Performance reporting information security

1. Statement

Within the Department of Health, data is valued and is managed as a strategic asset to support delivery of health services while protecting personal and confidential information.

2. Purpose

This policy describes the mandatory steps to be undertaken in preparing performance reports and insight dashboards to protect 'personal information' and 'confidential information'.

3. Scope

This policy applies to all employees, contractors and consultants within the Department of Health divisions and commercialised business units; and all entities acting as its agent.

4. Principles

Key principles of performance reporting include increasing and maintaining transparency of how performance data is prepared and presented. A balance of increased transparency is a risk of disclosing 'personal information', as defined by Section 12 of the Privacy Act 2009, and disclosing 'confidential information', as defined by Part 7 if the Hospitals and Health Boards Act 2011.

In maintaining the transparency of performance information and maintaining the security of information to prevent identification of an individual the System Performance Branch undertakes the following actions:

1. Data which is held on production servers are prepared to prevent the identification of an individual should the database's security be compromised. This is achieved by reporting by:
   a) Age groups as opposed to a patient's actual age
   b) Within an Hospital and Health Service (HHS), outside an HHS (Queensland), outside an HHS (New South Wales), outside an HHS (Northern Territory), outside an HHS (overseas), and outside an HHS (other); as opposed to patient's postcode.
2. Insight dashboards published on the System Performance Reporting (SPR) website will prevent data to be presented when selection criteria return less than 10 records.
3. Performance Reports will report 'n.p. – not published' where a result has been prepared using less than 10 records.

Therefore, users of System Performance Reports, published and dynamic, should not be able to identify individuals from the reports.

5. Legislation

- Information Privacy Act 2009
- Hospital and Health Boards Act 2011 (Part 7)
- Information Security Policy Framework, Department of Health (DoH).

6. Implications

As the System Performance Branch receives data for an individual's age, sex, indigenous status, location of service delivery, time of service delivery and in some instances postcode, a reasonable person may conceivably be able to identify an individual from a community with a small population, or where the individual has received a low volume specialised care. This information is used to assist with providing contextual information on the relative differences in performance and quality of information. Therefore, data held by the System Performance Branch may be classified as 'Confidential Information' or 'Personal Information'. To protect this information the System Performance Branch will restrict the granularity of information contained within the published reports and dashboards; in addition to the information placed onto the publication and test environment servers. This act should prevent identification of individuals from both published and dynamic reports; in addition to protecting data should a breach occur to the publication servers.

Data received by the Data and Technical Analysis Team will contain 'personal information' and 'confidential information'. This team managers the security of information by storing received data within a secured environment. This environment, a dedicated Virtual Machine, is accessible only by the Data and Technical Analysis Team and required RSA soft token and Novell sign on. The team also complete annual mandatory data privacy and security training.

7. Definitions

Term	Definition
Personal Information	Section 12 of the Queensland Privacy Act 2009 defines 'Personal Information' as *'information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained from the information or opinion'*.
Confidential Information	Part 7 Division 1 Section 139 of the Hospital and Health Services Act 2011 defines 'Confidential Information' as '*information acquired by a person in the person's capacity as a designated person from which a person who is receiving or has received a public sector health service could be identified*'.
Disclosure of information	In relation to disclosure of information from Section 23(2)(a) of the Hospitals and Health Services Act 2011 defines disclosure as '*an entity (the first person) disclosures personal information to another entity (second entity) if the second entity does not know the personal information and is not in a position to be able to find it out'*.

8. Policy version control

Version	Issue date	Comments
Version 1.0	05/09/2016	