



Divisions of General Practice

Information Management Maturity Framework
(IMMF)

Toolkit – Security and privacy audit
template



Information Management Maturity Framework (IMMF)

Toolkit – Security and privacy audit template

Purpose

The purpose of the “Security and privacy audit template” is to assist Divisions to address the action tasks below.

Action Tasks	Capacity Gap	IMMF Element
Implement a common security and privacy standard for all the Division’s programs and services	Reactive to Defined	Compliance and Quality

This task should have been identified from the Information Management Maturity Framework (IMMF) gap analysis and toolkit specification.

This tool provides Chief Executive Officers (CEOs) with a set of templates that can be used to develop a basic and consistent approach to a Division’s security and privacy requirements. It should be read in conjunction with the Tool – “Privacy guidelines for reuse of information”, which provides a template to manage a Division’s privacy requirements.

Knowledge of the privacy guidelines for reuse of information as they apply to a Division’s programs and services is a pre-requisite for the use of this tool. Knowledge of other tools that may be useful for applying this tool includes - “Guidelines for IM risk management” and “Business continuity checklist”.

Using this template will assist a Division to ensure that information is protected from unauthorised access, use or destruction. Application of the security principles described in this template will enable active staff recognition and ownership of information security initiatives in most of the Division’s programs and services. While all Divisions are responsible for ensuring they comply with privacy requirements and are all subject to the same security threats, this tool recognises that implementation of a range of security measures will vary depending upon the size of the Division and is designed to be scalable over Divisions of different size.

Explanatory Notes

A uniform approach to security and privacy requires Divisions to adopt a standard definition of security and privacy and a formalised approach in identifying and dealing with potential risks that may affect security and privacy of information.

This tool addresses aspects of information management (IM) legislation and community standards specifically concerned with Information (or IM) Security and Privacy. The tool provides the Division with a basic *internal audit template* with which can be used to self-assess a Division’s degree of conformity with accepted best practice in regards to security and privacy protection.

Use of this template will help a Division prepare for a subsequent formal external audit. By following this template, identifying non-conformities and acting upon them, the Division will be in an optimum position to undergo external audit by security and privacy experts. Even if the stage of external audit is not reached, by using this tool, a Division will be able to make a sound and defensible claim that it has examined its position with respect to accepted best practices and is in reasonable conformity with health sector norms.

The principal references used to create this Security and Privacy Audit Template are as follows:

- HB 174-2003 *Information security management Implementation guide for the health sector* (by Standards Australia);
- *GPCG Computer Security Self-Assessment Guideline and Checklist for General Practitioners* (by the General Practice Computing Group);
- *Privacy Act 1988 (Commonwealth)* – including later amendments that apply to the private sector; and
- *RACGP Handbook for the Management of Health Information in Private Medical Practice*.



There are other technical security and risk management standards that may be of interest depending on a particular Division’s circumstances. See References at the end of this document.

Instructional design

This tool consists of the following Parts:

Part 1 – Notes on “best practice” in Security and Privacy

Part 2 – Security Internal Audit Template

Part 3 – Privacy Internal Audit Template

Appendix – Register of Personally Identifiable Information Template

Part 1 – Notes on “best practice” in Security and Privacy

Provides an overview of best practice in security and privacy and its implications for Divisions.

Part 2 – Security Internal Audit Template

Makes available a basic template to help Divisions identify security non-conformities and act upon them.

Part 3 Privacy Internal Audit Template

Makes available a basic template to help Divisions identify privacy non-conformities and act upon them.

Division CEOs should review the guidelines and consider the Division’s requirements in relation to security and privacy. The guidelines and templates are not exhaustive. They are intended to assist CEOs in developing Information Security (IS) policy and procedures. CEOs may find that some elements of the template are irrelevant to their Division, while other template elements may require further detail and research. Security and privacy of health records are crucial to the Division and therefore requires senior management commitment. The guidelines should be read and discussed with senior staff of the Division, as well as any staff identified as critical to maintaining security and privacy of information.

Security and privacy procedures and policies should be included in the Division’s procedures manual and relevant position descriptions.

This tool is mentored for the implementation of new processes and procedures and for cultural adjustments.

Summary of outcomes and resources

Workstreams	Outcomes	Resources
New processes or procedures to be adopted	Policies and/or procedures are developed to enable the application of consistent and appropriate security standards to all of a Division’s programs and services.	Mentoring by CEOs of Divisions that have demonstrated a capacity for implementation of privacy principles.
Culture and change management requirements	<p>Security and privacy requirements are implemented in staff job descriptions.</p> <p>Staff are trained and aware of security and privacy requirements and take responsibility for their implementation.</p> <p>Staff apply security and privacy procedures in their day-to-day operations.</p>	



Part 1 – Notes on “best practice” in Security and Privacy

The concept of “Best Practice” in Security

It should always be borne in mind that *there is no such thing as perfect security*. It is often said that security is really all about *risk management* and there is much truth in this viewpoint. It is probably inevitable that a Division will suffer some sort of security or privacy breach one day. Some of the most important considerations in security relate to balancing the appropriate level of resources allocated to prevention of threats and the cost of threats should they actually occur. Further, if security breaches are inevitable, then what are the best ways to reduce their frequency, mitigate their impacts and to recover quickly from them?

Given that security is imperfect, some of the most important questions for a Division CEO are:

How can the Division determine if it is doing the best security job it can under the circumstances, and how can it demonstrate to its members, funding bodies, other stakeholders and regulators that its security is appropriate?

Information security can be rather less precise as a discipline than mainstream IM. Not only is perfect security unattainable, but a great deal of security is determined not by fast hard technology, but rather by human factors e.g. the most common security failures are poor password management and staff leaving sensitive information displayed on a screen when not present at their workstation. Furthermore, the threats we face today are changing rapidly, and it can be difficult to stay abreast of – much less ahead – of developments.

A flexible and pragmatic approach to security is therefore essential. Modern organisations must be realistic and *particular* about their own security goals. They must beware of generic security solutions, and take care instead to analyse and document their own circumstances. They must maintain an organisational self-awareness of their security position and how it evolves; they must take deliberate steps to keep their security systems up to date, and be seen to be keeping them up to date.

Current security standards (including the benchmark AS/NZS ISO 17799 and the newer ISO 27001) tend not to be prescriptive but instead usually emphasise the dynamic and particular nature of threats that apply to any given situation. That is, these are *management* standards. They generally require organisations to manage security in a certain cyclical way, including analysis of local conditions and business requirements, documented policies and procedures, risk assessment, measurement, and continuous improvement. It is not possible to slavishly follow any one security recipe and hope for protection against generic mishaps and attacks. Instead, each organisation’s “security posture” (see below) will be different. Standardisation in security applies at the level of having a uniform approach from one organisation to another in the way they go about establishing and maintaining their security posture. However, this style of standardisation leaves plenty of room for interpretation which is yet another factor that contributes to the nature of IM security being as much as ‘art’ as a ‘science’.

Divisions of General Practice need to concentrate on following what they can be satisfied represents *best practice* in IM security. Best practice is constantly evolving. Not many industries are actually subject to explicit mandatory (legislated) obligations in respect of IM security in Australia. For the most part, our regulatory environment takes a light touch to IM security. Nevertheless, in the health sector community expectations are high in regards to how their personal information will be managed, respected and safeguarded. A high degree of common law duty of care is to be expected.

What is “security posture”?

Security posture is a term that is increasingly used in the field to capture the idea that an ensemble of security practices and counter-measures need to be established to protect an organisation against threats peculiar to its business situation. Rather than trying to specify the state of play in detail and measure it against specific standards, the idea of a security posture is to characterise if, on balance, an organisation is equipped appropriately. There is as yet no more specific or prescriptive way of talking about security posture, but it can be illustrative to consider what the term might confer in different healthcare settings:

- In general terms, the appropriate security posture for a **pharmaceutical company engaged in testing a psychiatric drug** would be extreme. Important risks to be addressed would include corporate espionage and cyber-activism, as well as industrial scale identity theft of any large databases of personal information.



Strict access controls would be required to raw data and to double blinding keys. Data could be expected to be encrypted to 'military grade' specifications. Smartcards or biometric identification might be appropriate for select personnel to be able to access administrative systems. All personnel would be subject to strict clean desk protocols. All paper records would be locked in a safe and transported using secure couriers. Network systems might be isolated from the Internet by "air gaps" to prevent unauthorised access.

- The security posture for a **small general practice clinic** which is largely paper based would be lower key. While still treating patient confidentiality seriously, the IM security environment would be built at a level in keeping with security around paper records in the practice. Database encryption, two factor logon controls, hardware firewalls and so on could be adjudged as unnecessary provided for example that the practice's local area network was not accessible from the Internet. Computer security could be roughly comparable to that of a paper 'Compactus'. A regular backup of all hard drives would be important but perhaps not entirely mission critical if the majority of patient notes happened to be retained in hardcopy. The main risks in this type of setting might be inadvertent loss resulting from fire or vandalism, as opposed to deliberate targeted attack.
- Finally, the security posture **of a Division of General Practice** would be somewhat intermediate between the above two examples, in light of the fact that much greater volumes of health information are involved compared with one practice, and that such information tends to be shared with a great many external parties, albeit in de-identified form. It will be different again between Divisions which manage identified patient information and those that do not. The realities of a busy office environment means that attention needs to be paid to issues including computer network account management, the careful deactivation of old accounts, and controlling access to far flung computers in the building or in physically separate offices by visitors and contractors. Important threats in this type of environment include attack by disgruntled employees armed with inside knowledge. A larger network and high bandwidth external connectivity in general demands sophisticated firewalls and automated network backup.

How this tool was developed

In various industries including healthcare, best practice tools have been prepared by representative bodies to facilitate uniform approaches to the application of security management standards. Especially in the case of small businesses that typify general practice, good work has been done and made freely available in the form of template documents, guidelines and checklists.

Some of the best recent examples in the Australian healthcare sector have been used in preparing this audit template:

- HB 174-2003 *Information security management Implementation guide for the health sector* (by Standards Australia);
- *GPCG Computer Security Self-Assessment Guideline and Checklist for General Practitioners* (by the General Practice Computing Group);
- *Privacy Act 1988 (Commonwealth)*; and
- *RACGP Handbook for the Management of Health Information in Private Medical Practice*.

In preparing the current tool, the above resources have been extended to apply to Divisions as opposed to individual general practices and privacy and security considerations have been combined in one document. The tool design has allowed for the fact that Divisions in the majority of cases handle population data, rather than individually identifiable clinical data, but that they tend to share healthcare data with a large range of external organisations. Accordingly, one special focus of the current tool is on ensuring that privacy protections inherent in population data preparation are in fact realised.

Relationship with external security audit

Note that this audit tool makes assumptions as to Divisions having already established minimal policies and procedures for security and privacy management. It is beyond the scope of this tool to do more than name these policies and procedures generically. If a Division finds that it has yet to develop the level of documentation assumed in this tool, then it may have to draw on other resources to fill in those gaps.



Note also that the current audit tool aims to help Divisions establish reasonable conformity with “best practice” but stops short of formal standards compliance. Divisions may decide for themselves whether or not they will be audited externally in respect of security and privacy performance, or formal compliance with the requirements of such standards as AS/NZS 17799.

If the tool is applied to internal audit of security and privacy practices and indicated remedial actions undertaken, then the Division should be able to claim that its “security posture” is reasonable relative to accepted best practice. This may be especially relevant for smaller Divisions.

Approaches to security management

While security stands apart from mainstream IM practices, nevertheless information security remains closely aligned with the IM industry in respect of products and services. IM security is indeed a high tech business, subject to vigorous competition and innovation. Security products – such as firewalls, anti-virus and content scanning, email filters and so on – and managed service models continue to evolve rapidly.

There are several competing and legitimate viewpoints about the optimal way to structure security management and reporting lines in an organisation. One view is that all security – whether it be information security or physical and personnel security – relates to risk management and requires a common approach for that reason. In this case, security is structured “horizontally” with security responsibilities cutting across other organisational structures or silos. It is relatively common for security to be managed as part of an organisation’s corporate governance effort. An alternative approach is that information security is deeply and unavoidably technical, and that it should therefore be managed by technicians close to the organisation’s IM effort; that is, that responsibilities be structured “vertically” within one technical specialisation. The latter approach however, needs to account for the possibility that security and risk decisions can be compromised if they are not made independently.

In any case, IM security is a complex field and deserves significant human resourcing. Divisions of General Practice are not characteristically large organisations and are not always well resourced in information technology. It is not unusual therefore to assign Security Officer responsibilities to a member of a Division’s IM staff. As noted, such a vertical structure is workable so long as there is access to good, up-to-date security expertise, and that steps are taken to ensure independence in security decision making. This is where an internal audit template such as this tool can help, especially when audits and reviews are undertaken by personnel removed from the IM effort.

Recap: The Privacy Regime and the National Privacy Principles

While information security is not closely regulated in Australia, on the face of it, an organisation’s privacy obligations are laid down in law, namely the Privacy Act 1988 (Commonwealth) together with subsequent amendments that extended protections to much of the private sector. The cornerstone of privacy law is a set of 10 National Privacy Principles (NPPs) which are summarised below, together with a brief explanation of the major implications of each of them:

NPP1: Collection – Divisions must only collect personal information for reasons directly related to their business or operational requirements.

NPP2: Use and Disclosure – Divisions must explain how and why personal information can be used within the organisation or disclosed to external third parties under special circumstances.

NPP3: Data Quality – Divisions must take reasonable steps to ensure that personal information is up-to-date, accurate and complete.

NPP4: Data Security – Divisions must take reasonable steps to ensure that personal information is secure from loss, misuse and unauthorised access.

NPP5: Openness – Divisions must be open about how they handle health information and clearly explain how they handle health information.

NPP6: Access & Correction – Patients have a general right of access to their own health records, and a right to have information held by a Division corrected, if it is inaccurate, incomplete or out of date.



NPP7: Identifiers – Divisions must not use Commonwealth Government identifiers (such as Medicare numbers or Veterans Affairs numbers) to identify patients for their own record keeping purposes. These identifiers may only be used for the reasons for which they were issued.

NPP8: Anonymity – Divisions must, where lawful and practicable, provide patients with the option of using health services without identifying themselves.

NPP9: Transborder data flows – Divisions must take care that adequate privacy regimes apply in other jurisdictions – which in some states of Australia means other states – into which they might transfer personal information.

NPP10: Sensitive Information – Divisions have additional obligations when collecting health information from patients as this is counted as “sensitive” under the Privacy Act. These include collecting health information only with consent.

Note too that in some states, a Division may also be subject to additional laws and health privacy principles. For further details, please refer to the Tool “Privacy guidelines for reuse of information”. This tool provides a basic checklist of the topics to be considered when raising awareness of privacy principles within the Division and reviewing the effectiveness of their application. However, this tool takes the concept further and provides a template for internally auditing privacy controls.

A note about personal information

The Privacy Act and the NPPs only apply to information about someone where the identity of that person is reasonably apparent. Therefore, information that is de-identified, even if it pertains to a person’s healthcare, is not subject to privacy regulations. Notwithstanding the important point that de-identification can be a subtle and complicated topic (see also Tool 9 “Privacy guidelines for reuse of information”), the first and foremost measure taken by Divisions to safeguard privacy should be to avoid the handling of identifiable information wherever possible.

In order to reinforce the important distinction between data collections that fall under the Privacy Act from that which does not, in this document the more pedantic if somewhat unwieldy term “Personally Identifiable Information” is used rather than “personal” or “private” information.

When it comes to healthcare data, in the majority of cases, the business of a Division of General Practice is concerned with population issues rather than personally identifiable clinical information. However staff must remain aware at all times of cases of Personally Identifiable Information, treat the information accordingly, and take steps to minimise the retention of such information as far as possible, consistent with the Division’s business objectives.

A practical approach to privacy

While the Privacy Act and the NPPs set out detailed requirements, each Division and its staff need to set in place a culture and a set of pervasive mechanisms that safeguard privacy fundamental level, to prevent privacy breaches from occurring to the greatest extent possible. Divisions should pay attention to the following practical matters.

Know what information you’re collecting, why, where and how

A great deal of difficulty arises under the privacy regime when organisations are taken by surprise in respect of personal information they were not aware they had, or worse, personal information they have passed on to a third party without the appropriate controls. The most important practical tool for ensuring organisation-wide prevention of privacy breaches is to maintain a register of all the types of Personally Identifiable Information that is held.

An example Personally Identifiable Information Register template is included in the Appendix. The Register is organised in columns that record important attributes concerning the lifecycle of information. The idea is to not enter each and every actual data item (to do so might actually create fresh privacy problems by duplicating sensitive data unnecessarily) but rather to maintain the register at a high level so that staff have awareness of where all personal information is within the organisation and what it is doing there.



The important attributes are as follows:

- **What** Personally Identifiable Information is collected?
- **Why** exactly is it needed by the Division?
Note whether the individual concerned been made aware of the reason for collection, in line with the Openness principle, and of their other rights under the Privacy Act.
- **Where** is it collected and used?
All instances (which usually will relate to Division sub-systems and business processes) should correspond to a stated reason in the Why column). Typical sub-systems holding Personally Identifiable Information include:
 - client databases and Customer Relationship Management (CRM) systems
 - Human Resources systems
 - help desks and call centres
 - audit logs and transaction histories
- **How** is it collected?
There tend to be five main ways in which Personally Identifiable Information may be collected:
 - **Overtly** through forms, interview, correspondence, warrant and so on, with the individual's knowledge
 - **Covertly** without the individual's knowledge
 - **Automatically**, as with audit logs and transaction histories
 - **Indirectly** as with information disclosed to DOJ by other agencies or external organisations
 - **Transiently** as with short lived information collected for a specific transient purpose such as establishing the identity of someone making a help desk enquiry, and should be destroyed right away.
- **When** is it collected?
- **Who** else might the Division disclose the information to?

Be sure of consent and implied consent

In general, the privacy regime requires that an individual's consent be obtained wherever practicable before information about them is collected and used. However, there is reasonable allowance for the secondary use of Personally Identifiable Information on the basis that consent has been previously implied. In the health sector, secondary usage of information of course is routine: medical practitioners could not function if they did not share case notes, send orders and test results and so on.

However, this does not mean that we can take for granted that individuals have granted unlimited implied consent for information about them to be passed from one organisation to another throughout the system. It must be remembered too that lay people will not have a full appreciation of how far and wide healthcare information can flow, and that it is the individual's *reasonable expectations* that matter when it comes to adjudging implied consent. Therefore Divisions should err on the side of caution. Whenever a Division has cause to collect Personally Identifiable Information, it should firstly double check that there is a real need for that information to be held, and secondly it should review critically whether or not the individual has consented to the collection or could be reasonably assumed to accept the need for secondary use within the Division.



Part 2 – Security Internal Audit Template

How to use this Template

The following is a checklist that forms a useful starting point for an internal audit of the Division’s “security posture”. The checklist should be merged with any existing internal audit instructions that might apply, and be undertaken in accordance with any existing internal audit procedures.

In the absence of existing audit procedures, it is recommended that the audit be conducted by one or more staff members who are independent of the Division’s routine security and IM practices and who played no substantial part in IM security decision making or implementation. The audit will require a reasonable level of IM security knowledge so as to be able to interpret evidence, pursue incomplete or ambiguous findings, and to reach meaningful conclusions about conformity.

The results of the internal audit should be documented in keeping with Division practice, and reviewed and signed off by relevant senior management. The disposition, resolution and sign off of non-conformities must be handled in keeping with the Division’s quality assurance and corporate governance mechanisms.

Note that certain topics in the checklist are considered on pragmatic grounds to be higher priority and are indicated as such in bold face.



SECURITY POSTURE INTERNAL AUDIT

Topic Area	Topic	In place? Date if applicable	Follow up Actions	Rectification? Date if applicable
Division IT Security Officer	IM Security Officer role description written			
	IM Security Officer training provided (if applicable)			
Division IT Security Policies and Procedures	IM security policies and procedures documented (see below)			
	IM security policies and procedures documentation last reviewed/updated [DATE]			
	Staff trained in IM security policies and procedures			
	Policies & Procedures accessible by all Staff			
	HR procedures to include network account deactivation when staff depart			
	– Access Control and Password Policy			
	– Reasonable Use of Division IM Resources Policy (incl. Internet usage, e-mail usage, personal storage device usage etc.)			
	– Network Computer Backup Procedures			
	– Content Screening and Anti-virus Update Procedures			
	– Standard Operating Environment for PCs (incl. screensavers, anti-virus)			
	– Firewall Procedures (including rule sets)			
	– Disposal of Computer Equipment Procedures (incl. destruction of hard drives)			
Disaster recovery plan	Disaster Recovery Plan developed			
	Disaster Recovery Plan last tested [DATE]			
	Disaster Recovery Plan last reviewed/updated [DATE]			
Back-ups	Back-ups of data done daily			
	Back-ups of data stored offsite			
	Back-up procedure last tested [DATE]			
Firewalls	Firewalls installed			
	Firewalls last tested [DATE]			



Part 3 – Privacy Internal Audit Template

How to use this Template

The following is a checklist that forms a useful starting point for an internal audit of the Division's systemic approach to privacy. The checklist should be merged with any existing internal audit instructions that might apply and be undertaken in accordance with any existing internal audit procedures.

In the absence of existing audit procedures, it is recommended that the audit be conducted by one or more staff members who are reasonably knowledgeable in privacy, corporate governance and / or knowledge management.

The results of the internal audit should be documented in keeping with Division practice, and reviewed and signed off by relevant senior management. The disposition, resolution and sign off of non-conformities must be handled in keeping with the Division's quality assurance and corporate governance mechanisms.



PRIVACY SYSTEMS INTERNAL AUDIT

Topic Area	Topic	In place? Date if applicable	Follow up Actions	Rectification? Date if applicable
Fundamentals	Division Privacy Officer appointed			
	Privacy Policy documented and published			
	Staff trained in Privacy principles and obligations			
	Do all forms (paper & web) alert individuals to their Privacy rights?			
Handling Personally Identifiable Information	Establish a Register of all Personally Identifiable Information held by Division			
	Understand lifecycle of all Personally Identifiable Information			
	All data de-identified wherever possible			
	Personally Identifiable Information accessible by Division Staff on Need-to-Know basis only			
	Only release Personally Identifiable Information when:			
	– receiving organisations known to have comparable privacy protections AND			
	– consent or implied consent granted			
	All external releases of Personally Identifiable Information are logged and auditable			
All acquisitions of bulk Personally Identifiable Information are logged and auditable (e.g. databases, clinical data collections, epidemiological data, research data etc.)				
Privacy Procedures	<i>Responding to requests for access to Personally Identifiable Information</i>			
	<i>Responding to requests for corrections to Personally Identifiable Information</i>			
	<i>Alerting individuals when Personally Identifiable Information about them is acquired</i>			
Special Privacy vulnerabilities of interest	All forms (paper & web) reviewed against Collection Principle			
	Offsite data backup secure and private			
	Controlled access to Division systems by IM/IT contractors and service providers			



References

AS/NZS ISO/IEC 17799:2006 *Information technology: Security techniques; Code of practice for information security management*

AS 4360:2004 *Risk Management*

AS/NZS ISO/IEC 27001: 2006 *Information technology: Security techniques; Information security management systems requirements*

HB 174-2003 *Information security management Implementation guide for the health sector* (by Standards Australia)

Available from <http://www.e-healthstandards.org.au/drafts.asp?area=publications> or <http://tinyurl.com/3tdhao>

GPCG Computer Security Self-Assessment Guideline and Checklist for General Practitioners (by the General Practice Computing Group).

Available from www.gpcg.org.au and <http://tinyurl.com/2478g7>

Privacy Act 1988 (Commonwealth) – including later amendments that apply to the private sector

RACGP Handbook for the Management of Health Information in Private Medical Practice (by the Royal Australian College of General Practitioners)

Available from <http://tinyurl.com/4pa9fy>

Other information sources

The Privacy Commissioner <http://www.privacy.gov.au>, see also the OPC's list of Privacy Service Providers <http://www.privacy.gov.au/links/service/index.html>

Royal Australian College of General Practitioners (RACGP)

<http://www.racgp.org.au/privacy>

<http://www.racgp.org.au/gpcomputing>

General Practice Computing Group (GPCG)

www.gpcg.org.au

http://www.gpcg.org.au/index.php?option=com_content&task=view&id=75&Itemid=107

Disclaimer

The information contained in the "Privacy guidelines for reuse of information" tool is provided as a guide only and is not intended to be a substitute for independent professional advice. References to websites are provided for the user's convenience only and do not constitute Endorsement of material at those sites, or any associated organisation, product or service. The Commonwealth Department of Health and Ageing does not warrant or represent that the information contained in the "Privacy guidelines for reuse of information" toolkit is accurate, current or complete. Users should exercise their own independent skill or judgement or seek professional advice before relying on it. The Commonwealth Department of Health and Ageing does not accept any legal liability or responsibility for any injury, loss or damage incurred by the use of, or reliance on, or interpretation of, the information contained in the "Privacy guidelines for reuse of information" tool.

Appendix – Register of Personally Identifiable Information Template

Personally Identifiable Information Register					
WHAT List all instances of Personally Identifiable Information	WHY Give specific reasons for collection	WHERE ... is the information used? NB: map onto WHYs	HOW ... is it gathered?	WHEN ... is it gathered?	WHO [ELSE] ... outside the Division will this information be disclosed to?
1.					
2.					
3.					

End of Document