposited in offsite storage.
		  – The HIMS vendor 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

[6] 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.

[7] 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.

[8] 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.

Clause	Provisions in Cyber Essentials	Additional provisions for HIMS vendor
		NOTE: – HIMS vendor shall include the terms on unauthorised disclosure of information within the employment contracts and contractual agreement with its business partners (e.g., providing the maintenance services). – The HIMS vendor 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 NOTE: – Before disposing any hardware asset or data, the HIMS vendor shall ensure that all health information has been securely destroyed[9] (e.g. shredding physical documents, encrypting hard disk before reformatting, and overwriting electronic data in a storage medium completely[10]).
A.4 Secure/Protect: Virus and malware protection – Protect from malicious software like viruses and malware		
A.4.4 (a)	Requirement	Requirement
A.4.4 (b)	Requirement	Requirement NOTE: – Virus and malware scans shall be carried out regularly to detect possible attacks.
A.4.4 (c)	Requirement	Requirement
A.4.4 (d)	Recommendation	Recommendation
A.4.4 (e)	Requirement	Requirement NOTE: – HIMS vendor providing SaaS solution shall implement a Web Application Firewall (WAF) to mitigate threats, e.g., Open Worldwide Application Security Project (OWASP) Top 10, from external sources.
A.4.4 (f)	Recommendation	Recommendation
A.4.4 (g)	Recommendation	Recommendation
A.4.4 (h)	Requirement	Requirement
A.4.4 (i)	Requirement	Requirement
A.4.4 (j)	Requirement	Requirement

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

Clause	Provisions in Cyber Essentials	Additional provisions for HIMS vendor
A.5 Secure/Protect: Access control – Control access to the organisation's data and services		
A.5.4 (a)	Requirement	Requirement
A.5.4 (b)	Requirement	Requirement
A.5.4 (c)	Requirement	Requirement

A.5.4 (d)	Requirement	Requirement
		
		NOTE:
		– The HIMS vendor 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[11] engaged by the HIMS vendor, 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 HIMS vendor (e.g. a clinician is granted access rights to the HIMS vendor'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[12] the data protection and security measures in these CS/DS Essentials, relevant prevailing laws e.g. PDPA, the HIMS vendor's corporate policies and/or professional ethics/policies.
		– The HIMS solution shall allow HIMS administrator to apply the principle of least privilege to all accounts (e.g., users, services) so as to ensure excessive privileges are not granted. The HIMS solution should implement Attribute-Based Access Control (ABAC) using multiple attributes such as role, location, authentication method, IP address, mutual authentication and/or Role-Based Access Control (RBAC) mechanism that enforces access to all parts of the HIMS.
		– HIMS vendor shall ensure clear segregation of duties for privileged roles in the HIMS such as network, operating system, database, log management and security administrators to address risks associated with user-role conflict of interest.

[11] Third parties shall consult the HIMS vendor (that engaged them) when uncertain about data disclosure permissions, while the HIMS vendor 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 HIMS vendor, unless authorised by law.

[12] 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

Clause	Provisions in Cyber Essentials	Additional provisions for HIMS vendor
		– HIMS vendor shall establish access control matrix for HIMS's underlying infrastructure, with roles and responsibilities clearly documented. – HIMS vendor shall ensure that only authorised personnel is able to access the logs; operations personnel should not have access to logs to prevent risk of tampering or deletion.
A.5.4 (e)	Requirement	Requirement
A.5.4 (f)	Requirement	Requirement
A.5.4 (g)	Requirement	Requirement
A.5.4 (h)	Requirement	Requirement
A.5.4 (i)	Recommendation	Recommendation

A.5.4 (j)	Requirement	Requirement
		
		NOTE:
		– The HIMS vendor shall secure health information from unauthorised access or loss where stored within office premises[13], as follows:
		  – 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[14].
		– HIMS vendor providing SaaS solution shall implement Multi-Factor Authentication (MFA) for physical access to the room that host the HIMS solution and the room that host terminal(s) that has/have access to the HIMS solution.

A.5.4 (k)	Recommendation	Recommendation
A.5.4 (l)	Requirement	Requirement
A.5.4 (m)	Requirement	Requirement
A.5.4 (n)	Requirement	Requirement
A.5.4 (o)	Requirement	Requirement NOTE: – For HIMS vendor, the solution shall authenticate all login personnel through multi-factor authentication (MFA).
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 NOTE:

[13] See PDPC Advisory Guidelines on Key Concepts in the PDPA (Chapter 17 on the Protection Obligation).
[14] Please refer to PDPC's Data Protection Practices for ICT Systems.

Clause	Provisions in Cyber Essentials	Additional provisions for HIMS vendor
		– If the HIMS vendor is using cloud services (e.g. Amazon Web Services, Google Drive)[15], they shall ensure that they understand their responsibilities for setting security configurations. – HIMS vendor shall have vulnerability management processes to identify and manage vulnerabilities in the HIMS solution, as well as production and development environments. – HIMS vendor shall perform security testing (such as Vulnerability Assessment / Penetration Testing) on the HIMS solution and production environment before commissioning, periodically and upon major changes. – HIMS vendor shall remediate identified vulnerabilities that have a risk rating of "High". The risk rating should be based on industry best practices as well as consideration of potential impact. For example, criteria for the rating may include consideration of the CVSS base score, and/or the classification by the vendor, and/or impact to application functionality.
A.6.4 (b)	Requirement	Requirement
A.6.4 (c)	Requirement	Requirement

A.6.4 (d)	Requirement	Requirement
		
		NOTE:
		– If the HIMS vendor is using an IT service provider[16] 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 HIMS vendor.
		– When using third-party software and devices, the HIMS vendor shall ensure that it understands:
		  – Where health information[17] is stored (whether in Singapore or overseas);
		  – The safeguards[18] 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

[15] 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

[16] 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.

[17] 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).

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

Clause	Provisions in Cyber Essentials	Additional provisions for HIMS vendor
		– 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
A.6.4 (g)	Requirement	Requirement NOTE: – The HIMS vendor shall maintain log-in rules (i.e. tracking of users logging[19] in and out of systems) properly and ensure that only authorised individuals have access to security logs. – The "out-of-the-box" default installation shall log all user access and be able to link all activities to individual users. – The HIMS solution shall provide automated security-related logs to facilitate event reconstruction and incident investigation. – The HIMS solution shall generate logs that are readable in ASCII plaintext or UTF-8. – The HIMS solution shall store logs at secured locations to protect the integrity and ensure availability of the logs. It should have the capability to store logs in 3rd party solution. – HIMS vendor shall store logs at secured locations to protect the integrity and ensure availability of the logs. – HIMS vendor shall provide documentation that has information on the log formats, to facilitate log review. – HIMS vendor shall ensure that a log review process is defined, documented and implemented to detect suspicious activities and early indicators of security breaches. – HIMS vendor shall ensure that security logs are generated and monitored timely to detect suspicious or malicious activity (e.g., unusual administrative activities during off peak hours, creation of unknown administrator accounts, escalating privileges for user accounts, lateral traversal across multiple segments and attempted download/upload by single system within a short period, disabling security controls such as disable audit log etc.) – HIMS vendor shall ensure that security monitoring mechanisms are in place to monitor all security related events for timely detection of suspicious events or malicious activities.
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		

[19] 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 HIMS vendor shall also keep a manual log.

Clause	Provisions in Cyber Essentials	Additional provisions for HIMS vendor
A.7.4 (a)	Requirement	Requirement NOTE: – HIMS vendor, who is supplying HIMS solution to healthcare service provider, shall notify Licensees[20] the availability of updates/patches, and deliver those updates/patches to the Licensees in a secure and prompt manner, if possible, guide/assist the Licensee to ensure the updates/patches are implemented successfully.
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
		
		NOTE:
		– HIMS vendor shall establish backup strategies (e.g. scope and frequency for data backups is determined and implemented, etc.) and aligned with RPO.
		– HIMS vendor shall implement a version control system where developers can roll back to a previous version in the event of any show-stopping bug gets discovered.
		– If the scope includes cloud environment, the HIMS vendor 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
A.8.4 (c)	Recommendation	Recommendation
A.8.4 (d)	Recommendation	Recommendation
A.8.4 (e)	Recommendation	Recommendation
A.8.4 (f)	Requirement	Requirement NOTE: – The backup shall include configuration, source code and data. – The backup shall be encrypted with cryptographic algorithms and key lengths that follow the recommendations from National Institute of Standards and Technology (NIST) or equivalent.
A.8.4 (g)	Requirement	Requirement NOTE: – HIMS vendor providing non-SaaS solution shall also ensure that the solution has the feature to allow its backup data be kept offline.

[20] Licensee refers to clinics licensed under the Healthcare Services Act.

Clause	Provisions in Cyber Essentials	Additional provisions for HIMS vendor
		– The backup shall be encrypted with cryptographic algorithms and key lengths that follow the recommendations from NIST or equivalent.
A.8.4 (h)	Recommendation	Recommendation
A.8.4 (i)	Recommendation	Requirement NOTE: – Backups shall be tested annually, or more frequently, to ensure that business-critical systems and essential business information can be restored effectively. – HIMS vendor shall conduct at least annual testing of data recoverability to validate effectiveness of disaster recovery plan
A.9 Respond: Incident response – Be ready to detect, respond to, and recover from cybersecurity incidents		
A.9.4 (a)	Requirement	Requirement NOTE: – HIMS vendor providing SaaS solution shall also put in place incident response plan to assist healthcare provider in responding to their obligations under prevailing legislative or regulatory requirements.
A.9.4 (b)	Requirement	Requirement NOTE: – The incident response plan[21] 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

B-HIMS.3.5 Additional provisions for data security for HIMS vendor

Following shows the additional provisions for data security for HIMS vendor entity.

HIB Clause	Additional provisions for HIMS vendor
Additional HIA Data Security Requirements[22]	
B.5	Requirement (CS/DS Essentials B.5)

[21] 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.

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

HIB Clause	Additional provisions for HIMS vendor
	The HIMS vendor 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 HIMS vendor shall have policies and practices to ensure that its personnel maintain possession of all copies made (e.g. personnel of a HIMS vendor 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 HIMS vendor 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; – 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[23] 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 HIMS vendor shall have policies and practices[24] 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 HIMS vendor 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 HIMS vendor 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 HIMS vendor that handles health information on a day-to-day basis, or a third-party vendor

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

<table>
<tr><th>HIB Clause</th><th>Additional provisions for HIMS vendor</th></tr>
<tr><td></td><td>managing or delivering documents containing health information on behalf of a HIMS vendor); and
– Intent of the marking (i.e. to alert the recipient of the health information to protect the health information accordingly).</td></tr>
<tr><td>C.6</td><td>Requirement (CS/DS Essentials C.6)

The HIMS vendor shall periodically review[25] its implementation of cybersecurity and data security safeguards for health information.</td></tr>
<tr><td>C.7</td><td>Requirement (CS/DS Essentials C.7)

The HIMS vendor shall conduct checks (e.g. self-assessments, or audits conducted by external auditors, as determined by the HIMS vendor’s business or operational considerations) to review established corporate policies, its personnel’s compliance with its corporate policies.</td></tr>
<tr><td>C.8</td><td>Requirement (CS/DS Essentials C.8)

The HIMS vendor 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 HIMS vendor 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 HIMS vendors 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[26] cybersecurity incident involves:
i. a computer or computer system containing health information or interconnected with a computer or computer system containing health information; and</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[27] to an affected individual; or</td></tr>
</table>
</td></tr>
</table>

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

[26] 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.

[27] 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.

HIB Clause	Additional provisions for HIMS vendor		
		ii. The computer or computer systems are under the HIMS vendor's control.	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 **<u>2 hours</u>** after the HIMS vendor assesses that the incident is a notifiable cybersecurity incident or data breach meeting the reporting thresholds. • Affected HIMS vendor to provide an **<u>incident report within 14 days</u>** of initial notification. • The HIMS vendor 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.	