Health Information Governance Framework

PRIMARY HEALTH TASMANIA

December 2017

V 1.0

An Australian Government Initiative

Contents

Author	Planning and Evaluation Team, PHT
Authorised by	Chief Executive Officer
Date	15 December 2017
Internal/external dissemination	Internal/External

Primary Health Tasmania
t: 1300 653 169
e: info@primaryhealthtas.com.au
www.primaryhealthtas.com.au

Australian Government

phn TASMANIA
An Australian Government Initiative

While the Australian Government helped fund this document, it has not reviewed the content and is not responsible for any injury, loss or damage however arising from the use of or reliance on the information provided herein.

Glossary

Data custodians	The person responsible for, or the person with administrative control over, granting access to a data collection
Health information	Information or an opinion about: (i) the health or a disability (at any time) of an individual; or (ii) an individual's expressed wishes about the future provision of health services to him or her; or (iii) a health service provided, or to be provided, to an individual that is also personal information; or (b) other personal information collected to provide, or in providing, a health service; or (c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or (d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual
Information governance	The specification of decision rights and an accountability to ensure appropriate behaviour in the creation, storage, use, archiving and disposal of information. It includes the processes, roles and policies, standards and metrics that ensure the effective and efficient use of information in enabling an organisation to achieve its goals.
Risk assessment	A systematic process of evaluating the potential risks that may be involved in a projected activity or undertaking.
Risk management	The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, assessing, treating, monitoring and communicating

1. Preface

Primary Health Tasmania (PHT), has an important health intelligence function to support the planning, implementation and evaluation of initiatives aimed at improving system efficiency and effectiveness and health outcomes for Tasmanians.

As part of this role, PHT accesses and uses a range of administrative data sets, clinical data sets and service provider data.

To maximise the privacy and maintain confidentiality, integrity and availability of health information used by PHT, the organisation has recognised the need for a consistent approach to good information governance which demonstrates all PHT data users understand, prioritise and manage risks associated with data transmission, access, use, storage and disposal.

The PHT Health Information Governance Framework has been designed to:

- Clearly articulate requirements, standards and best practices that apply to the handling of health information, including but not limited to personal information, by PHT and its contracted and commissioned organisations; and
- Enable contracted and commissioned organisations to identify and manage individual risks with a checklist for achieving the requirements for health information governance expected by PHT.

This document forms the framework and is intended to inform and direct data custodians, policymakers, contracted and commissioned organisations and PHT's staff and governance bodies about the approach PHT is taking in regard to health information governance.

Focus

The framework is directed at ensuring that PHT health information infrastructure and resources adopts best practices for the protection of privacy of health information and complies with all applicable law.

The framework explains the processes that support high quality information governance and provides guidance on implementation through references to applicable information security standards.

The objectives are to clearly articulate a Health Information Governance Framework that covers:

- A systematic approach to safeguarding all personal information relating to data collection, collation, analysis and dissemination by PHT and its contracted and commissioned organisations;
- The use and storage of data upon supply to PHT by contracted and commissioned organisations and data custodians; and
- People, processes, IT systems, information and physical assets.

Key areas of the framework include:

- Roles and responsibilities;
- Risk assessment and risk management;
- Audit, reviews and reporting;
- Incident and breach management;
- Awareness, education and training;
- Compliance; and
- Implementation guidance.

Audience

The content of the framework is aimed at those with information governance responsibilities within PHT and within service delivery and other organisations contracted or commissioned by PHT. The overall approach to information governance is of interest to the general public, custodians and data users alike; therefore the framework provides the opportunity to demonstrate how PHT communicates the security requirements for all health data.

Review

The framework will be reviewed at least annually, to take into account elements such as developments in information governance and security standards, legislative and regulatory requirements, and the risk profile of PHT.

2. Introduction

The PHT Health Information Governance Framework has been developed to articulate PHT's requirements and outline best practice in health information governance.

Best practice has been established from international and national security standards for information security, privacy and risk management with specific reference to:

- ISO/IEC 27001:2005 Information Security Management Systems Requirements;
- ISO/IEC 27002:2005 Information Security Management Systems Code of Practice;
- ISO/IEC 27005:2008 Information Security Risk Management;
- ISO/IEC 31000:2009 Risk Management Principles and Guidelines;
- ISO/IEC 31010:2009 Risk Management – Risk Assessment Techniques;
- Australian Government Information Security Manual (AGISM);
- Australian Government Protective Security Policy Framework (PSPF).

PHT has recognised the need to create a health information governance framework to support these principles.

Definitions

Information governance can be best described as an accountability framework which controls the manner in which information is obtained, handled, used and disclosed.

In the context of PHT, information governance encompasses organisational structures, roles and responsibilities, standards, and compliance activities to ensure that information related to data linkages is dealt with legally, securely, efficiently and effectively, whilst providing the best possible service to stakeholders.

As such, information governance encompasses people, processes, information technology (IT) systems, information and physical assets that support the health intelligence activities of PHT.

Objectives

The key objectives of the PHT Health Information Governance Framework are to:

- Guide the development and management of health information governance throughout PHT and its contracted and commissioned organisations;
- Ensure PHT personnel adhere to high quality information governance practices when receiving health information from contracted and commissioned organisations and data custodians, and when providing health information to contracted organisations;

- Inform PHT's contracted and commissioned organisations of PHT's information governance requirements for health information governance; and
- Provide assurance to data custodians that PHT personnel and its contracted and commissioned organisations apply appropriate information governance when handling health data, including related personal information.

The framework is intended to complement rather than surpass any existing information governance or security requirements of data custodians or information governance arrangements of PHT contracted organisations and provide a mechanism for PHT to assess its own and its contracted and commissioned providers compliance against information governance requirement.

Scope of the Health Information Governance Framework

The scope of the Health Information Governance Framework is to provide a systematic approach to safeguarding all personal information and health data utilised by PHT in its health intelligence activities.

The framework scope includes:

- All PHT personnel and contracted organisations involved with health information;
- The Board of PHT and all related subcommittees;
- Physical premises, systems, applications and equipment used by PHT personnel and contracted organisations for health data collection, collation and analysis activities;
- Transfer of health information into/out systems between PHT and other parties;
- Management and storage of health information;
- Use of health information by end users; and
- Execution, management and monitoring of contractual and other agreements covering information governance with external organisations.

Roles and Responsibilities

Operational responsibility for managing information governance resides with all PHT personnel and contracted and commissioned organisations.

PHT personnel are expected to familiarise themselves with this Framework and operate in accordance with the information governance standards described herein.

PHT personnel and contracted and commissioned organisations should have an understanding of PHTs requirements regarding:

- information governance principles and practices;
- security management principles and practices;
- risk management; and
- legislation governing the use and disclosure of information.

Additional PHT Planning and Evaluation team roles may be identified to support PHT employees and / or contractors that cover:

- information and records management;
- information security;
- risk management;
- compliance.

Compliance with the Health Information Governance Framework

Compliance is measured by the degree to which health information governance is managed by PHT personnel and contracted organisations in accordance with this Framework.

Achievement and maintenance of compliance relies strongly on the process of risk management in order to monitor the gap between existing practices and the framework. The aim is to reduce the gap to zero and maintain it at that level.

Roles and Responsibilities

PHT Planning and Evaluation Team provides advice and guidance where necessary to assist PHT personnel and contracted or commissioned organisations to achieve compliance.

PHT personnel and contracted or commissioned organisations are responsible for the implementation and management of information governance and security controls that are relevant to their individual risk assessment and management program.

PHT contracted or commissioned organisations are required to provide evidence of compliance with the PHT Health Information Governance Framework to the Planning and Evaluation Team on an annual or project basis (where projects are less than 12 months in duration).

PHT recognises that, in some instances, PHT contracted or commissioned organisations may be able to place some reliance upon existing information management and security policies, practices, processes and infrastructure of their host organisation.

PHT and its contracted or commissioned organisations should ensure that:

- people with access to health information are aware of what may be considered an information governance incident and to whom an incident must be reported; and
- remedial action is quick and effective.

To support effective information governance incident management, contracted organisations must have the following processes in place:

- maintenance of an incidents log to record the assessment, management and resolution of incidents; and
- investigation of root cause analysis of incidents and corrective action to address the root cause.

3. Risk Assessment and Risk Management

Without an understanding of risks to information assets, PHT cannot be sure that the measures that are applied to protect those assets are justified or effective.

Information asset identification and classification together with risk assessments are essential in building an effective Health Information Governance control structure within PHT.

Information Assets and Classification

Information identification and classification is an input to the risk assessment process and ensures that risk assessments are focused on assets of most value to PHT. Information assets are identified and classified according to their confidentiality, integrity and availability requirements.

An information asset is anything that is of value to PHT and contracted or commissioned organisations in enabling them to function, and includes:

- people (e.g. employees, contractors, third parties, data custodians, data users);
- information (e.g. policies, procedures, guidelines, knowledge);

- hardware (e.g. servers, desktops, laptops, tokens);
- software (e.g. encryption software, data linkage applications);
- facilities (e.g. offices, computer room, cabinets, data centre, utilities);
- intangibles (e.g. memberships, licenses, agreements).

The value of an asset is measured in terms of:

- confidentiality – what are the implications of a breach of confidentiality?
- integrity – how accurate and complete must the information be?
- availability – how quickly must the information be restored if unavailable? Within hours, days or weeks.

Best Practice

To ensure information risk analysis is conducted in a consistent manner, PHT uses a documented risk assessment methodology. Contracted and commissioned organisations may develop their own methodology or leverage a methodology that is already in place within PHT.

Key characteristics of the risk assessment methodology in place within PHT and that contracted and commissioned organisations **must** demonstrate are in place for sensitive health information provided to the contracted or commissioned organisation include:

- defined criteria for measuring likelihood and impact of risks related to data collection, collation, analysis and dissemination; and
- a consistent process of data access within contracted or commissioned organisations whereby personnel manage risks associated with access to data regardless of the characteristics of the person.

The results from information risk assessments are:

- recorded in the risk register maintained by PHT and that is required to be maintained by each contractor / contracted/commissioned organisation;
- regularly reviewed by senior management within PHT and is required to be reviewed by senior management in the contracted organisation;
- reported by the contracted organisation to PHT at a frequency determined by PHT; and
- used to determine remedial action and develop risk mitigation strategies.

Individuals conducting risk assessments within PHT and contracted or commissioned organisations have the following skill sets and competencies:

- understanding of risk assessment methodologies;
- interview techniques;
- ability to evaluate and calculate risk;
- understanding of security controls and selection of relevant risk mitigation strategies and recommendations; and
- good reporting skills.

Risk Assessment Model

There are various models available to guide the risk assessment process. The most effective in regard to information security are ISO 27005:2008 Information Security Risk Management and ISO 31000:2009 Risk Management Principles and Guidelines (used as the basis for PHT's risk management policy and procedures).

PHT has recognised the need for flexibility given the organisational requirements of individual contracted or commissioned organisations. Therefore, the methodology needs to be aligned to existing standards. Overall it is expected that the approach selected by contractors follows specific standard in risk management and is able to support the goals and objectives of PHT.

Following best practice in risk management, methodologies are to take into account the following:

- compliance requirements with legislation, regulation, contractual terms, industry standards and internal policies;
- objectives of PHT;
- information classification requirements;
- characteristics of the operating environment;
- identification of project participants' information assets to identify:
  - threats to those assets;
  - vulnerabilities that might be exploited by threats;
  - impacts that the loss of confidentiality, integrity and availability may have on the assets.

Risk Analysis

PHT uses the risk analysis methodology to help:

- select security controls that will reduce the likelihood of serious security incidents occurring;
- select security controls that will satisfy relevant compliance requirements;
- identify specialised security controls required by particular environments (e.g. when using Commonwealth data); and
- evaluate the strengths and weaknesses of security controls.

The following activities require a formal risk analysis:

- data linkage systems in the early stages of development;
- existing information and information processing systems;
- systems and technology required to support the transfer of data.

Risk Treatment

For any given risk, PHT and contracted organisations will identify how the risk is to be addressed. This may be one of the following:

Risk Treatment	Example
Avoid the risk	Stop doing the activity that creates the risk
Manage the risk (preventative and contingency actions)	Implement required controls to prevent and mitigate risk
Transfer the risk	Transfer risk to a third party (e.g. insurance) **NOTE**: This does not transfer ownership or responsibility of risk and must be managed accordingly.
Accept the risk	Accept the current exposure (e.g. this may be due to financial constraints

	or cultural differences) Accepted risks must be signed off by senior management within PHT and contracted organisations.

Ongoing Risk Assessment and Management

The ongoing monitoring of risk and countermeasures is vital in maintaining effectiveness of the selected controls. This is achieved through regular management reviews, supported by both internal and external audits.

Triggers for a change to the risk register will include:

- corrective actions arising from internal or external audits;
- updates in information governance or security standards;
- realisation of risk;
- discovery of a new threat;
- the emergence of a new vulnerability;
- a change to asset classification;
- introduction of new technology or assets.

Roles and Responsibilities

PHT is subject to annual internal risk assessment, conducted by the Public Health Physician, Planning and Evaluation Team, PHT, in conjunction with PHT ICT services as needed.

Contracted or commissioned organisations are required to provide PHT with documented risk assessments at a frequency determined by PHT. This risk assessment is required to detail the following:

- risk register;
- risk management decisions;
- accepted risks together with justification of acceptance;
- summary of security controls.

PHT will:

- verify that accepted risks have been signed off by appropriate personnel;
- acknowledge the improvement program (as required).

4. Audit, Reviews and Reporting Guidelines

PHT and its contracted or commissioned organisations are required to conduct regular self-audits to a defined schedule.

The objectives of the audits are to give assurance to PHT senior management and the PHT Board that PHT and contracted or commissioned organisations can demonstrate:

- processes and controls with respect to information governance are efficient and effective;
- business processes are complete and are being followed according to defined policies

and procedures; and

- privacy requirements are understood and applied by all staff handling personal information.

The Public Health Physician, Planning and Evaluation Team, PHT, has sufficient experience and knowledge of information governance and PHT objectives to administer audit processes.

Audit Program

To support the requirement for internal audit and security review, PHT and its contracted or commissioned organisations should have:

- an approved schedule for internal audit and security review;
- an agreed reporting structure for results; and
- defined roles and responsibilities for reporting and acting upon audit and review findings.

PHT and contracted or commissioned organisations are required to participate in regular self-audit activities and produce evidence on request of compliance with this Health Information Governance Framework, and to advise of any breaches in information security.

Reporting

Audit and review findings are reported back to management at the appropriate level within the individual contracted or commissioned organisation's organisational structure to ensure that any findings are acted upon in a timely manner.

Significant non-conformities are reported immediately to the Public Health Physician, Planning and Evaluation Team and escalated to the PHT Board as needed.

Identified deficiencies are used as inputs to the risk registers of contracted or commissioned providers to ensure corrective action is taken to improve the controls over information assets. Follow up activities record the actions taken and are verified.

Guidance

ISO 19011:2002 provides guidance on the management of audit programs, the conduct of internal audits and the competence and evaluation of auditors. This is a recommended approach where no existing framework for conducting internal audits has been established.

Section 6 of ISO 27001:2005 sets out the specific requirements for internal security audits.

Reviews

Internal security reviews should be conducted on an annual basis by PHT and contracted or commissioned organisations to gain assurance that security controls are efficient and effective. The Public Health Physician, Planning and Evaluation Team, PHT, will conduct the PHT security reviews as part of the annual health intelligence business planning process.

Reviews may take a number of forms as indicated by the table below, and will be supported through the use of self-assessment tools.

Type	Purpose	Approach
Gap analysis	Determine whether controls are adequate.	Map selection of required controls to existing controls to find gaps.

Metrics and Measurements	Assess whether controls are effective and improvements are achieving desired results. Assess controls covering third parties.	Review contractual agreements / key performance indicators
Capability Maturity Modelling	Assess maturity of controls over information.	Use defined criteria to measure the ‘maturity’ of controls, e.g. 1 = ad hoc implementation to 5 = fully implemented and measurable

5. Incident and Breach Management

Incident and Breach Policy Statement

The purpose of incident and breach management is to enable PHT to manage and respond to unexpected events with the key objective being to minimise the impact.

Incident management and response is crucial in maintaining stakeholder confidence in PHT and its contracted organisations.

The key objectives are to:

- detect incidents in a timely manner;
- contain and minimise damage;
- manage incidents effectively; and
- prevent recurrences.

Incident and Breach Reporting

PHT personnel and contracted or commissioned organisations should report to the Public Health Physician, Planning and Evaluation Team, PHT, any actual or suspected incidents that are likely to impact health information security.

The objective is to ensure that the potential impact of actual or suspected incidents is assessed, communicated and managed by PHT and its contracted or commissioned organisations in a timely manner.

6. Awareness, Education and Training

Education Principles

It is essential that all personnel processing personal information and sensitive health information understand the privacy and confidentiality requirements.

PHT and its contracted or commissioned organisations must ensure these personnel understand their professional obligations in relation to;

- information privacy requirements;
- roles and responsibilities with respect to information governance;
- introduction of relevant policies and procedures;
- reporting information governance incidents; and

- acceptable use of assets.

Where individuals have specific information management or privacy roles and responsibilities, they should be provided with education and awareness training commensurate to the level of responsibility assigned.

Education also encompasses appropriate levels of training for Human Research Ethics Committees and data users.

7. Aligned documents

Primary Health Tasmania will apply this framework to a range of existing relationships and agreements in place, including:

- Memorandum of Understanding with the Department of health and Human Services and Tasmanian Health Service, including the associated Data Sharing Agreement.
- Data Sharing Agreements with non-contracted providers
- Contracted provider service agreements
- Software licencing agreements (such as PenCAT)

Primary Health Tasmania
t: 1300 653 169
e: info@primaryhealthtas.com.au
www.primaryhealthtas.com.au