Arrangements to manage confidential patient information within WA Health

Review report
Enquiries:

Conduct and Compliance
Public Sector Commission
Dumas House, 2 Havelock Street, WEST PERTH WA 6005
Locked Bag 3002, WEST PERTH WA 6872
Telephone: (08) 6552 8500
Fax: (08) 6552 8710
Email: admin@psc.wa.gov.au
Website: www.publicsector.wa.gov.au

© State of Western Australia 2018
There is no objection to this publication being copied in whole or part, provided there is due acknowledgement of any material quoted or reproduced.
Published by the Public Sector Commission, August 2018.
This publication is available on the Public Sector Commission website at www.publicsector.wa.gov.au

Disclaimer
The Western Australian Government is committed to quality service to its customers and makes every attempt to ensure accuracy, currency and reliability of the information contained in this publication. However, changes in circumstances over time may impact on the veracity of this information.

Accessibility
Copies of this publication are available in alternative formats upon request.
Consistent with my functions under section 22E of the *Public Sector Management Act 1994*, and in accordance with section 22F, I submit to each House of Parliament a report on a review of arrangements to manage confidential patient information within WA Health.

Observations and suggested improvements arising from the review are considered to be of such significance as to warrant reporting to Parliament in this manner.

SHARYN O’NEILL  
PUBLIC SECTOR COMMISSIONER

13 August 2018
Contents

Terms and definitions ........................................................................................................... 5
Executive summary .................................................................................................................. 6
Background ............................................................................................................................ 9
Approach taken in the review ............................................................................................... 12
The state of information management in WA Health ......................................................... 14
Observations and suggested improvements ....................................................................... 18
Appendix – Relevant policies, requirements and reports ...................................................... 26
## Terms and definitions

<table>
<thead>
<tr>
<th>Key term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AEDM</td>
<td>Accountable and ethical decision making.</td>
</tr>
<tr>
<td>APP entity</td>
<td>An agency or organisation subject to the Australian Privacy Principles (APPs) under the Privacy Act 1988.</td>
</tr>
<tr>
<td>APPs</td>
<td>The APPs as contained in Schedule 1 of the Privacy Act 1988.</td>
</tr>
<tr>
<td>BOSSnet</td>
<td>A clinical information system used in some hospitals for electronic medical records.</td>
</tr>
<tr>
<td>Code of conduct</td>
<td>Communicates the expected standards of conduct and integrity to all employees, from the Director General or a Chief Executive Officer through to trainees.</td>
</tr>
<tr>
<td>Data</td>
<td>‘Data’ generally refers to unprocessed information, while ‘information’ is data that has been processed to be meaningful. Throughout this report, the terms ‘data’ and ‘information’ are used interchangeably.</td>
</tr>
<tr>
<td>Data custodian</td>
<td>In WA Health terminology, a person(s) responsible for the day-to-day management of a data collection, as nominated by a data steward. Data custodians assist data stewards to protect information privacy, security and confidentiality. Data custodians aim to improve data accuracy, usability and accessibility.</td>
</tr>
<tr>
<td>Data steward</td>
<td>In WA Health terminology, a position with delegated responsibility from the Director General or a Chief Executive Officer to manage a data collection. A data steward’s primary responsibility is to protect the privacy, security and confidentiality of information. Data stewards approve conditions for use and disclosure of information in accordance with statutory obligations and the information management policy framework.</td>
</tr>
<tr>
<td>Data warehouse</td>
<td>A large store of data accumulated from a wide range of sources within a company and used to guide management decisions.</td>
</tr>
<tr>
<td>Health service provider (HSP)</td>
<td>A HSP is established under section 32 of the Health Services Act 2016 (HS Act) and includes North Metropolitan Health Service (NMHS), South Metropolitan Health Service (SMHS), Child and Adolescent Health Service (CAHS), WA Country Health Service (WACHS) and East Metropolitan Health Service (EMHS). For the purposes of this review, the Quadriplegic Centre was not considered a HSP.</td>
</tr>
<tr>
<td>HS Act</td>
<td>Health Services Act 2016 (WA).</td>
</tr>
<tr>
<td>Health Support Services (HSS)</td>
<td>Acts as a systems provider and administrator for core or enterprise systems used by WA Health.</td>
</tr>
<tr>
<td>IC</td>
<td>Generally refers to an information circular.</td>
</tr>
<tr>
<td>iSoft Clinical Manager (iCM)</td>
<td>An intermediary clinical system used by HSPs to access patient clinical notes and pathology results, generate handover notes, and lodge requests for pathology tests to be undertaken.</td>
</tr>
<tr>
<td>MP</td>
<td>Generally refers to a mandatory policy.</td>
</tr>
<tr>
<td>OD</td>
<td>Generally refers to an operational directive.</td>
</tr>
<tr>
<td>SHR</td>
<td>Refers to the Sustainable Health Review, the review of the WA health system.</td>
</tr>
<tr>
<td>WA Health</td>
<td>WA Health comprises the Department of Health, HSPs and HSS. Contracted Health entities and private-public partnership arrangements were excluded from this review.</td>
</tr>
</tbody>
</table>
Executive summary

The issue

The WA health system (WA Health) collects a vast amount of healthcare-related information in the course of delivering services to the community. This information may be personal and sensitive in nature, such as family history, lifestyle behaviours, health status and genetic data.

Multiple inputs feed into a health information system and multiple individuals or systems may access that information. When no longer actively required, information is either disposed of or placed in a data warehouse. These arrangements lend themselves to multiple risks in managing confidential patient information.

Patients generally understand that their information may be shared as part of their healthcare experience, with their consent. However, they also have a reasonable expectation that their information will not be shared with unauthorised parties and that it will only be used for the purpose for which it was collected.

The Public Sector Commissioner (the Commissioner) has previously released Public Sector Commissioner’s circular: Computer information and internet security (2010-05) as a response to risks identified in information systems. In any public authority, comprehensive management and technical and physical controls are essential to protect against the risk of personal and sensitive information being misused. As public authorities seek to improve services through information sharing, the importance of maintaining effective controls is increased.

In WA Health, the code of conduct requires staff to maintain confidentiality about any personal information that becomes available to them in the course of their employment and to only use it in connection with their position. Any unauthorised access or disclosure of patient information may result in improvement or disciplinary action in accordance with the relevant employment framework.

The review

On 21 August 2017, the Commissioner received correspondence from Professor Bryant Stokes AM, Board Chair, North Metropolitan Health Service, requesting that the Commissioner undertake an independent review of the handling by PathWest of a patient complaint.

In response to this request, the Commissioner initiated two parallel bodies of work at the end of 2017. The first exercise was an investigation into a particular case of unauthorised disclosure of patient information. A report on that matter was tabled in Parliament on 29 November 2017.
The second exercise focused on a review (this report) under s. 24B(1) of the *Public Sector Management Act 1994* (PSM Act) into the systems and controls applied more broadly across WA Health to mitigate breaches of patient confidentiality.

The objective was to assess the extent to which integrity risks associated with protecting the confidentiality of patient information are being appropriately managed.

**Maturity of arrangements in WA Health**

The maturity of arrangements for managing confidential patient information was observed to vary across WA Health as seen in Figure 1. Almost all health service providers (HSPs) had a sophisticated approach to leading and guiding behaviour to protect patient confidentiality. However, they were less likely to be taking a proactive and repeated approach to teaching this specific capability across the workforce.

**Figure 1: Observed maturity of arrangements in WA Health**

<table>
<thead>
<tr>
<th>Review focus area</th>
<th>Distribution of assessed levels across HSPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leadership commitment</td>
<td><img src="chart" alt="Bar chart showing distribution" /></td>
</tr>
<tr>
<td>Culture of engagement</td>
<td><img src="chart" alt="Bar chart showing distribution" /></td>
</tr>
<tr>
<td>Accountability</td>
<td><img src="chart" alt="Bar chart showing distribution" /></td>
</tr>
<tr>
<td>Guiding behaviour</td>
<td><img src="chart" alt="Bar chart showing distribution" /></td>
</tr>
<tr>
<td>Employing for integrity</td>
<td><img src="chart" alt="Bar chart showing distribution" /></td>
</tr>
<tr>
<td>Workforce knowledge and skills</td>
<td><img src="chart" alt="Bar chart showing distribution" /></td>
</tr>
<tr>
<td>Risk management</td>
<td><img src="chart" alt="Bar chart showing distribution" /></td>
</tr>
<tr>
<td>Continual improvement</td>
<td><img src="chart" alt="Bar chart showing distribution" /></td>
</tr>
</tbody>
</table>
Suggested improvements

The following improvements are suggested with the aim of assisting WA Health to strengthen its current arrangements to manage confidential patient information.

It is suggested that WA Health:

1. ensure leaders’ expectations in relation to confidential patient information are regularly communicated and reinforced to staff
2. regularly test perceptions of the commitment to patient confidentiality and misconduct reporting
3. where breaches of patient confidentiality occur, ensure sanctions are appropriate to the seriousness of misconduct
4. continue to improve awareness and understanding of the Data stewardship and custodianship policy and the responsibilities of data stewards and custodians
5. maintain awareness of accessible avenues for staff to report alleged breaches of patient confidentiality
6. ensure avenues for patients to make complaints about breaches of patient confidentiality are well-publicised
7. enhance risk management controls for positions of trust that access and manage confidential patient information (such as regular integrity checks or confidentiality agreements)
8. implement repeated training and education for all staff, such as an AEDM refresher course, that covers obligations for the protection of patient confidentiality
9. formally assess the risk of breaches in patient confidentiality
10. continue working to improve misconduct detection and monitoring capability in information systems like iCM
11. ensure detailed reporting of misconduct trends to relevant boards to enable a proactive response to emerging issues
12. implement regular audits of the framework and policies relating to patient confidentiality and related processes (e.g. data breach response) relevant to their respective roles within the system.
Background

This report details the observations and suggested improvements of a review of arrangements to manage confidential patient information across WA Health.

Catalyst and authority for the review

The Commissioner received correspondence from the North Metropolitan Health Service Board Chair on 21 August 2017, requesting that the Commissioner undertake an independent review of the handling of a patient complaint by PathWest, The complaint related to disclosure by a WA Health employee of the patient’s confidential medical information during 2014.

In response, the Commissioner initiated two parallel bodies of work:

1. An investigation under s. 24 of the PSM Act into PathWest’s response to the specific patient complaint. The report of this investigation was tabled in Parliament on 29 November 2017.

2. A review under s. 24B(1) into the arrangements in place within WA Health for managing confidential patient information. Under this section of the PSM Act, the Commissioner can undertake a review of the functions, management or operations of one or more public sector bodies. This review is the subject of this report.

These two bodies of work were completed separately.

Objective

The objective of the review was to assess the maturity of arrangements in place at WA Health to help protect confidential patient information.

Relevant considerations

The observations and suggested improvements of this review are not intended to be definitive or cover all matters of significance in relation to the management of confidential patient information across WA Health. They are formed from an assessment of information that is persuasive rather than conclusive. This report provides information for further consideration in regard to improving the management of confidential information.

For practical reasons, a sampling methodology was adopted for the review. There may be degrees of variance within individual sites and across HSPs. However, the observations and suggested improvements can be extrapolated and may be of relevance to any public authority that manages confidential client information.
Scope of the review

The scope of the review encompassed current arrangements for the management of confidential patient information across five HSPs.

In selecting a sample site within the HSPs, a diverse mix of workplaces was included, with selection based on factors such as size and age of WA Health facilities. A hospital site was selected from each HSP as an exemplar (see Table 1). These sites represented both large tertiary hospitals and smaller non-tertiary hospitals.

<table>
<thead>
<tr>
<th>HSP</th>
<th>Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>Child and Adolescent Health Service</td>
<td>Princess Margaret Hospital</td>
</tr>
<tr>
<td>East Metropolitan Health Service</td>
<td>Armadale Hospital</td>
</tr>
<tr>
<td>North Metropolitan Health Service</td>
<td>Sir Charles Gairdner Hospital</td>
</tr>
<tr>
<td>South Metropolitan Health Service</td>
<td>Fiona Stanley Hospital</td>
</tr>
<tr>
<td>WA Country Health Service</td>
<td>Northam Hospital</td>
</tr>
</tbody>
</table>

Health Support Services (HSS) was included as it acts as a systems provider and administrator for core or enterprise systems used by WA Health. HSS performs a number of functions which require access to confidential patient information.

The number of information systems in WA Health necessitated a sampling approach in considering physical and technical controls. In consultation with WA Health, iSoft Clinical Manager (iCM) was identified as a suitable focus system because:

- it stores pathology results
- it is used across all HSPs
- it has a large number of active users (approximately 22 000)
- it is a well-established system in WA Health.
Health reform context

While the HSPs were established as legal entities on 1 July 2016, the individual hospitals and health service sites comprised a range of health services prior to this date. There were re-arrangements of administrative and structural arrangements in the years leading up to the introduction of the Health Services Act 2016 (HS Act), in addition to the changes arising through the HS Act.

Each HSP has unique circumstances, with respect to size, geographic spread and duration of establishment prior to the new legislation. For this reason, they are not uniformly developed from a governance perspective. In undertaking this review, the Commission acknowledged the relative recency of the changes to WA Health and that HSPs could be at different stages of development and governance maturity with respect to the different factors considered.
Approach taken in the review

This section of the report discusses the methodology applied in conducting the review. The review was split into three distinct phases.

1. **Consultation phase:**
   - Initial consultation with the Department of Health (the Department), HSPs and HSS regarding the nature and scope of the review.
   - Refinement of the project scope.

2. **Assessment phase:**
   - Collection of documents and information provided by WA Health.
   - Interviews with key employees at the Department, HSS, HSP corporate areas and selected HSP hospital sites.
   - Follow up interviews and requests as required of specific staff to provide clarification and further information.
   - Analysis of all information and evidence provided.
   - Consultation with HSPs about preliminary findings.

3. **Reporting phase:**
   - Finalisation of an assessment summary for each HSP.
   - Drafting of this report.

Assessment methodology

The Commission assessed the maturity of arrangements for managing confidential patient information in WA Health against four preconditions (see Table 2).
Table 2: The preconditions for protecting confidential patient information

<table>
<thead>
<tr>
<th>Precondition</th>
<th>Focus area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right culture</td>
<td>Leadership commitment</td>
<td>The HSP communicates and models leadership commitment to patient confidentiality</td>
</tr>
<tr>
<td></td>
<td>Culture of engagement</td>
<td>Employee perceptions and behaviour demonstrate a broad commitment to patient confidentiality across the HSP</td>
</tr>
<tr>
<td>Robust decision-making framework</td>
<td>Accountability</td>
<td>Roles and responsibilities for managing confidential patient information are clearly defined and appropriately assigned</td>
</tr>
<tr>
<td></td>
<td>Guiding behaviour</td>
<td>Policies and procedures guide employees regarding patient confidentiality</td>
</tr>
<tr>
<td>Strong capability</td>
<td>Employing for integrity</td>
<td>Personal integrity is sought and reinforced through employment practices</td>
</tr>
<tr>
<td></td>
<td>Workforce knowledge and skills</td>
<td>Capability is managed such that employees have the skills and knowledge to maintain patient confidentiality</td>
</tr>
<tr>
<td>Good governance</td>
<td>Risk management</td>
<td>The risk of a breach of patient confidentiality has been identified and assessed</td>
</tr>
<tr>
<td></td>
<td>Physical and technical controls</td>
<td>There are physical/technical controls to protect against and detect any breaches of patient confidentiality</td>
</tr>
<tr>
<td></td>
<td>Continual improvement</td>
<td>There are corporate monitoring and reporting activities to help inform improvements in patient confidentiality</td>
</tr>
</tbody>
</table>

An assessment was made of the extent to which arrangements within WA Health indicated a mature approach to managing confidential patient information. Table 3 shows the maturity levels applied in the review.

Table 3: Maturity levels

<table>
<thead>
<tr>
<th>Maturity level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded</td>
<td>Systems to manage integrity risks are strategic and joined-up. All roles carry key responsibilities and there is ongoing monitoring of the effectiveness of controls by the executive/board that informs any systems improvement.</td>
</tr>
<tr>
<td>Managed</td>
<td>Systems are formally compliant. Particular roles formally carry key responsibilities and there is some regular tracking of controls to inform systems improvement.</td>
</tr>
<tr>
<td>Defined</td>
<td>There are examples of formal compliance. Particular roles are specified as carrying key responsibilities (but may not in practice) and monitoring of controls is generally responsive in nature to inform systems improvement.</td>
</tr>
<tr>
<td>Developing</td>
<td>Systems are largely ad hoc. Key responsibilities are scattered across various roles and there is minimal monitoring of controls. Systems improvement activities are random.</td>
</tr>
<tr>
<td>Undeveloped</td>
<td>Few or no systems are in place. A single role carries key responsibilities and there is no monitoring of controls or systems improvement activities.</td>
</tr>
</tbody>
</table>

The review took into account the maturity of each HSP’s practices relative to the review framework. The assessments for the individual HSPs were moderated to ensure consistency in the overall assessment.
The state of information management in WA Health

The introduction of the HS Act on 1 July 2016 provided for a legal framework with clear roles, responsibilities and accountabilities at all levels and a devolved governance model for WA Health (see Figure 2).

Figure 2: WA Health structure, 2016/17

The following elements\(^1\) have been established:

- The Department, led by the Director General, as the ‘system manager’, responsible for the overall management, performance and strategic direction of the WA public health system to ensure the delivery of high-quality, safe and timely services.
- The HSPs as separate board-governed statutory authorities, legally responsible and accountable for the delivery of health services for their local areas and communities.
- HSS as a chief executive-governed statutory authority that is accountable for the delivery of key support services.

---

\(^1\) Adapted from the Health reform fact sheet: The role of the Department of Health and WA Health’s ‘Establishing an effective system manager’ discussion paper.
The cascading policy framework in WA Health

The operating levels

Three key 'operating levels' in WA Health contribute to the policy framework for the management of confidential patient information:

1. System manager

The HS Act provides for mechanisms for the Minister for Health and the system manager to set standards and manage the governance and performance of the HSPs. The system manager may issue binding policy frameworks to HSPs 'to ensure consistent approaches to…the management of information, including the way in which information is collected, used and disclosed.' These binding policies operate across WA Health.

The HS Act requires the Department to 'establish and maintain systems for the collection, receipt, storage and disclosure of, and access to, health information.' The Act also prescribes the information to be held in a health information management system, who can have access and how it may be disclosed. There are specific provisions for confidentiality and authorised collection, use or disclosure.

2. HSPs

HSPs as legal entities in their own right also set their own service-wide policies and procedures to complement and provide further detail on system-wide policies. Under the HS Act, they 'have the function to develop and implement corporate…arrangements for the HSP.'

3. Hospitals/sites

At the hospital or site level, there may be policies and procedures developed to complement health service-wide and system-wide policies.

The framework

This cascading system of policies and procedures forms the framework to be applied. The system-wide policies take precedence over the health service-wide policies, which in turn take precedence over the hospital or site level policies.

Since the introduction of the HS Act, the Department has progressed the refinement of its policy frameworks to reflect its role as system manager. This involves articulating standards which must be followed and reported on by all HSPs and ensuring the appropriate level of prescription. The practical effect is for the system manager to transition to setting the overall direction with limited involvement in operational policies, which are set at the HSP level.
WA Health responsibilities for information management

Responsibility for the management of confidential patient information is shared across WA Health. The Data stewardship and custodianship policy sets out the following responsibilities for protecting data confidentiality, integrity and availability:

- Data stewards have overall accountability and responsibility, including managing risks; approving conditions for use and disclosure; and setting the strategic direction for data collection.
- Data custodians are responsible for the day-to-day and long-term management of data. This encompasses data collection planning, management and production; and data access, use and disclosure.
- HSS manages many of the applications that are integral to collecting data. HSS assists with the management of WA Health's information and communication technology hardware, infrastructure, applications and website and also implements technical safeguards to protect information and minimise the risk of unauthorised access or use.
- Authorised users are required to maintain agreed standards, use data for approved purposes only, and maintain confidentiality and security of information in accordance with conditions of use, legislation and policy frameworks.

The data stewards and custodians are usually Department or HSS leaders for core or enterprise systems and HSP-equivalent leaders fill these roles for local systems.

Other key information management policies within WA Health are:

- **WA Health information management strategy 2017-2021**
  
  This strategy sets out the vision and direction for health information management. It has priorities for the next five years, in the areas of governance, workforce, policies and standards, consumers, carers and the community, current and future requirements, and investment.

- **WA Health information management policy framework**
  
  This framework contains clear principles that underpin the collection, disclosure, disposal, governance, storage, and usage of health information and clearly addresses the confidentiality of information.

- **WA Health code of conduct**
  
  The code applies to all WA Health employees. It emphasises confidentiality, outlines a process for reporting suspected breaches of the code and references the potential consequences of a breach.

Other key WA Health policy documents, external requirements and relevant reports are provided in the Appendix.
Factors affecting information management

Managing confidential information is becoming increasingly complex with the digitisation of data. This is particularly true for health information, where a significant amount of personal and sensitive data is stored across thousands of discrete and integrated information systems. This presents significant challenges for WA Health.

A number of background factors which impact the management of information in WA Health are discussed below.

Number of information systems

Across WA Health, there are more than 11,000 core and shared information systems. These systems were purchased at different points in time and, as such, they may have substantially different features and functionality. The interaction between these systems creates a complex web of information management arrangements. For example, there are differences in user access monitoring and audit capability between iCM and another WA Health clinical information system, BOSSnet.

Security of technology

Notwithstanding the rapid pace of improvements in technology, the cost of upgrading information management systems can be prohibitively expensive. Financial constraints mean that upgrades and replacements may be postponed, resulting in legacy systems with potentially less sophisticated mechanisms to detect or combat breaches in patient confidentiality.

Operating conditions

Patient information may be accessed and used under a variety of workplace conditions and in a number of work environments. For example, a doctor accessing a clinical information system in an emergency department is likely to require different access to that of information and communications technology staff accessing a data warehouse.

Privacy interests

Health staff and patients demonstrate a spectrum of requirements for patient confidentiality. Clinicians and patients in need of medical attention may favour more open arrangements around patient information, with health outcomes viewed as more important than maintaining individual privacy. This is balanced with limiting access to sensitive information in order to reduce the risk of unauthorised access and disclosure.

Risk management

Information management is more than technology—it is underpinned by a range of business practices. The size and complexity of health information systems means that fully identifying and assessing the potential risks associated with managing confidential patient information can be complicated.
Observations and suggested improvements

This section of the report discusses observations made from an assessment against the Commission’s framework for managing confidential patient information.

The right culture

In assessing culture and leadership, the review sought to observe strategic integrity initiatives for building and testing the cultural climate with respect to managing confidential patient information across WA Health. The review focused on proactive organisational communication and monitoring of staff behaviour and awareness of obligations and responsibilities.

Leadership commitment

Clear and consistent messages from leaders that demonstrate a commitment to confidentiality are essential to building a culture of integrity. The review considered general integrity messages by leaders as well as evidence of specific means of communicating and modelling a commitment to maintaining patient confidentiality.

A workforce that does not value patients’ privacy or is unaware of relevant obligations is more likely to inappropriately access, use or disclose information. Likewise, if an organisation’s leadership is unaware of breaches of confidentiality—or does not communicate its expectations—it is more likely that staff will see unauthorised access and disclosure as permissible behaviour.

A strong leadership commitment to promoting the right culture was evident in all HSPs. The specific observations made during the review in relation to this focus area were that:

- the *WA Health information management strategy 2017-2021* sets out the vision for a system that protects patient confidentiality
- there was reference to organisational values in strategic plans, patient charters, posters and pamphlets displayed in public areas and other HSP-level documents
- in many cases, all-staff emails and newsletters from the HSP chief executives communicated the importance of integrity in general (and were disseminated through WA Health management levels and across geographic locations)
- the obligation to protect patient confidentiality had been communicated in some cases as part of a response to breaches of confidentiality (there was less evidence of proactive and targeted reminders of obligations to prevent breaches).

Culture of engagement

Monitoring organisational culture and staff behaviour helps understand issues associated with unauthorised access and disclosure of confidential patient information. Staff surveys are a common means of gauging perceptions but other strategies can be applied. Leaders and managers may also use other methods such as agenda items at team
meetings, or informal discussions with employees. Consideration of any relevant issues arising from feedback or complaints processes can also provide insight into staff behaviour and attitudes.

While understanding employee commitment to maintaining patient confidentiality does not predict employee behaviour, it does help inform the nature, scope and necessary frequency of staff awareness and knowledge raising programs. Such knowledge can also contribute to planning and the implementation of risk mitigation processes.

Most HSPs were observed to have some means of assessing employee attitudes and awareness, although not in relation to the specific topic of managing confidential patient information. Specific observations made during the review were that:

- several HSPs ran staff surveys (separate to the Commission’s own employee perception survey program)
- where surveys were undertaken, they typically included a few questions regarding integrity or misconduct issues, although none specifically referred to patient confidentiality issues
- HSPs can generally rely on employee professional standards in the health sector as underpinning a respect and responsibility for patient confidentiality (however, this may mean less attention to formally seeking assurance of employees’ ongoing commitment to confidentiality)
- overall, there was a small number of allegations made regarding breaches of patient confidentiality
- where breaches were substantiated, sanctions typically took the form of a written warning.

**Suggestions for improvement**

Given the announcement made on 12 October 2017 by the Minister for Health regarding a new dedicated employee engagement program for WA Health, some HSPs have refrained from introducing their own surveys. Nevertheless, monitoring employee perceptions and attitudes remain important.

The areas within the Department of Health and HSPs with broader responsibility for employee perception surveys may wish to liaise with the Commission on the inclusion of relevant questions to test employee perceptions of the commitment to patient confidentiality and misconduct reporting.
Suggestions for improvement
In relation to ‘the right culture’, the Commission suggests that WA Health:

- ensure leaders’ expectations in relation to confidential patient information are regularly communicated and reinforced to staff
- regularly test perceptions of the commitment to patient confidentiality and misconduct reporting
- where breaches of patient confidentiality occur, ensure sanctions are appropriate to the seriousness of misconduct.

Robust decision-making framework
In assessing the decision-making framework, the review observed how employees are guided to make appropriate choices when interacting with confidential patient information. Focus areas were the appropriate assignment of accountabilities for key roles, clearly laid out and accessible policies and procedures, and the implementation of WA Health’s Data stewardship and custodianship policy.

Accountability
Assigned roles and responsibilities are crucial to the effective administration of system priorities and policies. Legislative obligations may provide the foundation for accountability, supported by mandatory system-wide policies. Organisational networks associated with particular roles and responsibilities can assist to disseminate key messages, support good practice and monitor compliance with policy frameworks.

Roles and responsibilities were generally well articulated in the system-wide and HSP-level policy frameworks. Some HSPs performed more strongly in this area, showing increased awareness of relevant frameworks and recent reviews of roles and responsibilities. Specific observations made during the review were that:

- the roles and responsibilities for the management of confidential patient information are well described in WA Health policies and procedures
- most HSPs had a documented overarching framework, such as an ‘Integrity and ethical governance framework’
- the roles of data stewards and custodians, as outlined in the Data stewardship and custodianship policy, was not widely understood (some HSPs reported difficulties in applying aspects of the policy and some officers in relevant roles appeared not to be fully aware of their responsibilities under the policy)
- in general, ethics and integrity staff managed allegations and investigated misconduct, including alleged breaches of patient confidentiality (there was less capacity for proactive misconduct prevention and education work outside of reacting to ‘spot fires’)
- one HSP was observed to use health information management networks to disseminate and embed good practice in information management (including confidential patient information) as a key part of follow-up on audit and assurance activities.
Guiding behaviour

Policies and procedures guide employees at all levels of an organisation to appropriately manage confidential information. These should be easy to understand and apply in various operating contexts, and be accessible to employees in different work locations.

An important avenue for detecting inappropriate access of confidential patient records is misconduct reports and complaints. These require staff and patients to be adequately informed about confidentiality provisions and aware of how to lodge a report or complaint. Therefore, organisations have to put in place accessible avenues for reporting suspected breaches.

It was evident in all HSPs that the policy and procedural framework provides comprehensive guidance to employees in managing confidential patient information. Specific observations made during the review were that:

- WA Health has a comprehensive suite of policies covering management of information in general and the protection of patient confidentiality in particular
- the WA Health code of conduct applies to all HSPs and contains specific provisions to help safeguard patient confidentiality
- internal WA Health systems provided for misconduct reports to be made by staff (however, it was observed that public-facing avenues to report misconduct were less well advertised).

Suggestions for improvement

In relation to a ‘robust decision making framework’, the Commission suggests that WA Health:

- continue to improve awareness and understanding of the *Data stewardship and custodianship policy* and the responsibilities of data stewards and custodians
- maintain awareness of accessible avenues for staff to report alleged breaches of patient confidentiality
- ensure avenues for patients to make complaints about breaches of patient confidentiality are well-publicised.

Strong capability

In assessing capability, the review sought to observe staff being actively trained and educated to maintain patient confidentiality. Focus areas were staff recruitment for ‘positions of trust’ (as described in the Commission’s 2017 evaluation report, *Integrity checking of employees managing misconduct allegations*) and staff training programs.

Employing for integrity

Integrity checking of employees is important to ensure the risks of misuse of confidential patient information are minimised. Checks are primarily conducted at the
pre-employment phase and also during employment as required. Any ‘positions of trust’ may require additional checks and balances to appropriately respond to risks associated with the positions.

Due to the WA Health-wide requirement for checking personal integrity of staff, HSPs were observed to have mature systems in this focus area. Some performed even more strongly due to customised risk treatments, applied particularly to non-clinical staff with access to datasets. Specific observations made during the review were that:

- WA Health conducts pre-employment checks, including criminal record screening, as a condition of employment
- some HSPs had strengthened controls for positions of trust by ensuring completion of annual confidentiality agreements (however, there was limited attention to repeating checks during the employment period).

**Workforce knowledge and skills**

A skilled and knowledgeable workforce is more capable of making appropriate decisions in the course of day-to-day work. It is important that staff are regularly provided with contemporary information on integrity through multiple pathways. Policies and guidelines related to integrity matters, such as the ‘Accountable and ethical decision making’ (AEDM) program should be a key part of employee induction and ongoing training. Such programs communicate the importance of acting with integrity and promote understanding of what this involves in the context of the agency’s business and conduct risk. The Commission makes one-hour refresher session materials available to public sector entities that wish to revisit key AEDM messages with employees who have already completed the full program.

In addition to AEDM training—delivered both as face-to-face and online—there are other resource efficient mechanisms for delivering integrity education to reinforce relevant policies and procedures, such as:

- communication from the chief executive officer or other senior leaders, such as regular or ad hoc messages
- regular discussion at team meetings
- posters or messages in the workplace
- performance discussions.
HSPs did not perform as strongly in this focus area due to a lack of repeated and targeted education and training for employees. Other observations made during the review were:

- routine training programs with integrity content included induction and the mandatory one-off AEDM program
- AEDM completion rates were relatively high across all HSPs
- the existing training load and operational requirements were observed to present challenges to any introduction of widespread additional or refresher training
- some HSPs had been able to provide additional specific training to all staff that encompassed obligations for patient confidentiality (such as records awareness training), as part of their response to a breach of confidentiality.

**Suggestions for improvement**

In relation to ‘strong capability’, the Commission suggests that WA Health:

- enhance risk management controls for positions of trust that access and manage confidential patient information (such as regular integrity checks or confidentiality agreements)
- implement repeated training and education for all staff, such as an AEDM refresher course, that covers obligations for the protection of patient confidentiality.

**Good governance**

In assessing governance, the review observed what arrangements were in place to manage and mitigate risks; physical and technical barriers to misuse of confidential patient information; and the various audit and oversight activities undertaken with respect to management of patient confidentiality. A key focus of the review was ‘closing the loop’ through evaluation and improvement activities.

**Risk management**

The specific attention to confidentiality of information within a risk management framework helps to reduce the risk of breaches of confidential patient information. Such consideration might include, amongst others, the consideration of routine workplace practices and physical work areas.

Some opportunities for improvement were identified in the HSPs for this focus area. Specific observations made during the review were that:

- HSP-level audit and risk management committees were observed to be in place
- the risks of staff misconduct and information and communications technology issues (such as cybersecurity) were generally covered in HSP risk registers
- the specific risk of a breach in patient confidentiality was less well recognised.
Physical and technical controls

Physical and technical controls can protect against and detect any breaches of patient confidentiality. However, it is acknowledged that the type and sophistication of these controls are affected by the operating environment and the resources available to develop and implement these controls.

The review considered a range of these controls at the HSP and site levels, with a primary focus on the iCM system for the assessment. Specific observations made during the review were that:

- all HSPs had security controls in place for physical access to patient records, such as swipe cards, covered transport methods and confidential bins
- there were some controls inherent in the iCM system, such as passwords, idle logouts and reminders
- a limitation in the iCM system’s ability to detect and monitor unauthorised access of information was observed.

Due to the restrictions in auditability of the iCM system, this focus area was not further assessed in the review.

Continual improvement

Corporate monitoring and reporting activities help inform improvements in practices surrounding patient confidentiality. Such activities may include audits and evaluations and reporting to the executive on breaches of discipline.

Continual improvement activities were a feature of all HSPs. Some performed better due to targeted audits of arrangements to manage confidential patient information and detailed reporting to the board. Specific observations made during the review included:

- most HSPs had an ethical conduct review committee in place to oversight misconduct matters
- there was generally some form of regular reporting to the board on misconduct cases, statistics and trends (one HSP was observed to undertake comprehensive ‘dashboard’ reporting and monitoring of implementation of action items)
- accreditation programs were a significant part of continual improvement activities
- some HSPs had scheduled or conducted specific audits into the management of confidential patient information.
Suggestions for improvement

In relation to ‘good governance’, the Commission suggests that WA Health:

- formally assess the risk of breaches in patient confidentiality
- continue working to improve misconduct detection and monitoring capability in information systems like iCM
- ensure detailed reporting of misconduct trends to relevant boards to enable a proactive response to emerging issues
- implement regular audits of the framework and policies relating to patient confidentiality and related processes (e.g. data breach response) relevant to their respective roles within the system.
Appendix – Relevant policies, requirements and reports

WA Health policies

Policies and frameworks within WA Health which provide guidance on the management of confidential patient information include:

- Acceptable use of information and communications technology policy (MP 0066/17)
- Criminal record screening policy
- Data breach response policy (OD 0564/14)
- Digitisation and disposal of patient records policy (OD 0583/15)
- Disposal of information & communications technology (ICT) equipment and data storage media
- Guidelines for the release of data
- Information classification policy (OD 0537/14)
- Information lifecycle management policy
- Information security policy (MP 0067/17)
- Information use and disclosure policy (MP 0015/16)
- Patient confidentiality policy
- Personally controlled electronic health record (PCEHR) system policy (OD 0463/13)
- Pre-employment integrity check policy (MP 0032/16)
- Security protocols and ongoing management of digitised patient records
- WA Health code of conduct
- WA Health information management strategy 2017-2021

WA Health reviews and activities

There are a number of reviews and programs relevant to the management of confidential patient information by WA Health, which are listed below.

Sustainable Health Review

Commissioned by the WA Government, the Sustainable Health Review (SHR) is currently in progress. Its purpose is to provide advice to Cabinet to help guide the delivery of patient-centred, integrated, high quality, and financially sustainable healthcare across WA. The SHR panel is supported by clinical and consumer reference groups. While not a specific focus of the SHR, the two groups have considered the issue of information management. With respect to data sharing, the groups found that ‘both consumers and clinicians agreed that increased information sharing could have positive
effects on the delivery of care and patient outcomes if done in a secure environment. The groups discussed building on existing initiatives, privacy for consumers, and the need for integrated systems.²

Review of safety and quality in the WA health system

Safe, reliable healthcare depends on access to, and the use of, information that is transparent, timely, reliable and attributable. The 2017 Review of safety and quality in the WA health system found that the WA health system should move towards greater transparency and a presumption in favour of publication at all times.

Office of the Auditor General

In November 2015, the Office of the Auditor General published an Information systems audit report. This contained the results of an audit conducted in seven agencies of database security. The databases audited were critical to agency functions and held personal and sensitive information. WA Health was one of the sample agencies and a patient administration system was one of the systems chosen for audit.

External standards

WA Health policies also reference various national standards. These are described below.

National safety and quality health service standards

The National safety and quality health service standards (NSQHS Standards) are issued by the Australian Commission on Safety and Quality in Health Care. It is mandatory in WA for all public hospitals to achieve and maintain accreditation status to these standards. The principles and content of the standards were strongly reflected in the WA strategic plan for safety and quality in health care 2013-2017.

There are 10 standards, with the first two covering governance and partnering with consumers. These set overarching requirements for effective implementation of the remaining eight standards, which address specific clinical areas of patient care.

The governance standard specifically refers to patient confidentiality under the criterion ‘Patient rights and engagement’. It is achieved through ‘implementing procedures that protect the confidentiality of patient clinical records without compromising appropriate clinical workforce access to patient clinical information’. Action to achieve this requires that ‘systems are in place to restrict inappropriate access to and dissemination of patient clinical information’.³

More broadly in relation to the management of confidential patient information, the governance standard refers to ‘accurate, integrated and readily accessible patient clinical records’ and outlines broader systems and structures for safety and quality, such as

³ Standard 1, item 1.19.
policies, procedures and protocols; executive oversight; risk management; and workforce roles, responsibilities and accountabilities.

In addition to evaluation activities undertaken at the HSP level, HSPs are evaluated against the standards through external accreditation programs. The documentation from these accreditation programs was supplied by some HSPs to the Commission as part of the review.

**Other health standards**

The core NSQHS Standards are complemented by non-mandatory standards developed by other bodies. For example, the Australian Council on Healthcare Standards, an agency accredited to assess health services to the NSQHS Standards, has developed an additional **five standards**. One of these, Standard 14, specifically relates to information management.

In addition to assessment against the 10 NSQHS Standards, some HSPs have undergone assessment against these non-mandatory standards.

**International and Australian Standards**

While several Australian and international standards could be considered relevant to this review, the most closely related are the **27000 series of standards** and, in particular, **AS ISO/IEC 27001:2015** and **AS ISO/IEC 27002:2015**. These standards provide organisations with comprehensive guidance and a toolkit to develop an effective risk management framework for information management.

**AS ISO/IEC 27002:2015** has broader application than technical controls, such as ensuring that appropriately structured and implemented policy frameworks are in place, the acquisition and maintenance of technology is appropriate for an organisation’s current and future business needs, and that information security incidents are responded to effectively.

**Related documents and further information**

**Privacy principles**

The Office of the Australian Information Commissioner (OAIC) and the Privacy Commissioner have carriage of several functions related to the **Privacy Act 1988** (Privacy Act).

The 13 **Australian Privacy Principles** (APPs) in the Privacy Act outline requirements placed upon ‘APP entities’. While WA Health is not bound by the Privacy Act, the APPs still provide a useful point of reference. The following APPs are considered most relevant to the review’s subject matter:

- APP 1: open and transparent management of personal information
- APP 3: collection of solicited personal information
- APP 6: use or disclosure of personal information
• APP 11: security of personal information
• APP 12: access to personal information.

In order to assist APP entities to comply with their Privacy Act requirements, the OAIC has published a number of useful documents which provide prompts, examples and case studies.

**Productivity Commission report**

A report published by the Australian Productivity Commission in March 2017, entitled *Data availability and use – Productivity Commission inquiry report no. 82*, outlines potential costs and benefits surrounding information sharing, with specific reference to health information. Some key points are:

• the creation of a data sharing and release structure that indicates a strong and clear cultural shift towards better data use is central to the proposals made in the report
• it is vital that the principles of openness and transparency are translated into the use of health information, noting there is often greater concern around the sharing of health information
• marginal changes to existing arrangements do not adequately change the risk aversion and avoidance dynamic to one of transparency and confidence in data processes
• data should be treated as an asset rather than a threat.