Privacy Commissioner sets expectations of reasonable IT security standards to ensure compliance with Rule 5 of the Health Information Privacy Code.

The Privacy Commissioner has issued a Compliance Notice to Manage My Health setting out the minimum IT security safeguards needed to ensure compliance with rule 5(1)(a) of the Health Information Privacy Code. The safeguards are those the Commissioner considers reasonable for health agencies to have in place to protect sensitive health information against loss, access, use, modification, unauthorised disclosure or other misuse.

Read the Compliance Notice [link to website].

In developing the Compliance Notice requirements, the Privacy Commissioner identified seven areas where security protections were ineffective:

1. The need for multifactor authentication (MFA)
2. Identity and access management
3. Web security
4. Patch and vulnerability management
5. System acquisition, development, and maintenance
6. Logging and monitoring
7. Data leak prevention.

These expectations are set out in detail below for use by any health agency dealing with health information. The expectations align with the Health Information Security Framework.

This information is intended for a technical audience and will likely be best read by the people who make the IT decisions in your agency.

Multifactor authentication

The risk of unauthorised access through compromised credentials should be reduced through effective MFA controls across all systems containing sensitive information. This can be achieved by:

1. Enforcing MFA consistently across all user groups and access methods.
2. Providing alternative secure authentication methods to users, including app-based or equivalent MFA mechanisms.
3. Implementing monitoring and alerting for suspicious authentication activity and indicators of credential misuse.

Identity and access management

Users should only be able to access information they are authorised to access, and effective authorisation and access control mechanisms should be implemented across all systems and interfaces containing sensitive information. This can be achieved by:

1. Ensuring users can only access information they are authorised to access.
2. Developing and implementing appropriate standards, policies and/or procedures, and system configuration to ensure access to information is validated against the identity and permission of the requesting user and not based solely on user-supplied identifiers or parameters.
3. Remediating any functionality that allows access to information outside a user's authorised scope.
4. Implementing monitoring and alerting to identify unauthorised or inappropriate access to information.
5. Conducting a review of all relevant systems and interfaces and identify and remediate any ineffective authorisation controls.
6. Implementing a schedule for testing and validating that users are unable to access information outside their authorised scope.

Web security

External access to systems should be appropriately controlled and protected against malicious activity in a manner proportionate to the exposure and sensitivity of the services provided. This can be achieved by:

1. Ensuring all inbound access is routed through controlled and secure entry points.
2. Implementing and maintaining WAF and firewall protections to detect and block malicious or abnormal traffic.
3. Implementing controls capable of identifying and responding to automated abuse patterns.
4. Implementing logging, monitoring, and alerting of web and API activity to support detection of malicious and abnormal traffic.
5. Implementing a schedule for the regular review, test, and validation of web security controls.
6. Establishing accountability and assurance mechanisms for third-party managed controls.

Patch and vulnerability management

Vulnerabilities should be effectively identified, managed, and remediated in a structured and consistent manner proportionate to the sensitivity and criticality of the information and

systems involved. This can be achieved by developing and implementing appropriate standards, policies and/or procedures that:

1. Specify timeframes for the remediation of vulnerabilities that are appropriate to their level of risk.
2. Ensure that remediation activities address underlying causes of vulnerabilities, particularly where similar issues have been identified over time.
3. Ensure that vulnerabilities identified through internal and external sources (including testing and independent assessments) are incorporated into a consistent management and remediation process.
4. Ensure that remediation activities are validated to confirm that identified vulnerabilities have been effectively addressed in practice.
5. Ensure that recurring vulnerability themes are identified and treated as indicators of broader issues requiring systemic remediation.
6. Ensure that vulnerability management activities are subject to appropriate governance, including oversight of remediation progress and formal risk acceptance where applicable.

System acquisition, development, and maintenance

Systems should be securely designed, developed, tested, and maintained, using effective secure development and system assurance controls. This can be achieved by:

1. Developing and implementing appropriate standards, policies and/or procedures to effect a structured secure development lifecycle that incorporates security considerations throughout system acquisition, development, and maintenance.

   These standards, policies and/or procedures should ensure that:

   a. Security requirements are formally defined, documented, and considered as part of system design and development.
   b. Secure-by-design principles are applied in development activities, including appropriate controls for access management, API security, and protection of health information.
   c. Security testing activities are comprehensive, risk-aligned, and capable of identifying vulnerabilities relevant to the system and its exposure.
   d. Security testing outcomes are validated, and that remediation activities are verified to be effective prior to production release.
   e. Vulnerabilities identified through development and testing activities are incorporated into a consistent process for remediation and closure.

f. Recurring vulnerability themes identified through testing or operation are used to inform improvements in development practices.
g. Appropriate independence exists between development and security assurance activities, particularly where responsibilities may overlap.
h. Clear roles, responsibilities, and accountability are established where system development or operation is outsourced.

Logging and monitoring

Security relevant activity should be appropriately monitored, detected, and responded to, by:

1. Ensuring that logging is enabled across systems and services to provide visibility of security relevant activity.
2. Developing and implementing defined operational processes for reviewing, triaging and responding to security alerts including appropriate measures to ensure that:
    a. Logs are retained and accessible to support investigation and response activities.
    b. Log data is monitored and analysed to identify suspicious, abnormal, or unauthorised activity.
    c. Security alerts are configured to identify relevant threat scenarios and are actively monitored.
    d. Logging and monitoring controls are capable of supporting timely detection and response to incidents in practice.

Data leak protection

Sensitive health information should be protected from unauthorised disclosure or exfiltration, in a manner proportionate to its sensitivity and volume. This can be achieved by ensuring data loss prevention controls are in place to:

1. Detect and prevent unauthorised access to, or extraction of, health information.
2. Restrict large-scale or abnormal data retrieval, including mechanisms to limit excessive or high-volume access.
3. Ensure MMH can accurately identify, analyse, and quantify data access and potential exfiltration during an incident.
4. Ensure suspected data exfiltration events generate alerts and are responded to in a timely manner.
5. Implement logging, monitoring and alerting to identify bulk data access, export activity, and anomalous data access patterns.
6. Implement a schedule for the regular review, test, and validation of data loss prevention controls.