

# *Notifiable Data Breaches Scheme – Readiness Assessment*

## Final Report

*Department of  
Health*

*Readiness  
Assessment of  
Notifiable Data  
Breaches Scheme*

*March 2018*

## Contents

1. Executive Summary .....	3
1.1 Introduction.....	3
1.2 Objective and Scope.....	3
1.3 Key Observations and Insights .....	3
1.4 Summary of Findings and Recommendations .....	4
1.5 Summary of Ratings .....	4
1.6 Key Strengths.....	5
2. Detailed Findings and Recommendations .....	6
2.1 Understanding of NDB scheme and drafting of the response plan has been undertaken in an appropriate manner .....	6
2.2 Governance structures have been established related to accountability/decision making and the process development and reporting approach related to the NDB scheme are in place.....	9
2.3 The tools and systems to identify and communicate a breach are already in place	13
Appendix A - Consultations .....	15
Appendix B - Internal Audit Risk Ratings .....	16

## Limitations

Our Internal Audit work will be limited to that described in the Terms of Reference. It will be performed in accordance with the International Standards for the Professional Practice of Internal Auditing from the Institute of Internal Auditors, and in accordance with the Official Order (Number 127074) dated 29 July 2016, between PricewaterhouseCoopers and the Department of Health. It will not constitute an 'audit' or 'review' in accordance with the standards issued by the Auditing and Assurance Standards Board, and accordingly no such assurance under those standards will be provided.

The Terms of Reference and PricewaterhouseCoopers deliverables are intended solely for the Australian Financial Security Authority's internal use and benefit and may not be relied on by any other party. This scope may not be distributed to, discussed with, or otherwise disclosed to any other party without PricewaterhouseCoopers prior written consent. PricewaterhouseCoopers accepts no liability or responsibility to any other party who gains access to the Terms of Reference.

Report timing and sponsor	
Period of review:	February 2018
Month of final report:	March 2018
Review Sponsor:	Jackie Davis, General Counsel, Legal and Assurance Division.

THIS DOCUMENT HAS BEEN RELEASED UNDER  
THE FREEDOM OF INFORMATION ACT 1982  
BY THE DEPARTMENT OF HEALTH

# **1. Executive Summary**

## **1.1 Introduction**

The Department of Health ('the department') is responsible for a large volume of client and staff data which it maintains and shares with Portfolio partners/third parties in performing its function. The handling of this information is subject to a number of legislative and regulatory obligations to protect unauthorised or inappropriate access to this information.

The Notifiable Data Breaches (NDB) scheme under Part IIIC of the Privacy Act 1988 (Privacy Act) establishes requirements for entities in responding to data breaches to notify particular individuals and the Australian Information Commissioner (the Commissioner) about 'eligible data breaches'. A data breach is eligible if it is likely to result in serious harm to any of the individuals to whom the information relates.

To support government agencies in getting ready for the NDB scheme, the Office of the Australian Information Commissioner (OAIC) has developed guidance to help organisations understand their obligations and be prepared for commencement in 2018.

In preparation for meeting its obligations under the NDB scheme, the department's Privacy Team<sup>1</sup> has developed a draft Data Breach Response Plan<sup>2</sup> (DBRP) to outline the reporting and response processes related to a notifiable data breach.

As part of this audit, the department is reviewing the appropriateness and completeness of the activities undertaken to prepare the department in meeting its obligations under the NDB scheme.

## **1.2 Objective and Scope**

The objective of this audit was to examine the readiness of the department to address its obligations under the Notifiable Data Breaches scheme, including the governance structures, policies, processes and activities to enable an appropriate response.

This audit examined the departments:

1. Understanding of the obligations of the NDB scheme as applicable to the department's data holdings;
2. Governance structures established related to accountability/decision making, policy and process development and reporting approach related to the NDB scheme; and
3. Supporting systems and tools to enable a timely and appropriate response in the event of a notifiable breach.

## **1.3 Key Observations and Insights**

The process put in place by the departments' Privacy Team to address the NDB scheme obligations is well considered and appropriately applies existing department line area's processes and tools. While some further detail is recommended for inclusion into the draft DBRP, the planned response process scenario walk-through will provide greater insight into what other enhancements

<sup>1</sup> The Corporate Governance and Data Analytics Section within the Corporate, Commercial and Litigation Branch.

<sup>2</sup> Draft dated 31 January 2018.

are required to strengthen the prescribed process.

#### 1.4 Summary of Findings and Recommendations

The following table provides a summary of the audit findings and recommendations:

	Finding	Risk Rating	Recommendation
1	Understanding of NDB scheme and drafting of the response plan has been undertaken in an appropriate manner.	Medium	<ol style="list-style-type: none"> <li>1. The department should seek, in its role as lead agency for the Health Portfolio, assurances from Portfolio Agencies and Statutory Offices regarding their approach in addressing the NDB scheme obligations. At a minimum, the department should seek a formal means by which to be notified if an eligible breach occurs within the Portfolio.</li> <li>2. For relevant third party contracts, the department should update these with conditions requiring they also have appropriate response plans in place.</li> </ol>
2	Governance structures have been established related to accountability/decision making and the process development and reporting approach related to the NDB scheme are in place.	Medium	<ol style="list-style-type: none"> <li>3. Update the draft DBRP to incorporate additional details related to timeliness and the link to incident categories.</li> <li>4. Incorporate into the planned scenario test, full examination of line area processes which support the DBRP actions.</li> </ol>
3	The tools and systems to identify and communicate a breach are already in place.	Medium	<ol style="list-style-type: none"> <li>5. The Privacy Team should explore the incorporation and use of the existing social media/other media monitoring capability within the Communications and Change Branch during a set-period post breach notification.</li> </ol>

#### 1.5 Summary of Ratings

The overall review rating reflects Internal Audit's view of the overall exposure to the Department after consideration of all findings highlighted in this report. More detail on the rating scales used throughout this report can be found at Appendix B.

Number and rating of findings				Overall Report Priority
Very High	High	Medium	Low	Medium
0	0	3	0	

## **1.6 Key Strengths**

The following key strengths were highlighted through our review:

- Good engagement with line areas undertaken by the Privacy Team during the planning of the DBRP. Stakeholders (refer to Appendix A) highlighted appreciation that their points of view and initial feedback have been incorporated.
- The Privacy Team sought and gained insights from another Federal Government Department (Department of Agriculture and Water Resources) and an example of their Response Plan to help guide their own considerations.

THIS DOCUMENT HAS BEEN RELEASED UNDER  
THE FREEDOM OF INFORMATION ACT 1982  
BY THE DEPARTMENT OF HEALTH



## **2. Detailed Findings and Recommendations**

The detailed findings and recommendations section outlines the key audit findings, risks, and recommendations resulting from the audit fieldwork. It also details the agreed management actions to address the audit recommendations.

### **2.1 Understanding of NDB scheme and drafting of the response plan has been undertaken in an appropriate manner.**

#### **Background**

The Notifiable Data Breaches (NDB) scheme, which came into effect on the 22 February 2018, establishes requirements for entities in responding to data breaches. Entities have data breach notification obligations when a data breach is likely to result in serious harm to any individuals whose personal information is involved in the breach.

To understand the department's obligations under the NDB scheme and to determine the appropriate approach to address them, the Privacy Team (part of the Corporate, Commercial and Litigation Branch of Legal and Assurance Division of the department) took on the responsibility of fully understanding the NDB requirements and leveraging the available guidance to develop a departmental response to them.

To support government agencies in getting ready for the NDB scheme, the Office of the Australian Information Commissioner (OAIC) has developed guidance to help organisations understand their obligations and be prepared for commencement in 2018. One of those reasonable steps may include the preparation and implementation of a Data Breach Response Plan (DBRP).

A DBRP is a framework that establishes the roles and responsibilities for managing an appropriate response to a data breach, as well as prescribing the actions for managing a breach if one occurs. The more comprehensive that this plan is, the higher the chance to respond in a timely and efficient manner to a data breach and to meet all obligations under the NDB scheme. Implementing a DBRP can mitigate any damage or harm to affected individuals and reduce significant costs and reputational damage associated with data loss.

The development of a DBRP also requires organisations to carefully consider the practical issues that arise in responding to a data breach, and the unique crisis management challenges that these events can bring. This requires close coordination between an organisation's management, privacy officers, risk management, ICT/forensic support, legal, communications, HR, and records management teams to effectively and efficiently investigate, triage and manage the breach.

OAIC provided following guidelines for the comprehensive DBRP development<sup>3</sup>:

1. A strategy for assessing, managing and containing data breaches, including notification and management of affected individuals.
2. A clear definition of what constitutes a data breach in the context of the Department and breach eligibility for NDB scheme.
3. The reporting line that includes immediate contacts.

---

<sup>3</sup> <https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-developing-a-data-breach-response-plan.pdf>

4. The circumstances in which the breach is handled by a line manager or escalated to the response team.
5. Who is responsible for escalation to the Response Team?
6. Management of data breach records, including those that are not escalated to the response team.
7. A strategy to identify and address weakness in data handling that contributed to the breach.
8. Post-breach review of the Response plan effectiveness.

### **Observations**

The department's Privacy Team undertook a considered review of the NDB scheme obligations and has developed a DBRP which provides the department with an appropriate means of response to any eligible data breach. In determining this assessment, Internal Audit observed the following:

- In developing the DBRP draft the Privacy Team leveraged the OAIC Guide to developing a DBRP and also considered the approach undertaken by another agency (the Department of Agriculture).
- While drafting the DBRP the Privacy Team consulted all divisions/branches across the Department to seek comment from their respective teams. Specific additional consultation was undertaken with Information Technology Division, People, Communications and Parliamentary Division; National Cancer Screening Register Program Division; Health Analytics Branch; and Investigations and Fraud Section.
- The Assistant Secretary of the People Services Branch states that while her Branch has been contacted during the process to develop the Response Plan, she is yet to have direct involvement with the details in the plan or the responsible actions assigned to her team. She states that her Branch is able to address these requirements, however, would seek a wording change for each action from 'Manage' to 'Support, facilitate and provide' services relevant to the 2 impact scenarios listed.
- The department made a considered decision that it held no obligation to other Health Portfolio agencies for the development of their own response plans.
- The Privacy Team is working with their commercial colleagues to determine whether the department has sufficient obligations in their contracts with third parties.

### **Risk**

Inadequate understanding of the department's obligations under the NDB scheme could lead to gaps in the planned response leading to financial loss and reputational damage in the event of an eligible data breach.

### **Risk rating**

Likelihood	Consequence	Overall Rating
Unlikely	Minor	Medium

### **Recommendations**

1. The department should seek, in its role as lead agency for the Health Portfolio, assurances from Portfolio Agencies and Statutory Offices regarding their approach in addressing the NDB scheme obligations. At a minimum, the department should seek a formal means by which to be notified if an eligible breach occurs within the Portfolio.



2. For relevant third party contracts, the department should update these with conditions requiring they also have appropriate response plans in place.

### **Management response**

1. Agree - The Privacy Team will take a two stage approach to engaging with Portfolio Agencies and Statutory Offices within the Health portfolio. The first stage will involve correspondence with each Portfolio Agency and Statutory Office:
  - Outlining the start of the new scheme.
  - Referring to the circumstances in which the department would request/would require notification from the Portfolio Agency or Statutory Office holder (as the case requires) in relation to a data breach.

The second stage will coincide with the review of personal information holdings that is to be conducted as part of compliance with the Australian Government Agencies Privacy Code (**Code**). Under the Code the department must maintain a record of the department's personal information holdings. Once this list is established by the Privacy Officer(s), the Privacy Team will liaise with Portfolio Agencies and Statutory Offices identified in that list to reach agreement on formal notification arrangements.

2. Partially Agree - The Privacy Team has consulted with the Commercial Section in Legal and Assurance Division and the department's standard contract terms and standard funding agreement already require third parties to comply with the Australian Privacy Principles and notify the department in the case of any breach of those responsibilities. This would encompass events that would otherwise trigger a response under the NDB scheme. <sup>s42</sup>

The department will also ensure that privacy training provided in compliance with the Code will include information for contract managers as to the obligations under the NDB scheme.

Accountable Officer	Date of completion
Miriam Moore Assistant Secretary Corporate Commercial and Litigation Branch	<ol style="list-style-type: none"> <li>1. Correspondence will be sent to Portfolio Agencies and Statutory Offices by <b>19 March 2018</b> (Stage 1) and formal arrangements regarding notification will be sought after the record of personal information holdings is established. The Code commences on 1 July 2018, formal arrangements will be sought once the list is established, <b>1 August 2018</b> at the latest (Stage 2).</li> <li>2. A preliminary review of standard contract terms has already been completed. <sup>s42</sup> and training to be developed to comply with Code obligations which commence on <b>1 July 2018</b>.</li> </ol>

## **2.2 Governance structures have been established related to accountability/decision making and the process development and reporting approach related to the NDB scheme are in place**

### **Background**

According to OAIC guidance, once it has been confirmed that an eligible data breach has occurred, an entity must:

- prepare a prescribed statement and provide a copy to the OAIC as soon as practicable
- if it is practicable to do so, take reasonable steps to notify the contents of the statement to individuals to whom the information relates, or to those at risk from the eligible data breach.

Failure to comply with the notification regime is considered an *"interference with the privacy of an individual"* under the *Privacy Act 1988* (Cth) which can currently result in fines of up to AUD 1.8 million.

Therefore, the DBRP should set out the actions the Response Team must take in the event of a data breach. These actions are:

**Step 1: Contain the breach and do a preliminary assessment**

**Step 2: Evaluate the risks associated with the breach**

**Step 3: Notification**

**Step 4: Prevent future breaches**

The department's draft DBRP prescribes the steps of actions that should be undertaken during a data breach. Each division in the Response Team is allocated specific responsibilities and is expected to perform standard business processes relevant to a data breach and advise the Privacy Team.

### **Observations**

The department's draft DBRP addresses the key governance considerations with clear accountabilities and reporting structures in place. The associated process flow and instructions address the 4 key steps outlined in the OAIC guidance. In determining this assessment, Internal Audit observed the following:

- There are prescribed actions in the determination and recording of a potential data breach. A supporting proforma to capture necessary information related to the suspected breach is also provided as an annexure.
- It is clear that in the case of a suspected breach, the Privacy Team is the primary contact. The Privacy Team manages the initial response and escalates decisions about notification to the General Counsel. Acting on advice from the Privacy Team, the General Counsel determines whether an eligible data breach has occurred and decides whether to form a Data Breach Response Team. The General Counsel also determines whether to notify the Information Commissioner and affected individuals.
- The method of notification will depend on factors such as the ability to identify the affected individuals and any prior method of communication the department has used with those individuals. The General Counsel will make her decision in consultation with communication staff as flagged in the responsibilities set out for the Data Breach

#### Response Team.

- The Privacy Team have scheduled a workshop to develop resources for internal use during a data breach. Previous written notifications used for previous data breaches will be modified to form a template for future communications (and this will be submitted to Communications and Change Branch for review). Communications and Change Branch will be further engaged for guidance in relation to other forms of communication with stakeholders (for instance, the use of a spokesperson, media releases and website alerts).
  - The Privacy Team does not have an agreed approach to responding to media enquiries and would look to the expertise within the Communication and Change Branch in framing any response.
- The Privacy Team will maintain records of each breach report received and the relevant follow up action. This information will inform the Privacy Teams' bi-annual review of the DBRP and assist in preventing future breaches.
- To further support post breach reviews, the Privacy Team states that in consultation with the Investigation and Fraud Section, the Data Breach Report form (Annexure A of the DBRP) was drafted to require a substantial amount of information in relation to the circumstances surrounding a suspected breach. As per the plan, the Privacy Team will assess this information once it is received and liaise with Investigations and Fraud Section when necessary. As the plan notes under step 5, the General Counsel and line areas will review necessary changes to practices and procedures in response to a data breach.
- The Privacy Team will maintain an online TRIM record (with restricted access) of all submitted Data Breach Report forms. The Privacy Team is in the process of developing internal protocols concerning, among other things, the manner in which submitted forms will be handled by the Privacy Team, including the undertaking of assessments.
- Relevant material on the purpose, obligations and department response for the NDB scheme will be incorporated in the privacy training module (which is due to be updated prior to the commencement of the Australian Government Agencies Privacy Code on 1 July 2018). The Privacy Team is also looking to further develop the intranet site specific to data breach reporting, which may include further information on, for example, circumstances that might give rise to a data breach; and steps that line areas can take (in consultation with the Privacy Team) to contain a data breach .
- The DBRP is clear on the '**what**' needs to occur during a response, but in some instances lacks granular detail on the '**how**' it will occur and relies upon existing processes within line areas to address these requirements. The Privacy Team is conducting an internal workshop (planned for 30<sup>th</sup> April 2018) to familiarise Response Team members with the plan, to discuss the specifics around the team's role in the process and to run through scenarios.
- Some line areas require clarity regarding the timeliness of response actions. They would seek further information and detail on the linkage to the stated 'categories of urgency' as outlined in the DBRP.
- The DBRP has incorporated links to other relevant department policies and process such as the Business Continuity Plan when implementing any containment approach.

#### **Risk**

The ability of the department to respond in an appropriate and timely manner is yet to be tested prior to the commencement of the NDB scheme. An inability of any area within the Response Team to meet required actions may increase delays in the containment of a data breach and further add to the risk of reputational damage for the department.



### ***Risk rating***

<b>Likelihood</b>	<b>Consequence</b>	<b>Overall Rating</b>
Possible	Minor	Medium

### ***Recommendations***

3. Update the draft DBRP to incorporate additional details related to timeliness and the link to incident categories.
4. Incorporate into the planned scenario test, full examination of line area processes which support the DBRP actions.

### ***Management response***

3. Partially Agree – Some specific timelines were deliberately excluded from the Data Breach Response Plan. As part of the central co-ordinating role of the Privacy Team and the General Counsel it is expected that specific guidance on timeframes will be given to the Data Breach Response Team members in relation to each individual breach, based on the severity and urgency of the breach. There was concern that setting out specific timeframes for some processes would establish inflexible expectations among the Data Breach Response Team members that would be difficult to displace in instances where more urgent responses were required.

To provide greater guidance to Data Breach Response Team members, part of the proposed workshop (see response to Recommendation 4) will involve the Privacy Team discussing a number of scenarios. These discussions will provide the basis for shared expectations going forward. To reinforce this discussion written follow-up material will be provided to Data Breach Response Team members, likely as a supplement to the Data Breach Response Plan, which will set out the factors that will impact on required timelines and some example scenarios.

In addition to the timeframes already outlined in the plan (page 3), more explicit guidance will be provided that line areas should report a suspected breach within 24 hours. The legislated time frame for investigating a suspected data breach (30 days) will also be added to the Data Breach Response Plan as it relates to 'Category 2- further information required'.

4. Agree - To ensure an efficient workshop the Privacy Team will individually meet with each member of the Data Breach Response Team to discuss their processes, resources and/or capability as they relate to their function on the team. This information will inform a more detailed role description that will be used to supplement the Data Breach Response Plan. After this supplement is developed each team member will be invited to a scenario walkthrough where they will gain a better understanding of their role and the role of other team members.

<b>Accountable Officer</b>	<b>Date of completion</b>
Miriam Moore Assistant Secretary	3. Data Breach Response Plan to be updated in relation to Category 2 timeframe by <b>14 March 2018</b> . Workshop to be conducted with all Data Breach Response Team Members present by <b>30</b>



Accountable Officer	Date of completion
Corporate Commercial and Litigation Branch	<p><b>April 2018</b> (see response to Recommendation 4). Updated material to be provided within two weeks of workshop.</p> <p>4. Individual meetings with each Data Breach Response Team member will be organised in preparation and prior to a workshop walk through to be held by <b>30 April 2018</b>.</p>

THIS DOCUMENT HAS BEEN RELEASED UNDER  
THE FREEDOM OF INFORMATION ACT 1982  
BY THE DEPARTMENT OF HEALTH

### ***2.3 The tools and systems to identify and communicate a breach are already in place.***

#### ***Background***

If an entity is aware of reasonable grounds to believe that there has been an eligible data breach, it must promptly notify both individuals at risk of serious harm and the OAIC about the eligible data breach. On the other hand, if an entity only has reason to suspect that there may have been an eligible data breach, it needs to move quickly to resolve that suspicion by assessing whether an eligible data breach has occurred. If, during the course of an assessment, it becomes clear that there has been an eligible breach, then the entity needs to promptly comply with the notification requirements.

The OAIC guidelines expect entities to have practices, procedures, and systems in place to comply with their information security obligations under APP11, enabling suspected breaches to be promptly identified, reported to relevant personnel, and assessed if necessary.

#### ***Observations***

The department's tools and processes to provide an appropriate notification in the event of an eligible breach are in place. The associated process flow and instructions address the 4 key steps outlined in the OAIC guidance. In determining this assessment, Internal Audit observed the following:

- The department does not possess any large scale SMS notification capability, rather the Communications and Change Branch are responsible for mass communication techniques such as the Health.gov.au website and the department's Twitter account. These will be utilised if a large scale data breach has occurred.
- The decision to notify and the form of the notification is determined by the General Counsel. The method of notification will depend on factors such as the ability to identify the affected individuals and any prior method of communication the department has used with those individuals. The General Counsel will make her decision in consultation with the Communications and Change Branch.
- For individual related data breaches or smaller scale events, personal contact via writing or email will take place.
- As stated previously, the Privacy Team does not have an agreed approach to responding to media enquiries and would look to the Communications and Change Branch expertise in framing any response.
- The Communications and Change Branch has suggested the possible inclusion of Social Media monitoring after the notification of a breach incident. This would be used to measure sentiment to the response approach and/or provide guidance on other actions required to address 'false or misleading' statements made on social media accounts.

#### ***Risk***

In the event of a large scale data breach, the department may not have the means to reach all impacted individuals in a timely manner, thereby adding to the reputational risk caused by the initial breach.

### ***Risk rating***

<b>Likelihood</b>	<b>Consequence</b>	<b>Overall Rating</b>
Unlikely	Minor	Medium

### ***Recommendations***

5. The Privacy Team should explore the incorporation and use of the existing social media/other media monitoring capability within the Communications and Change Branch during a set-period post breach notification.

### ***Management response***

5. Agree - The Privacy Team will consult with Communications and Change Branch about their capability to monitor media (including social media) in a one on one session (see response to Recommendation 4). Subject to their views, this role will be added to the Data Breach Response Plan and any associated documentation.

<b>Accountable Officer</b>	<b>Date of completion</b>
Miriam Moore Assistant Secretary Corporate Commercial and Litigation Branch	<ol style="list-style-type: none"><li>5. Capability will be assessed in one on one meeting with Communications and Change Branch prior to <b>21 March 2018</b>.  Documentation, including the Data Breach Response Plan, will reflect this additional function by <b>30 April 2018</b> (to allow time for the combined walk through of the plan).</li></ol>

## Appendix A - Consultations

Appendix A details the staff members consulted throughout the course of the audit.


Stakeholder	Position
Jackie Davis	General Counsel, Legal and Assurance Division.
Miriam Moore	Assistant Secretary, Corporate Commercial and Litigation Branch.
Ian Crettenden	Assistant Secretary (in transition), Health Analytics Branch.
Adrian Bugg	Assistant Secretary, Data Service Branch (Information Technology Division).
Jodie Grieve	Assistant Secretary Communication and Change Branch (People, Communication and Parliamentary Division).
Christine Svarcas	Assistant Secretary People Services (People, Communication and Parliamentary Division).
Michael Culhane	Assistant Secretary, Health Analytics Branch.
s22	Director, Corporate Governance and Data Analytics.
s22	Assistant Director, Legal.
s22	Director, Data Governance.
s22	Director Investigation and Fraud Control Section.



## Appendix B - Internal Audit Risk Ratings

Appendix B provides an overview of the risk matrices outlined in the Department's Risk Management Policy. Each individual internal audit finding has been assigned a risk rating, consistent with the Department's Assessment Matrix at Figure 1 below. The Department's Risk Tolerance Table at Figure 2 below outlines the required actions against each risk rating.

**Figure 1:** The Department of Health Risk Assessment Matrix

 <b>Australian Government Department of Health</b>			<b>RISK ASSESSMENT MATRIX</b>				
Date Approved:			Likelihood				
General description of Consequences			Rare <small>Exceptional circumstances only</small>	Unlikely <small>Not expected to occur</small>	Possible <small>Could occur at some time</small>	Likely <small>Will probably occur in most circumstances</small>	Almost Certain <small>Expected in most circumstances</small>
Consequence	Would stop achievement of functional goals/objectives	Severe	High	High	Extreme	Extreme	Extreme
	Would threaten functional goals/objective(s)	Major	Medium	Medium	High	High	Extreme
	Requires significant adjustment to overall function to achieve objective(s)	Moderate	Medium	Medium	Medium	High	High
	Would threaten an element of the function and would require some adjustment to achieve objective(s)	Minor	Low	Medium	Medium	Medium	High
	Lower consequence to achievement of objectives.	Insignificant	Low	Low	Low	Medium	Medium

**Figure 2:** The Department of Health Risk Tolerance Table.

Reference	Risk Ratings	Action required
E	Extreme risk	Risk must be given immediate senior management attention. Risk assessment and an approved risk management plan, including treatments must be undertaken.
H	High risk	Risk must have considerable management attention to reduce risk to as low as reasonably possible. Risk assessment and an approved risk management plan, including treatments must be undertaken.
M	Medium risk	Risk should be managed and monitored. Risk assessment and an approved risk management plan required. If controls are working effectively then additional treatments are optional.
L	Low risk	Risk should be managed and controls monitored. Full risk assessment and additional treatments not required.

THIS DOCUMENT HAS BEEN RELEASED UNDER  
THE FREEDOM OF INFORMATION ACT 1982  
BY THE DEPARTMENT OF HEALTH