

nehta

**Electronic Transfer of a Prescription**

**Preliminary Privacy Impact Assessment**

26/06/2009 (version 0.4)

---



## Contents

1	Executive Summary .....	6
2	List of Abbreviated Terms Used .....	10
3	Project Outline.....	11
3.1	Overall Aims: .....	11
3.2	What is a Privacy Impact Assessment? .....	12
3.3	This PIA study: .....	13
3.4	Process taken: .....	13
3.5	Scope: .....	14
3.5.1	In Scope:.....	15
3.5.2	Out of Scope: .....	15
3.6	Links with other projects:.....	15
3.7	Personal Information to be Handled:.....	16
3.8	Type of Information Collected: .....	16
4	Information Flows.....	17
4.1	Change in Terminology: .....	17
4.2	Mapping the Information Flows.....	18
5	Mapping Flows to Principles.....	20
5.1	Privacy Principles to be applied .....	20
6	Collection .....	20
6.1	The collection process:.....	20
6.2	Personal Identifiable Information being Collected: .....	20
6.2.1	Collection at registration (current practice) .....	20
6.2.2	Collection during an appointment.....	21
6.2.3	Information collected for prescriptions.....	21

6.3	Will information be collated from other sources?.....	22
6.4	Can other languages be used? .....	23
6.5	Information Confidentiality:.....	23
6.6	Which agencies need the data? .....	24
6.7	What is de-identified data?.....	25
6.7.1	Is de-identified data appropriate for the ETP system?.....	26
6.8	Can individuals choose what information they supply? .....	26
6.9	Are individual’s informed of the choices they have?.....	27
6.10	Are the organizations open about their policies?.....	27
7	Use .....	27
7.1	Uses relating to Purpose .....	27
7.2	Changes to Purpose.....	28
7.2.1	In General.....	28
7.2.2	Dispense Notifications .....	29
7.3	Protection over Secondary Use.....	30
7.4	Linking and Matching .....	30
8	Disclosure .....	30
8.1	Disclosing to third parties .....	30
9	Access and Correction .....	32
9.1	Individual Access .....	32
9.2	Correction to Information Held.....	33
10	Data Security.....	34
10.1	Security Measures .....	34
10.1.1	Backup and Audit Security .....	35
10.2	Outsourcing .....	35

10.3	Access Rights .....	35
10.4	Prevention of Inappropriate Access.....	36
10.5	Breach Notification .....	36
10.6	Retention and Destruction .....	36
11	Data Quality .....	37
12	Identity Management .....	37
12.1	Anonymity .....	38
12.2	Transborder data flows .....	38
12.3	Sensitive information .....	38
13	The risks with the PDP.token .....	39
13.1	Comment and Analysis.....	40
13.2	Risk Analysis .....	41
14	Management Recommendations .....	45
14.1	As a High Priority:.....	45
14.2	As a Medium Priority:.....	45
14.3	As a Lower Priority: .....	46
	Appendix .....	47
	Questions addressed in the PIA Information Mapping .....	47
	National Privacy Principles (NPPs) .....	53

# 1 Executive Summary

- ❖ A Privacy Impact Assessment (PIA) has been undertaken on the proposed Electronic Transfer of a Prescription (ETP) project to provide a high level analysis and recommendations on the most pertinent privacy aspects to the electronic Medication Management (eMM) team.
- ❖ For the purpose of this PIA the scope has been restricted to: 1) the exchange of electronic prescribing and dispensing messages that incorporates paper based prescriptions, and; 2) the ability for a healthcare provider to review the electronic dispensing history of a given prescription.
- ❖ A high level mapping of the information flows was undertaken to capture the complete context of the prescription service system and to identify which information contained personal information. The map was enhanced to include flows to external connections that are expected for a working information system, e.g. back up and audit functions.
- ❖ The PIA took into account the developmental nature of the ETP project (which at the time of this PIA was half way through the solution development stage) and therefore incorporated the changes in terminology that were being introduced as the business requirements and standard document templates evolve.
- ❖ The main focus for this PIA has been on the impact of integrating an electronic system alongside the existing paper-based systems (noting that the existing Pharmaceutical Benefits Regulations only deals with paper-based prescriptions).
- ❖ One key additional feature with the introduction of the electronic system is the proposed unique identifier for each prescription, now referred to as the 'PDP.token'. Analysis showed that the token was central to many of the privacy requirements. Hence, a more detailed analysis and risk assessment was undertaken in regard to the PDP.token to determine its suitability and robustness for providing the necessary protections.
  - This PIA study found that the PDP.token presents a reasonable mechanism for securing and protecting the privacy of personal information held on the Prescription Exchange Service (PES) providing it can be generated in a secure and dependable manner and that suitable precautions were made to ensure lists of PDP.tokens are not kept.
- ❖ Another main consideration brought about by the introduction of the electronic service is the ability for a Prescriber to be informed when a particular prescription

has been dispensed, i.e. 'Dispense Notifications'. This is a feature that is not normally tracked with the current paper based system (although there is a clinical relationship with a prescriber and dispenser today where this information is shared when required). This raised the following issues:

- It was noted that the commercial eRx system includes the options of recording both the agreement of a patient to use an electronic prescription service and the fact that they have given consent for Dispense Notifications. (Note that, it is not clear at this stage if this consent information collected by the Prescriber's system gets sent to the eRx Script Exchange service and on to the Dispenser).
  - This PIA considered the necessity with the proposed PES to provide such consent over and above the general consent given when registering with the Prescriber's practice.
  - This PIA found that an individual does not need to provide explicit consent that would be recorded on the PES to permit the use of electronic prescriptions.
  - This PIA found that with regard to additional functionality of Dispense Notifications, that this might be regarded as a secondary use and would not necessarily meet an individual's expectations, that such notifications would have to be considered 'necessary' for the provision of a health service and that such notifications were collected in accordance with rules established by competent health or medical bodies, unless the individual explicitly consented to this dispense information being disclosed.
  - The issue of how to deal with Dispense Notification, since it deviates from current practice, will need to be addressed. It is recommended that this is referred to the appropriate reference groups for further consultation.
- ❖ This PIA study has identified that the specifications given in the Structured Document Template make it mandatory to provide personal information that has previously been optional with paper-based systems. Some of this information is a legal requirement for claiming from Medicare, for example residential address. With individuals who choose to pay privately the information provided on a paper based prescription is at the discretion of the Prescriber, for example with newly arrived overseas students. From a privacy perspective, it is important to provide the Prescriber with the discretion of choosing what information will be entered in the mandatory fields on the PES to accommodate situations when an individual has special circumstances or chooses to refrain from providing certain personal details.

- ❖ It was noted that in the Structured Document Template that English is specified as the default language for the PES. Current prescription practice allows for a second language to be added on the paper based prescriptions and drug labels and this option is utilised in some communities. The continuation of this practice will need to be considered to cover any implications from a safety viewpoint. From a Privacy perspective, second language labelling on prescriptions and medicines is not required but it is recommended that access to the relevant privacy policies should be made available in other languages wherever possible.
- ❖ The current practice for prescriptions provides an individual with choice over how their confidentiality may be handled. For example, they may choose to go private and not have their details disclosed to Medicare through PBS online and they also may select which Dispenser will handle their prescription. The proposed ETP Solution accommodates these choices. From a privacy perspective, it is important that any future changes to the proposed ETP design do not result in the removal of these options.
- ❖ The proposed electronic prescription includes a data item referred to as the 'confidentiality indicator'. The definition and use of this item has not been given and its exact meaning is still under debate. This PIA has identified a high risk for the use of such an indicator while it is undefined. That is, the expectations of the individual as explained by the Prescriber on how their confidentiality will be handled may differ from what happens in practice by a Dispenser who has a different understanding. The privacy impact depends on how a Dispenser uses and discloses the personal information based on their interpretation of the meaning of the confidentiality indicator. It is therefore recommended that the definition and application of a confidentiality indicator should be considered as a high priority.
- ❖ The proposed ETP solution introduces an electronic record of the prescription that duplicates what is printed on the paper version. Consideration of how an individual can request access to the contents of the electronic version and request modifications will need to be incorporated if they believe the personal information held about them is incorrect. From a privacy perspective, it is important that the avenues to achieve this are not cut off by the introduction of an electronic version.

- ❖ In summary, the analysis undertaken has shown that the proposed approach would satisfy the Privacy requirements provided the higher risks identified can be suitably addressed. This PIA has developed a number of recommendations (see Section 14 for more detail). They have been prioritised to reflect the importance on the effects over the ETP designs currently under development to include:
  - As a High Priority:
    - Resolve the issue of consent for Dispense Notification by referring to the appropriate reference groups for further consideration.
    - Provide clear definitions on the confidentiality indicators and their use.
    - Ensure robust mechanisms are employed for generating PDP.tokens in a secure and dependable manner.
  - As a Medium Priority:
    - Develop methods and policies that minimise the risk associated with the creation of lists of previously assigned PDP.tokens.
    - Standardise the terminology used in the ETP project associated with the various sub-systems and encryption keys.
    - Provide the Prescriber with the discretion of choosing what information will be entered in the mandatory fields on the PES to accommodate situations when an individual has special circumstances.
  - As a Lower Priority:
    - Include specifications of the back-up and audit functions of the PES to ensure that personal data is only stored in encrypted form which is protected by the proposed PDP.key.
    - Ensure that individuals can readily access the applicable privacy policies associated with eMM and wherever possible provide these policies in other commonly used languages, in line with Government practice (e.g. Medicare and Centrelink).
    - Provide suitable access mechanisms (e.g. via the Prescriber or Dispenser) that permits individuals to exercise their right to access any personal information stored electronically and to request corrections to errors if necessary.

## 2 List of Abbreviated Terms Used

ABN - Australian Business Number

eMM = electronic Medication Management

EDS - Electronic Dispensing System

EPS - Electronic Prescribing System

eRx = Electronic Script Exchange gateway

ETP = Electronic Transfer of a Prescription

GP = General Practitioner

HPI-I = Healthcare Provider Identifier (Individual)

HPI-O = Healthcare Provider Identifier (Organisation)

IEHR = Individual Electronic Health Record

IHI = Individual Healthcare Identifier

NPP - National Privacy Principles

PBS = Pharmaceutical Benefit Scheme

PDP.key = Prescription Dispensing 128 bit (encryption key)

PDP.id = Prescription Dispensing 128 bit (identity key)

PDP.token = Prescription Dispensing 128 bit (token) i.e. bar code 'master' key

PES = Prescription Exchange Service

PIA = Privacy Impact Assessment

SDT = Structured Document Template

## 3 Project Outline

### 3.1 Overall Aims:

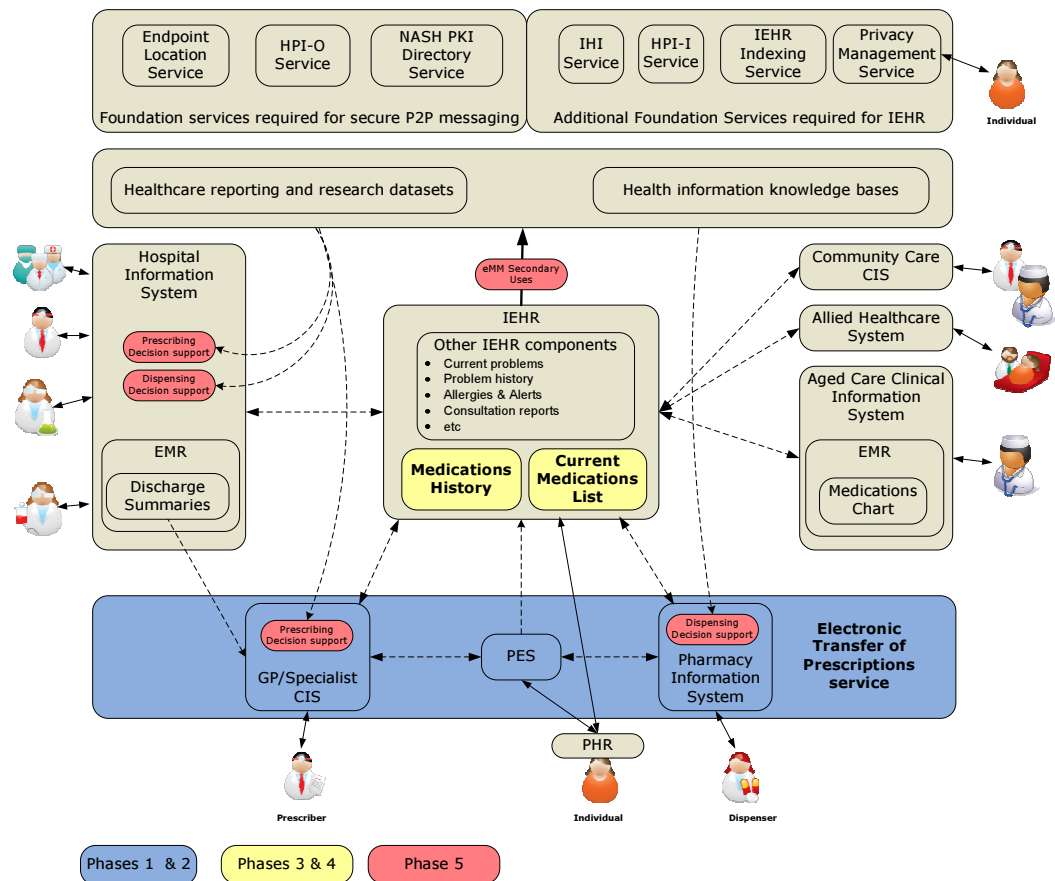
Electronic Transfer of a Prescription (ETP) is a project that aims to provide electronic transfer of essential prescription information between a Prescriber (e.g. a G.P.) and a Dispenser (e.g. a Pharmacist). The ETP project aims to provide the documentation required to specify how this electronic prescription service will function. The benefits and capabilities of the ETP project are outlined in a Concept of Operations document (version 0.8). The functional specifications and requirements for electronic prescriptions are detailed in the following documents:

- Business Process and Requirement Specifications (version 0.04);
- Standard Document Template – ePrescribing: General Practitioner to Community Pharmacist (Version 0.6 – 17/03/2009).

The ETP services, as shown in Figure 1, will form one component of a set of healthcare service provisions that will link healthcare information electronically.

Privacy is an important requirement with all healthcare service provision. The overall aim was to undertake a Privacy Impact Assessment (PIA) on the proposed Electronic Transfer of a Prescription (ETP) project. The PIA had to take into account the developmental nature of the ETP project which was half way through the solution development stage.

This PIA needed to incorporate changes in terminology that were being introduced as the business requirements and standard document templates evolve. The scope of the PIA was restricted to: 1) the exchange of electronic prescribing and dispensing messages that incorporates paper based prescriptions, and; 2) the ability for a healthcare provider to review the electronic dispensing history of a given prescription.



**Figure 1: Overview of eMM and related services**

### 3.2 What is a Privacy Impact Assessment?

A Privacy Impact Assessment (PIA) is a tool that can help determine if an organisation is following their vision and values, and can reduce the risk of not meeting their contractual and legal obligations. A PIA has been defined as “an assessment of any actual or potential effects that the activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated”. A PIA considers the future consequences of a current or proposed action, and looks to prevent or minimise any negative impacts on privacy. In designing or managing any project or system, there may be several competing public interests to be considered, including the protection of privacy. Decision-makers need tools to assist them to get the balance right. A PIA is one such tool. Where legal rights and obligations are affected, the reassurance offered by a PIA can be important as a risk management tool and as a way of building trust.

Risk management “impact” itself is a neutral term. Privacy impacts can be positive (privacy-enhancing) or negative (privacy-invasive). A PIA should examine both, but primarily the focus will be on the negative impacts. Privacy “risk” means the risk that a project will not comply with privacy laws, will not meet community expectations, or will have unmitigated or unnecessary negative impacts. A PIA can give confidence to those taking action—and those who will be affected by it—that the impact on privacy has been considered, and any

risks arising have been appropriately addressed. In other words, a PIA is a tool which should offer both a diagnosis of a project's well-being in terms of its privacy impacts, and a prescription of ideas to help treat any problems diagnosed.

Privacy risk can be avoided or mitigated by:

- ensuring a project complies with the law;
- ensuring a project meets community expectations;
- making a project less privacy-invasive; and
- making a project more privacy-enhancing.

*As with any process of risk management, you may not be able to eliminate or mitigate every risk, but ultimately you have to judge whether the public benefit to be derived from the project will outweigh the risk posed to privacy.<sup>1</sup>*

### **3.3 This PIA study:**

This PIA will be a high level analysis leading to an executive report of recommendations based on the scope defined below. It is understood that further more detailed analysis may be necessary once the full information flows have been mapped by the eMM team. The steps to be undertaken in this PIA include:

- Project Outline;
- Information Flows;
- Mapping Flows to Principles;
- Establishing Compliance Exposure;
- Analysing Risks and Impact;
- Mitigating Unacceptable Risks;
- Legal Standing;
- Management Recommendations.

### **3.4 Process taken:**

The process taken for the PIA involved study of the supplied documentation (as detailed in the following section), interviews with members of the eMM team, interim reporting and

---

<sup>1</sup> Blair Stewart, "Privacy Impact Assessments", (1996) 3 *Privacy Law + Policy Reporter* 61, 62

feedback on progress together with presentation of the key recommendations to the eMM management team.

The PIA was carried out by Dr Peter Croll (Consultant) in consultation with the following members of the Privacy and Policy section in NEHTA:

- Tonya Rooney (A/g Manager, Privacy)
- Miranda Margetts (Privacy Advisor).

The members of the eMM team consulted include:

- Toby Mathieson (Program Manager, eMM Package)
- Jane Connolly (Project Manager, eMM Package)
- Andrew Zander (Solutions Architect)
- John Taylor (Subject Matter Expert - eMM Package)

In addition, a presentation was provided to Paul Williams (Head of Solution Development) and the eMM management team on the key recommendations of the PIA.

### **3.5 Scope:**

The Concept of Operation document (ver 0.8) identifies 5 capabilities for the eMM service.

These include:

1. Exchange of electronic prescribing and dispensing messages;
2. Adherence monitoring;
3. Current Medication Lists;
4. Medication History Lists, and;
5. Medication Decision Support and Secondary Uses.

The plan of the eMM project team is to phase in these services.

The proposed approach taken will allow for integration with existing paper-based prescriptions (note that currently the prescription legislation<sup>2</sup> only deals with paper-based prescription). Modification to the paper-based system is necessary to include a unique identifier on each prescription (known as the PDP.token) that can be read both manually and electronically. The aim of the eMM project team is to ensure that the specifications produced also support future implementations that do not rely on the paper prescriptions.

---

<sup>2</sup> *National Health (Pharmaceutical Benefits) Regulations 1960 (Cth) Part V 19 (1)(d)*

The Concept of Operation documentation and the associated Business Process and Requirement Specifications (ver 0.04) are both in draft form at the commencement of this PIA study. They will continue to be developed by the eMM project team and refined based on feedback from their Reference Group. This PIA may provide recommendations that contribute towards the ongoing design and development of the ETP project.

### **3.5.1 In Scope:**

It was agreed that the PIA will include capabilities 1) plus an initial component of Adherence Monitoring under capability 2) as outlined in the Concept of Operation document. That is:

1. Exchange of electronic prescribing and dispensing messages:  
*this capability is concerned with the generation and exchange of electronic records that represent prescriptions and their associated dispensing records.*
2. Dispense status checking:  
*this capability introduces the ability for a healthcare provider to review the electronic dispensing history of a given prescription.*

These are covered by Phases 1 & 2 as shown on the overview diagram, figure 1.

Furthermore, the PIA considers the implications from the proposed modifications to the existing paper based system e.g. adding a bar code and manually readable identifiers.

### **3.5.2 Out of Scope:**

Capabilities 3), 4) and 5) (as reflected in Phases 3, 4 and 5 at Figure 1) are considered out of scope for the purpose of this study.

This PIA will only consider:

- a) the initial hybrid paper-based implementation. Therefore, the fully electronic only version is considered out of scope;
- b) the impact of introducing a unique identifier (PDP.token) to paper-based prescriptions. Therefore, issues with the current paper-based prescriptions, not resulting from the changes introduced by the eMM, are considered out of scope;
- c) the high level information flows supplied and derived from this study prior to July 2009. Therefore, detailed information flows under development by the eMM project team after June 2009 are considered out of scope.

The exceptions to the above is when critical issues are identified as part of this study that in the opinion of the Privacy team should be commented on for further consideration.

## **3.6 Links with other projects:**

The eMM project has direct links with other NEHTA and external ehealth projects. The overview diagram, Figure 1, shows the other key services. Of particular interest to this PIA

are: 1) the Secure Messaging project that will provide the transportation of secure messages between providers and services; and 2) the Identifiers projects to include the IHI services and the HPI-O services. The Individual Electronic Health Record service and the Hospital Information Systems that include the Electronic Medical Records and Electronic Discharge services are of future interest but considered out of scope for this PIA.

### **3.7 Personal Information to be Handled:**

Prescription services require that an individual concerned is identified by both the Prescriber and Dispenser. Furthermore, to claim back for prescription costs on the Pharmaceutical Benefits Scheme (PBS)<sup>3</sup> there is a legal requirement to provide certain personal information. There are some exceptions to this to allow for special circumstances that involve highly sensitive information. Whatever method is selected for determining what information will be collected, as detailed in this report, it is essential that the person who presents to a Prescriber is the person to whom the prescription is dispensed (either directly or via an authorised carer).

### **3.8 Type of Information Collected:**

The personal information collected will include information that demonstrates that the person who presents is who they say they are. It will include contact details to allow an individual to be contacted, for example, in case of an error or when prescriptions are ready for collection. When claiming back on the PBS further personal details are required to include residential address and issued government identifiers e.g. a Medicare number.

The Prescriber may request other details associated with provisions of care, e.g. current or previous medications prescribed. The full details of the information collected is detailed in the 'Structured Document Template - ePrescribing: General Practitioner to Community Pharmacist' (Version 0.6 – 17/03/2009).

---

<sup>3</sup> Further information can be located on the Pharmaceutical Benefits Scheme at: <http://www.pbs.gov.au/>

## 4 Information Flows

Information flows that relate to Privacy requirements have been mapped for the ETP project.

The information flow map has been derived from the basic scenarios and architectural diagrams provided in the Concept of Operation document (version 0.8) and the Business Process and Requirements Specification (version 0.04). This information flow map, shown in Figure 2, represents a refinement of the documented design based on interviews with the eMM team members.

The key differences of the information flow map are that it shows:

- 1) the inclusion of external flows outside of the specified requirements, e.g. communicating with Medicare, data backup, auditors and discarded or lost prescriptions;
- 2) which information contains identifiers (in red arrows) that could be used to readily identify a person;
- 3) the complete context of the system under analysis for the purpose of the PIA, and;
- 4) the flow map on a single sheet to help determine completeness.

It does not show the internal communications of self contained computer systems, e.g. the internal workings and communications across of the set of applications that make up a GP's Health Record System.

### 4.1 Change in Terminology:

Some of the terminology has been changed from the original Concept of Operations diagrams based on the updates given in the interviews and terms used in the Business Process Requirements. These include:

- 1) *Electronic Prescribing System* replaces GP/Specialist Computer Information System (CIS);
- 2) *Electronic Dispensing Systems* replaces Pharmacy Information System (PIS);
- 3) *PDP.token* replaces Master key or Prescribing Process Identifier (PPID);
- 4) *PDP.id* has been introduced to show the search key generated by the *PDP.token*;
- 5) *PDP.key* has been introduced to show the key used to encrypt the prescription.

*Italics* is used to indicate a term used on the information flow map.

**Recommendation:** Standardise the terminology used in the ETP project associated with the various sub-systems and encryption keys.

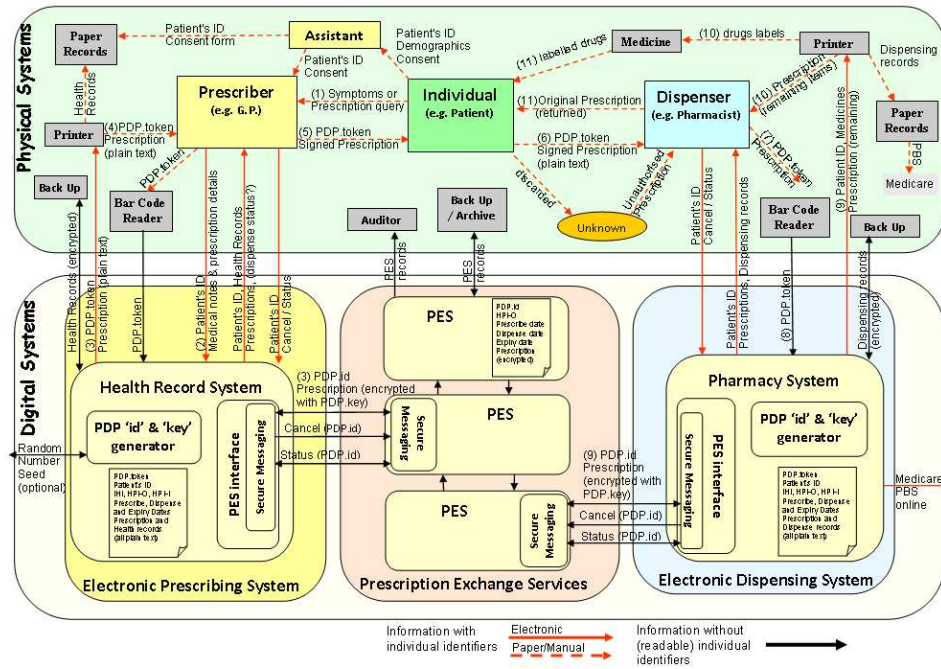
## 4.2 Mapping the Information Flows

The purpose of this stage of the PIA is to describe and map the flows of personal information in the project. The information compiled during this stage will form the basis for the forthcoming analysis of privacy impacts.

The elements of the project that are most likely to be relevant to information privacy impact include:

- the collection of personal information;
- its use and disclosure;
- the ability individuals have to access information about them;
- the ability individuals have to correct information about them if need be;
- the applicable security safeguards;
- the processes for ensuring data quality; and
- whether an identity management system is involved.

Figure 2—Information Flow Mapping for the Electronic Transfer of a Prescription (ETP) project



## **5 Mapping Flows to Principles**

### **5.1 Privacy Principles to be applied**

Information privacy legislation governs the handling of individual's personal information, including health information. The legislation aims to protect an individual's right to privacy while at the same time supporting the benefits of the free flow of information.

Currently, Australian privacy laws are a complex patchwork of legislation and guidelines across governments and private sectors. The National Privacy Principles (NPPs) found in the Privacy Act 1988 (Cth) apply to all health service providers in the private sector. The NPPs are broadly applicable and closely reflect the proposed future changes for the Privacy Act.

Privacy Laws are intended to define principles to be followed and do not, therefore, prescribe any particular technological solutions for organisations to implement. NEHTA does therefore not intend to prescribe which technology should be used, but rather seeks to provide guidance as to best privacy practice to ensure the technological solutions implemented ultimately meet the expectations of national privacy standards.

## **6 Collection**

### **6.1 The collection process:**

Information is normally collected by the Prescriber (e.g. General Practitioner) when an individual presents for an appointment relating to their health and wellness. Under privacy laws, consent is not always required for the collection of information when a health service is being provided. (See NPP 10.2). Where consent is required, often implied consent is relied on. In some instances, healthcare providers may seek explicit written consent from the individual (e.g. at the point of initial registration with a service) in relation to the handling of personal information, or in relation to the secondary use of information such as for research. Consent forms used by healthcare providers are not standardized and hence may differ from one health service provider to another. The recording of an individual's consent electronically is not standard practice. The standard consent forms used by Prescribers do not normally make any direct reference to prescription services.

### **6.2 Personal Identifiable Information being Collected:**

#### **6.2.1 Collection at registration (current practice)**

It is necessary to collect personal information relating to an individual that provides assurances over their identity. This is required for both healthcare safety and to minimize

fraud. When registering with a health service provider an individual will usually be asked to provide their full name, date of birth, sex, and residential address, Medicare number and any Private Healthcare number. Some practices may request a photo identity depending on their local policy.

Notwithstanding these requests for personal details an individual does have rights to obtain healthcare provision without necessarily providing all the requested information. When the healthcare is more sensitive, e.g. sexual and mental health, special provisions may be made to accommodate individuals who wish to remain anonymous. Detailing the full range of options for identification and healthcare provision is considered outside the scope of this study. Although it should be noted that accommodating for individuals who have not provided their full identity should be included in any ETP system. Whatever method is selected it is a requirement to safely link a prescription to the individual for whom it was prescribed.

### 6.2.2 Collection during an appointment

Information not collected at the time of registration may be requested when an individual presents for an appointment. This will normally be additional registration information required for Medicare or Prescription services that has not been previously recorded or information that may have changed since the individual's last appointment. The previous consent obtained at registration would normally be regarded by the health service provider as adequate to cover such additional requests. This may happen at the front desk or during the appointment with the Prescriber. It is generally on an ad-hoc basis. Some practices may have a policy to check personal details periodically (e.g. annually) and/or check essential details (e.g. current address) on every visit. An individual can volunteer at anytime to change their details as a result of, for example, moving house or name change through marriage. The practice may require individuals to provide some evidence of these changes depending on their policy.

### 6.2.3 Information collected for prescriptions

The information that will be collected from individuals for the purpose of providing an electronic prescription is defined in the Structured Document Template - ePrescribing: General Practitioner to Community Pharmacist (Version 0.6 – 17/03/2009). The individual to whom the prescription applies is referred to as the "Subject of care".

NAME

(This is labelled as the 'Role Name' for the Subject of Care).

ENTITY IDENTIFIER

**(Must** contain the Individual Healthcare Identifier (IHI) if available and **Should** include the patient's Medicare Number (including the individual reference number) or Veterans' Repatriation entitlement number).

#### ADDRESS

(**Must** include residential address).

#### ELECTRONIC COMMUNICATION DETAILS

(Inclusion of the subject of care's preferred means of contact should be included to facilitate clinical follow-up. A subject of care may have more than one method of contact.)

#### PERSON NAME

(**Must** contain name details and name usage type. Name may be required as both a visual prompt for reading the prescription, and as an electronic aid for linking to the subject of care's electronic record. It may therefore be necessary to include multiple names, including preferred and legal names (and known aliases))

#### PERSON ADDITIONAL DEMOGRAPHIC DATA

**Must** contain the following details: Date of Birth (can be estimated), Sex

### 6.3 Will information be collated from other sources?

The normal method of collecting information is outlined above. When essential information is missing then, depending on the policy of the practice, it may be collected by other means. Normally, this would be obtained by phoning the individual concerned or referring to the health records kept within the practice. They may write to the patient if they cannot be contacted by phone. With prescriptions they are normally completed when the patient is still present and information can be collected directly from the individual as described above. It is feasible that a prescription is completed when the patient is not present, although this would be the exception and not permitted under some legislation (e.g. some States and Medicare). The proposed electronic PES system does not allow a prescription to be issued when mandatory information is incomplete. Note that, the fields which are mandatory are defined in the Standard Document Template (SDT). The PES requires more mandatory information when compared with the current paper based prescriptions. There is a risk that the Prescriber may collect the additional mandatory information from other sources to complete an electronic prescription if the Prescriber cannot find out directly from the patient. The privacy impact with this risk of collecting from others sources is that it may not be accurate and up to date information and may link the individual in a way that they would not be agreeable to, e.g. using an address for a teenager who is no longer living at his parents' home.

**Recommendation:** Provide the Prescriber with the discretion of choosing what information will be entered in the mandatory fields on the PES to accommodate situations when an individual has special circumstances.

## 6.4 Can other languages be used?

There are requirements that English (Australian) is used on the prescription, any drug labels and throughout the PES. A second language can be utilised for individuals with a limited understanding of English. For example, Cantonese (written using Chinese characters) is commonly used in the Sunnybank community of Brisbane when appropriate. The mandatory requirement is for English to appear on the prescription and drug label and a second language can be used as an option. The specification of the Standard Document Templates for use in the PES accommodates English language as the default and can only accept English characters (i.e. Latin based alphabet). It would be the responsibility of the Electronic Dispensing System to produce other language labels on medicines, if appropriate, at the discretion of the Prescriber.

When individuals are provided with written information regarding privacy issues or asked to complete forms that give consent this would normally be in English. The practice concerned may have a policy to explain in other languages when their staff are able to assist. To reduce the risk that individuals do not understand what they are agreeing to in regard to how their personal information is handled the opportunity, with the move to electronic systems, to explain the privacy policies in commonly used languages should be considered.

Organizations that do this normally make the provision on the Web or via dedicated phone lines with a reference on the printed documents in different languages on where to find this information.

**Recommendation:** Ensure that individuals can readily access the applicable privacy policies associated with eMM and wherever possible provide these policies in other commonly used languages, in line with Government practice.

## 6.5 Information Confidentiality:

A tag for a 'Confidentiality Indicator' is provided for in the Structured Document Template. There is no specification for its format or its purpose provided in the documentation. Discussions with members of the eMM team reveal that the Confidentiality Label has been included to allow for its future use. While the Confidentiality Label remains unspecified there is a risk of misinterpretation in its use. That is, the expectations of the individual as explained by the Prescriber on how their confidentiality will be handled may differ from what happens in practice by a Dispenser who has a different understanding. The privacy impact depends on how a Dispenser uses and discloses the personal information based on their interpretation of the meaning of the confidentiality indicator.

NPP2.1 requires that an organisation cannot use or disclose personal information about an individual for a purpose other than the primary purpose. A secondary purpose, such as marketing or research, is only permitted when specific conditions apply. NPP2.1 (a) allows

for secondary use if it can be demonstrated that the secondary purpose is related to the primary purpose. Furthermore, with sensitive information, such as health information, the secondary purpose would have to be 'directly' related to the primary purpose. Examples, of a directly related purpose would include any checks done by a Dispenser to ensure quality control and safety for the individual concerned. It would not include providing information for marketing purposes to pharmaceutical companies. NPP 2.1 (b) allows secondary use when an individual would reasonably expect a disclosure to happen. For example, disclosing information to other staff working at the Dispenser's organisation would be considered reasonable; whereas passing information to a university research unit would not. Note that both conditions in NPP2.1 (a) and (b) must apply, hence for health information, secondary use must be directly related to primary use and any disclosure would be something that the individual concerned would expect to happen. The only exceptions with health information is when an individual consents to the use and disclosure for the specific secondary use (e.g. they give consent for their information to be used for research) or when there is a safety concern to include serious risk of harm to the individual or a case can be made relating to public health safety.

The concept of providing different confidentiality levels has been addressed before in NEHTA privacy workshops.<sup>4</sup> These workshops have found this to be a complex and sometimes contentious topic. Recommendations in NEHTA's Privacy Blueprint for the IEHR state: "...it is proposed that the functionality for sensitivity labels should be allowed for in the IEHR design but that further detailed analysis, including cost/benefit, is required".

**Recommendation:** The definition and application of a confidentiality indicator should be considered as a high priority. As an interim measure the confidentiality indicator should be specified as 'reserved' and clearly stated that this is reserved for future application and cannot be assigned any value.

## 6.6 Which agencies need the data?

On the front of the prescription just above where the individual signs their name is printed the wording: "Please turn over for privacy note". On the back of the prescription the following 'Privacy Note' is printed that informs the individual which agencies will be provided with the information that is recorded on the prescription.

**Privacy Note:**

The information recorded on this form, including your Medicare, Centrelink and/or Department of Veterans' Affairs number, will be used to assess your entitlement to benefits under the Pharmaceutical Benefits Scheme, and Repatriation Pharmaceutical Benefits

---

<sup>4</sup> See 'sensitivity labels' in NEHTA Privacy Blueprint for the Individual Electronic Health Record, 2008

Scheme, and to determine the payments due to pharmacists. With your consent, the pharmacist or doctor may store your Medicare number for use on future scripts. The collection of this information is authorised by the National Health Act 1953 and may be disclosed to the Department of Health and Ageing, Department of Veterans' Affairs and Department of Human Services or as authorised/required by law. This information may also be disclosed to doctors and pharmacists.

It is noted that no reference is made to where an individual should go to obtain a full privacy policy and if this is made available in other languages.

An individual who chooses to go private and does not wish to claim back from the PBS does not need to sign the prescription. The Privacy Note contains information that would not be applicable to private patients (i.e. those that have 'NON PBS' is printed on their prescriptions). The Privacy Note shown above contains generic information about privacy and does not necessarily constitute a set of terms and conditions that an individual is consenting to agree with by signing.

**Consideration:** A reference is provided on the prescription to where an individual can find the full set of privacy terms and conditions and which ones would apply to private and PBS claimed prescriptions respectively.

## 6.7 What is de-identified data?

Privacy laws apply to personal information – that is identifiable (and in some instances re-identifiable) data. It is therefore important to be able to make a distinction between identified or de-identified data, as different requirements apply.

The term 'de-identified' data is commonly used but can be misleading. The [National Statement](#)<sup>5</sup> clarifies this by using three different terms as follows:

- a) **Individually Identifiable data** – this is data which has information that would allow the person concerned to be readily identified.
- b) **Re-identifiable data** – this is data that has had the personal information removed (e.g. names and addresses) but can still be linked back to the individual concerned when necessary. Typically, the name and address may be replaced with a numeric identifier that can be linked back to the individual concerned (if necessary) by an organization with the linking information.

---

<sup>5</sup> [National Statement on Ethical Conduct in Human Research](#), published by NHMRC/AVCC (2007)

- c) **Non re-identifiable data** – this is data that has had sufficient information removed to make it highly unlikely that any individual can be identified from the data remaining. No linking information is recorded.

Note that even though identifiable information has been removed it can sometimes be possible to link information back to an individual based on inference with the remaining information. For example, if the name and address was the only information removed then a person's age, sex, post code and medical condition may be sufficient to allow an individual to be identified from a small population sample. Mechanisms to minimize these privacy risks are ongoing areas of research.

### 6.7.1 Is de-identified data appropriate for the ETP system?

This section considers if de-identified data can be used within the ETP system to provide greater privacy protection.

'Individually Identifiable Data' needs to be collected by a Prescriber from the individual for the purpose of registration and correct linking to any related medical records, as detailed in Section 6.2. The Dispenser will also need to check identifiable data when dispensing a prescription and will be required to keep records of this data for any PBS claims, etc.

The data held within the PES would be classified as 'Re-identifiable Data'. The PDP.token on each prescription is used to generate the relevant PDP.id which is the identifier used for locating a particular prescription stored within the PES. The PDP.token is also used to generate the PDP.key for decrypting the personal information contained within the electronic prescription. This is appropriate for giving privacy protection from unauthorised users yet allows for 'Individually Identifiable Data' to be decrypted when required on production of the PDP.token.

'Non Re-identifiable Data' is appropriate for secondary use. This would include research and other non primary purposes. The secondary use of data in the ETP systems falls outside of scope for this PIA.

## 6.8 Can individuals choose what information they supply?

There will be some circumstances when an individual cannot supply all the information required, for example when they have no current residential address. It is common practice for Prescribers to use the address of the practice in these circumstances. Individuals may wish to hold back information. This could apply when the information is relating to highly sensitive matters, for example, sexual and mental health. Other examples are when they wish to restrict information that they may not wish to be seen by certain people, e.g. relatives working in the health services or the media/press. It is important that a health service is not restricted and dependent on the provision of such information and allowances are needed to accommodate for special circumstances.

## **6.9 Are individual's informed of the choices they have?**

NPP 5 on 'Openness' requires an organisation to ensure that an individual can find out about how they handle their personal information. NPP 5.1 requires organisations to ensure they make documents available that describe how they manage any personal information they hold. NPP5.2 requires that an organisation on request should provide details about the type of personal information it holds, for what purpose and how it is handled. The Prescriber and Dispenser organisations will have to comply with these expectations and provide documents that clearly express their policies to include the choices an individual has. With the introduction of the proposed PES the individual has no direct way of accessing their personal information without going through a registered HPI-O. The Prescribers and Dispensers should amend their privacy policies where necessary to accommodate the ETP system.

## **6.10 Are the organizations open about their policies?**

NPP 5.1 requires that an organisation is open about its privacy policies. As detailed in the previous Section 6.9 above, the Prescribers and Dispensers should amend their privacy policies where necessary to accommodate the ETP system.

# **7 Use**

## **7.1 Uses relating to Purpose**

It is a privacy requirement that the way personal information is used should relate to the purpose for which it was collected. NPP 2.1 (Use and Disclosure) states that: "An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection". There are some permitted exceptions to include, for example, when an individual gives consent or when an individual would reasonably expect such use or disclosure to occur. In particular, with health information, exceptions apply when it is considered necessary for reasons of public health or public safety.

The personal information used by the Prescriber and Dispenser and stored in the PES should relate to the purpose of generating a prescription. This may also include information that is necessary for checking, auditing, safety and maintenance purposes that is not normally required for dispensing a prescription provided it can be justified. This section looks at what information is required and what is actually collected.

The 'Electronic Medication Management, Business Process and Requirements Specification Version 0.04 - 16/04/2009' document specifies (Process Description 2.2.1) the following details that will be required by the Dispenser:

*“The dispenser checks that the individual’s details on the paper prescription are complete. The individual details required are:*

- *Name*
- *Address*
- *Date of Birth*
- *Phone Number*
- *Concessional Entitlements*
- *Medicare number*
- *Allergies*

*If there are missing details the dispenser will request them from the individual.”*

The Structured Document Template provides details on the information collected for prescriptions as detailed in Section 6.2 above on ‘Personal Identifiable Information being Collected’. From analysis of these documents it would appear there is a discrepancy between what is collected by the Prescriber and what is actually required by the Dispenser. For example, Concessional Entitlements, Medicare Number and Allergies will be checked by a Dispenser or requested from the individual when missing.

While these discrepancies remain there is a risk that information will need to be supplied to and collected by the Dispenser that is not provided for on the PES. This PIA does not comment on the impact of these risks but assumes these discrepancies will be addressed in later versions of the related documents.

## **7.2 Changes to Purpose**

### **7.2.1 In General**

The information in the PES has a very specific purpose relating to the prescribing of medicines and prescription items for an individual. The individuals concerned have a right to be notified if there is any change in the purpose for which this information will be used.

There are protections in place to prevent the information being accessible for other purposes through the use of PDP.token keys that are unique to each prescription. The safety of these keys as a secure way of protecting any personal data is discussed in later sections. Any lists of PDP.tokens that would allow access to the PES data would need careful protection. This will reduce the risk of PES data being used for purposes other than the exchange of information relating to an individual prescription, provided these protections are in place.

The fact that an electronic system is employed primarily to improve patient safety is not regarded as a change of purpose from the necessary provision of the health service. Hence, with the proposed PES the necessity to provide explicit consent over and above the general consent given when first registering with the Prescriber’s practice is not required for using an electronic system that duplicates the same purpose, i.e. dispensing a prescription.

### 7.2.2 Dispense Notifications

The introduction of the electronic service now provides the ability for a Prescriber to be informed when a particular prescription has been dispensed, i.e. 'Dispense Notifications'. This is a feature that is not normally tracked with the current paper based system (although there is a clinical relationship with a Prescriber and Dispenser today where this information is shared when required). At this stage in the development of the ETP it has not been specified whether such notification will occur automatically. If the Prescriber wanted to look this up they would need the PDP.id (generated from the PDP.token) to access the relevant prescription on the PES.

Existing commercial systems, e.g. the eRx Script Exchange service ([www.erx.com.au](http://www.erx.com.au)), includes the options of recording both the agreement of a patient to use an electronic prescription service and the fact that they have given consent for Dispense Notifications. Note that, it is not clear at this stage (based on the demonstration provided on the web) if this consent information collected by the Prescriber's system gets recorded in the eRx Script Exchange service and then forwarded on to the Dispenser.

With regard to functionality of Dispense Notifications this could be regarded as an additional purpose. It therefore raises new privacy considerations.

NPP 2.1 requires that an organisation does not use or disclose personal information other than for its primary purpose. The primary purpose with dispensing a prescription would not necessarily include informing the Prescriber of dispense notification, i.e. informing when an individual chose not to pick up the prescription and what pharmacy they went to. On the one hand the Prescriber may consider dispense notification information as part of their duty of care and will act upon it as necessary. On the other hand they may use this information to determine which pharmacy is most likely to issue brand name over generic drugs. This raised the question of whether dispense notification could be regarded as a secondary use? If it is, then health information NPP2.1 (a) would require a dispense notification to be directly related to the primary purpose and that the individual would expect dispense notification to happen. Note that, dispense notifications would not necessarily meet an individual's expectations since it deviates from current practice. Although they may be aware that the Dispenser may share information with the Prescriber they have the option of intervening and requesting that a Dispenser does not inform the Prescriber. The Dispenser would be obliged to respect this request and would then dispense at their discretion. Note that NPP2.1 (b) would permit dispense notification provided the individual consented to such use and disclosure.

NPP10.2 on the collection of sensitive information, states that "information is necessary to provide a health service to the individual" and does not need explicit consent provided it is collected "in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation". This

additional purpose questions if Dispense Notifications is considered 'necessary' for the provision of a health service.

The rules in regard to what the "competent health or medical bodies" would apply for dispense notification are not clear.

**Recommendation:** Resolve the issue of consent for Dispense Notification by referring to the appropriate reference groups for further consideration.

### 7.3 Protection over Secondary Use

At this stage the legitimate secondary use of any information collected for the PES is out of scope of this PIA. Protection against unauthorised secondary use is necessary. For the same reasons given in Section 6.2.1 above under 'Changes of Purpose' the PDP.token keys will provide protection against unauthorised secondary use. The risks are minimal if the risks with the PDP.token are minimised.

### 7.4 Linking and Matching

The data stored in the PES can only be retrieved by the 128 bit PDP.id number. The PDP.id is generated from the PDP.token as detailed in Section 13. The PDP.token is located on the prescription in machine readable (bar code) and human readable formats. The PDP.token is also used to generate the PDP.key that is required to decrypt the personal information held on the electronic prescription stored in the PES. Hence, any linking and matching requires the PDP.token to first generate the PDP.id to retrieve the data from the PES then second to generate the PDP.key to decrypt the personal information. Linking and matching can only be achieved with the PDP.tokens and then only after decrypting the information. Since the PDP.tokens are not stored in the PES no linking or matching is achievable until the information has been retrieved and decrypted outside the PES. The PDP.token only provides the ability to access one prescription.

The PES records contain some plain text information that could be linked and matched. This includes PDP.id, HPI-O, Prescribe date, Dispense date and Expiry date. This information would not permit any linking to personal information contained within the PES.

## 8 Disclosure

### 8.1 Disclosing to third parties

One identified area of concern is where personal information on prescribed medicines is disclosed to, or accessed by, unauthorised third parties (whether deliberately or inadvertently). Whenever prescription information can be linked to an individual, good privacy protection is required to safeguard against potential privacy violations. In a recent

case in Australia, a pharmaceutical company was accused of re-identifying patients from health records in order to target them for a new drug. This is a potential high risk area and one that the community would generally regard as unacceptable practice.

The ETP project proposes a method for generating sets of keys to encrypt and protect data. An analysis of this is provided below, finding that this approach provides a reasonable level of security protection for message passing and storage (NPP 4.1). The analysis also suggests ways to limit the risk of unauthorised disclosure.

The only effective way that an individual can be identified from an encrypted PES file is through access using the PDP.token assigned to each prescription. The PDP.token is printed in both bar code and human readable format on each printed prescription. The token permits the decryption of the prescription by the Dispenser. The ETP project has also identified the requirement to include decryption by the prescriber necessary for safety and quality control procedures. The main risk is the local storage of PDP.tokens that link to individual identifiers within the Prescriber or Dispenser systems. That is, there is nothing to prevent a Prescriber from keeping records of prescriptions and the allocated PDP.tokens on their local Health Information System. They may consider this necessary to allow them to check the PES for prescriptions they have previously prescribed when doing quality and safety checks. Note that a Dispenser would not be able to do this until the individual presents a paper prescription with the bar code showing the PDP.token. The risk of unauthorised disclosure can be reduced by not allowing the storing of lists of PDP.tokens and by limiting access, e.g. only permitting a one-shot access policy for any HPI-O. The privacy impact is that a list of PDP.tokens could be used by any HPI-O to access the PES to disclose personal information. The potential risk is heightened by recent alleged claims made against a pharmaceutical company for paying nurses to access medical records<sup>6</sup>.

**Recommendation:** Develop methods and policies that minimise the risk associated with the creation of lists of previously assigned PDP.tokens.

The risks with keeping lists of PDP.tokens is discussed further in Section 13 on 'The risks with the PDP.token'.

---

<sup>6</sup> Commissioner to probe potential privacy breaches:  
<http://www.australianit.news.com.au/story/0,27574,25517817-15306,00.html>

## 9 Access and Correction

### 9.1 Individual Access

If an organization holds personal information about an individual then it must provide access to that information on request. NPP 6.1 states: “If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual”. There are some exceptions, for example when gaining access raises legal issues or relates to ongoing legal proceedings and, in the case of health information, if there is a serious threat to the safety of an individual.

The PES as proposed does not provide for direct access by individuals only by HPI-Os. The personal information is encrypted in the PES and can only be decrypted by an HPI-O’s system on production of the PDP.token. Note that this only allows for decryption of a single prescription as each prescription record in the PES is encrypted with a different key (i.e. the PDP.key) based on the unique PDP.token. Provided the requirement remains that only an HPI-O can access the PES then the individual will have to seek access via either a Prescriber or a Dispenser. As it stands the PDP.token is created by the Prescriber system each time a prescription is issued. Hence, for the Prescriber to access the record in the PES they will need the PDP.token. This will be available on the paper prescription and would allow an individual to request access on production of the paper prescription. They could also request a Dispenser to access the prescription using this method.

How an individual could request access to information without producing the paper prescription needs further consideration. They might for example present their Medicare card or other suitable ID and ask for a copy of their prescription history. Since it is only possible to access the PES by knowing the PDP.token then without a paper prescription a Prescriber would have to refer to the patient’s record on their Health Record System. They may have kept a record of the individual’s prescriptions together with each PDP.token that was issued. The Pharmacy System may also have a record after an individual has had a prescription dispensed by them. An individual will not be able to go to any Prescriber or Dispenser and request this information unless they have the paper-based prescription with the PDP.token. They will have to return to the original Prescriber or Dispenser to gain access to this information and they in turn will have to have kept a record with the PDP.token in order to access the PES.

Provided the Prescriber or Dispenser did not believe one of the exceptions (NPP 6.1 a-k) applied they would be obliged, on request, to inform the individual of the information that was being held on the PES system. They may choose to charge individuals for such requests (NPP 6.4.). While it may be impractical to provide the individual with a copy of their PES record (due to the fact it is encrypted), the individual would be entitled to access a copy of

their prescription information that is held with a Dispenser or Prescriber upon request (unless one of the exceptions under NPP 6.1 applies).

If the personal information kept in the PES remains identical to the personal information printed on the prescription and the individual was made aware of this, it would minimize the occurrences of such requests. When electronic only prescriptions come into common practice it is anticipated that requests for access could become more frequent and should be readily accommodated for.

## **9.2 Correction to Information Held**

If an individual can establish that the personal information held about them in the prescribing system is incorrect the organization would be required to correct that information or explain why they have not corrected it. That is under NPP 6.5 “If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up-to-date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up-to-date” and under NLP 6.7 “An organisation must provide reasons for denial of access or a refusal to correct personal information”.

For the PES system the most likely request for changes to personal details will come from changes to names, incorrect spelling of names and changes of contact details and residential address. A prescription may reside in the PES system for a period of time and it is not unreasonable that individual’s circumstances may change while a prescription is current. It is also highly likely that the Prescriber will enter outdated information that already resides on their health record system. The individual may not notice that, for example the address is wrong, until reading the prescription and after leaving the Prescriber. Depending on personal circumstances an individual may feel very strongly about outdated information particularly when they have for example had a relationship break-up. The organisation would need to have the capability of correcting both the prescription and the electronic record. The proposed approach with the ETP is to cancel a prescription and re-issue a corrected version. It is important from a privacy perspective to consider what might happen with the personal details on cancelled prescriptions and if they can for any reason be accessed at later dates, i.e. will they be marked as cancelled or deleted from the systems and any backups? From an audit perspective it would be appropriate to keep a note of any cancelled records to minimise fraudulent behaviour, etc. An audit function cannot reveal the encrypted payload containing the personal information since this requires the PDP.key generated by the PDP.token. Hence, it is recommended that the plain text record header is retained (possibly marked as cancelled) but the encrypted payload is deleted from the system whenever a prescription is cancelled. This will remove the privacy concern over outdated personal information being retrieved.

**Recommendation:** Provide suitable access mechanisms that permit individuals to exercise their right to access any personal information stored electronically and to request corrections to errors if necessary.

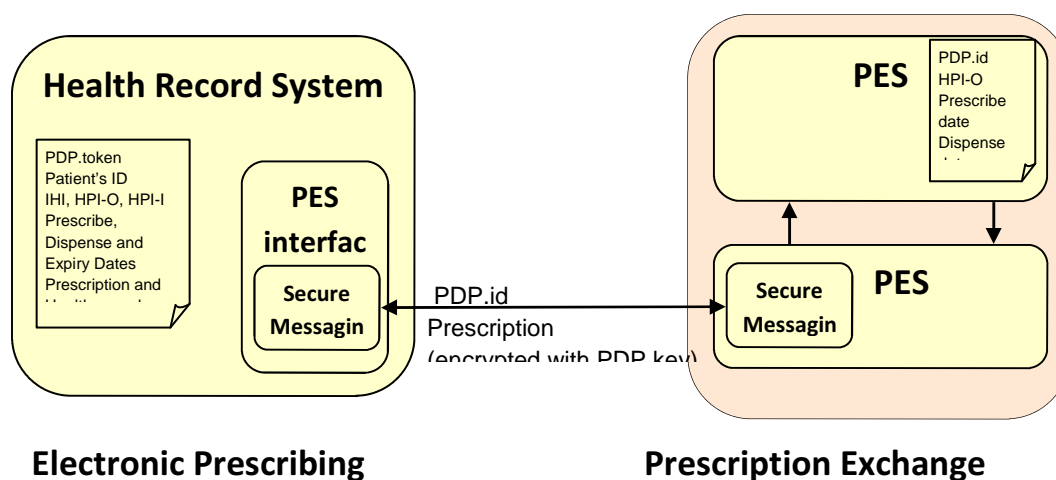
**Consideration:** Plain text record header can be retained but the encrypted payload should be deleted from the system whenever a prescription is cancelled.

## 10 Data Security

### 10.1 Security Measures

Security measures are required to protect the personal information from loss, unauthorised access, use, modification, disclosure or other misuse, including how data is transferred between sites. This is a requirement of NPP 4.1 which states “An organisation must take reasonable steps to protect the personal information it holds”. Information is already collected by the Prescriber and Dispenser, the majority of whom are using their own Electronic Prescribing System and Electronic Dispensing System respectively (as shown on the Information Flow Map). For the purpose of this PIA it is assumed that the Prescriber and Dispenser systems have complied with their own privacy requirements and adopted reasonable security measures. The focus for this PIA is on the security of messages passed to and from the PES.

The PES will use NEHTA’s secure messaging technologies to transfer information from and to the PES as shown below.



NEHTA's proposed secure messaging project will ensure that all data is encrypted whenever it is being transmitted from source to destination. The protocols used ensure that the information cannot be accessed, lost or modified in transit.

In addition to the secure messaging, the personal information within the prescription is further encrypted using the PDP.key. This ensures that the personal information cannot be read while in transit or while stored in the PES. The prescription encrypted using the PDP.key will need to be accessed using the PDP.id and then decrypted using the PDP.key. These keys can only be generated using the original PDP.token. The mechanism to achieve this is described in more detail in the later analysis section on describing 'The risks with the PDP.tokens'.

### 10.1.1 Backup and Audit Security

Backup and Audit of personal information may present a privacy risk when information is taken outside of the security protections given to online data storage. The Information Flow Map in Figure 2 shows Backup and Audit functions as external to the PES and the Prescriber and Dispenser systems. For example, data can be backed up on disk or tape and kept off site to allow for business continuity following a disaster. For the PES this does not present a risk since the payload with the personal information can only be decrypted knowing the PDP.token assigned to each prescription. The main risk is with the Prescriber Information Systems and the Dispenser Information Systems. The policy should ensure that all health data is encrypted prior to backup, particularly if the Prescriber or Dispenser health record systems are permitted to keep copies of the PDP.tokens that have been assigned against each patient record.

**Recommendation:** Include specifications of the back-up and audit functions of the PES to ensure that personal data is only stored in encrypted form.

## 10.2 Outsourcing

The proposed token-based encryption security method allows for the outsourcing of the PES to other agencies without concerns over privacy (provided suitably contractual arrangements have been made that limit access based on the PDP.token and via registered HPI-Os). That is, the agencies cannot reasonably decrypt the personal information that resides in the PES.

## 10.3 Access Rights

To protect the PES from misuse, access rights would be limited to HPI-Os. The HPI-Os have to be registered with the government or authorized agency and prove they are a legitimate

Healthcare provider. Audit functions would be able to track access requests made by each HPI-O.

#### **10.4 Prevention of Inappropriate Access**

Inappropriate access of the PES is minimised through the use of the PDP.id generated by the PDP.token, see Section 13. The use of a 128 bit key reduces the risk to a negligible level that a given HPI-O will be able to access a record without the correct PDP.id being used. PDP.token used to generate the PDP.id is not accessible on the PES and can only be found by a Dispenser or Prescriber on the printed prescription.

Although this method minimises the risk of inappropriate access it is not possible to determine if it is the correct HPI-O accessing the PES. That is, the specific HPI-O dispensing the prescription is not stated on the electronic, nor the paper, prescriptions since it is the choice of the individual which Dispenser they will go to. The system relies on the HPI-O having the PDP.token.

#### **10.5 Breach Notification**

The Prescriber and Dispenser should have appropriate breach notification policies in the case of a major security breach. [Current guidance](#)<sup>7</sup> by the Office of the Privacy Commissioner is for organizations to notify individuals when there is a “real risk of serious harm” resulting from a security breach. Currently breach notification is recommended but not mandatory. The Commonwealth government has plans for introducing legislation on breach notification.

Breach notification with the PES would not be applicable since the identity of the individuals could not be ascertained from the encrypted data without the PDP.token.

#### **10.6 Retention and Destruction**

The prescription has an expiry date in the plain text header of the prescription record held in the PES. It is recommended that the encrypted payload is deleted when reasonably practicable past the expiry date. Deletion would need to consider any legal requirements around retaining records for potential medical liability claims. Any such requirement might be addressed through Prescriber or Dispensers electronic record systems. Since the PES record headers contain no personal information or personal identifiers they can be retained as long as necessary for audit purposes.

---

<sup>7</sup> [http://www.privacy.gov.au/publications/breach\\_guide.html](http://www.privacy.gov.au/publications/breach_guide.html)

**Consideration:** The encrypted payload in the PES is deleted when reasonably practicable past the expiry date.

## 11 Data Quality

Data quality is critical for the safety of the individual in any prescription service. NPP 3 requires that: “An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.” The introduction of the PES does need not change the practices used by the Prescriber and Dispenser in ensuring data quality. The proposed ETP solution only allows for prescription information stored on the PES to be modified through access by the Prescriber or Dispenser. The initial dual use of both paper and electronic prescriptions provides an additional opportunity for Prescribers and Dispensers to check for completeness and accuracy by comparing the paper prescription with the data retrieved from the PES.

## 12 Identity Management

The ETP services depend on a reliable identity management service to ensure the correct individual is being prescribed to and subsequently dispensed with the prescribed items. Identity management is a key project under development within NEHTA.

The ETP services will make use of the following services (once they have passed legislation):

- 1) Individual Health Identifier (IHI) Service that provides a unique identifier for the individual seeking care (i.e. subject of care);
- 2) the Health Provider Identifier – Individual (HPI-I) service that provides a unique identifier for each registered healthcare service professional; and;
- 3) the Health Provider Identifier – Organisation (HPI-O) service that provides a unique identifier for each registered healthcare organisation.

These are described in more detail in the respective Concept of Operation documents for IHI, HPI-I, HPI-O. These identifiers are under development and will require specific legislation to be passed before their usage. A privacy assessment of identifiers has been undertaken through separate PIAs.

It should be noted that to allow for migration to the proposed Health Identifiers described above, other identifying attributes will be accommodated in the PES as an interim measure, for example Medicare number. These identifying attributes would not be regarded as ‘unique’ identifiers. NPP 7.3 states that an; “identifier includes a number assigned by an

organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. However, an individual's name or ABN is not an identifier”.

The individual identifiers (e.g. IHI, HPI-I) that are used in a prescription to uniquely identify an individual are encrypted using the PDP.key. The only identifier used to locate prescriptions stored in the PES is the PDP.id. This is a special search key that can only be generated from the PDP.token. The PDP.token is not stored on the electronic prescription in either plain text or encrypted form. The PDP.token is only printed on the paper based prescription (although a copy may be kept by the Prescriber on their Health Record System). Hence, information stored in the PES can only be accessed through the PDP.id. and cannot be accessed through any personal identifier. This minimises the privacy risk that a person can be readily identified from the prescriptions stored on the PES.

### **12.1 Anonymity**

There is a privacy requirement allowing for individuals to remain anonymous if possible. NPP 8 states that: “Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation”.

There are special circumstances (as described in the section above ‘Can individuals choose what information they supply’) when some information may not be provided. It would not be acceptable with prescription services to remain totally anonymous. Some services, at the Prescribers discretion, may allow for pseudonyms to be used, for example sexual health clinics. They may issue their own identifier that allows the individual concerned to be matched to the correct person.

### **12.2 Transborder data flows**

There are privacy requirements that relate to the transfer of data to a foreign country (NPP9). This relates to personal information held about an individual. It is permitted under certain conditions such as when the countries concerned have similar privacy laws or the individual consented to this or for special contractual reasons.

With the ETP service the personal information can only be accessed while it is with the Prescriber or the Dispenser. Personal information in the PES is encrypted and there is a minimal risk of this encryption being broken. Hence, provided the Electronic Prescription Systems and the Electronic Dispensing Systems are located in Australia (or its Territories) then the issue of transborder data flows of personal information will not apply.

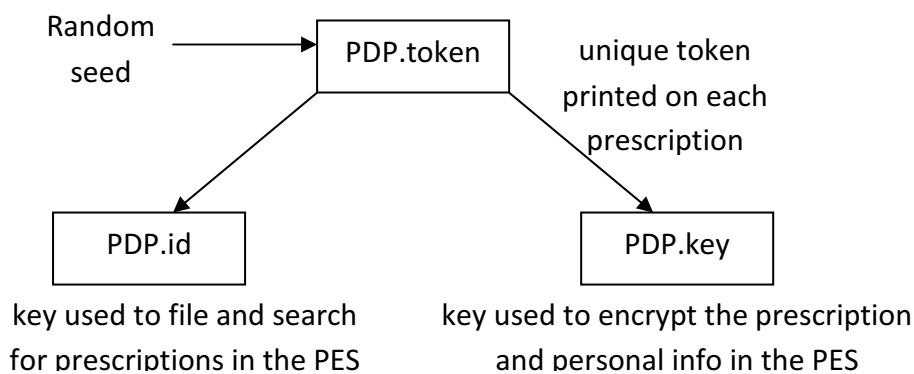
### **12.3 Sensitive information**

NPP 10 sets out special provisions for sensitive information. Health information would be regarded as sensitive information which can be collected by competent health or medical bodies when it is necessary to provide a healthcare service to an individual or it is required

by law. Consent is normally explicitly given by individuals when they initially register with a Prescribing practice or it is implied, as detailed in Section 6.1.

### 13 The risks with the PDP.token

A PDP.token is a 128 bit key generated by a random number seed. The probability of two identical keys being generated from truly random number seeds is close to zero. For the purpose of the ETP project the PDP.token will be considered to be unique over its lifetime. The proposed PDP.token is used to generate two key pairs namely the PDP.key and PDP.id. This is shown in the following diagram:



The PDP.key is used to encrypt the personal information relating to a prescription. The PDP.id is used as an index for filing and retrieving this encrypted information. It is not possible to determine the PDP.key by knowing the PDP.id. The reverse is also true, i.e. the PDP.id cannot be determined from knowing the PDP.key. The only practical way that the PDP.key and PDP.id can be determined is generating them again from the PDP.token. Hence, the PDP.token holds the secret that will allow searching and decryption of the information held in the Prescription Exchange Service (PES). The proposed format of the PES records is as follows:

- PDP.id
- HPI-O
- Prescribe date
- Dispense date
- Expiry date
- Prescription (encrypted)

Hence, to retrieve an electronic prescription requires the PDP.id (note that, the PDP.id is a 128 bit key and cannot therefore be reasonably guessed). The PDP.id would normally be generated from the original PDP.token. Having retrieved the PES record using the PDP.id the prescription would need to be decrypted using the PDP.key. The PDP.key would normally be generated by the original PDP.token.

The PDP.token is therefore the critical component for accessing and decrypting information held in the PES.

The following risks for unauthorized access have been identified with the PDP.token.

- 1) the printed token is read or copied;
- 2) the token can be guessed at random or generated in sequence;
- 3) the token can be predicated;
- 4) the random number seed could be intercepted;
- 5) the token could be misread by the bar code reader or mistyped when using manual entry;
- 6) the token(s) can be located on the Electronic Prescribing System (EPS) and
- 7) the token(s) can be located on the Electronic Dispensing System (EDS).

These points are addressed in turn in the analysis below.

### **13.1 Comment and Analysis**

- 1) This risk currently applies to paper-based prescriptions and would remain. That is, the person's name and the Prescriber's name is printed on the prescription together with the medicines prescribed. Knowing the PDP.token will only provide access to one prescription stored on the PES. From a privacy perspective the information stored on the PES will match the information on the paper prescription. The only change in risk is the fact that information is now stored in electronic form which may increase the speed of access and distance from which the information can be reached.
- 2) The proposed PDP.token is a 128 bit key. The claim is that with 128 bit ( $3.4 \times 10^{38}$ ) random numbers the probability of duplicating keys presents a negligible level risk. In practice this means that if 10 million random numbers were generated every second it would take on average 1,079,028,307,080,601,418,897,052 years before a number was repeated. The risk of guessing a known key is from negligible to zero and on average billions of billions of numbers would need to be generated before one was reached in a given sequence.
- 3) Given the statistics in (2) above, the only risk of predicting the token is by intercepting the random number seed used or by interfering with the random number generating algorithm.
- 4) The main risk here is when the random number seed is sourced externally. An internally generated seed is only likely to be at risk if the algorithms or system is interfered with by an external source.
- 5) The misreading of a token presents a negligible to zero risk of generating the wrong token based on the arguments given in (2) & (3) above. The proposed use of check digits will identify the most common misreads that will occur. A poorly printed or damaged paper document that prevents a successful read (via bar code or typing) will prevent the PES record from being retrieved. The only way that the PES record

can be retrieved when the PDP.token is irreparably damaged is through access to a separate record holding the PDP.token on the Electronic Prescribing System (if such records are kept).

- 6) When the EPS generates a PDP.token, a local copy may be made and held securely in the Health Record System. Information in the PES will, in the main, be a subset of information in the Health Record System. If unauthorized access is made to the Health Record System then any personal details could be breached. If lists of PDP.tokens are linked to an identifier, e.g. linked to an IHI, this could present a higher risk. Unauthorized access of such a list of PDP.tokens would allow for the PES to be directly interrogated for personal information. It has been proposed that the HPI-O would be required to access the PES. The risk is that any HPI-O can access the PES and it is not practical to block their access (i.e. under current practice the Prescriber could be any prescriber the individual selected) and checking the authority of a given HPI-O to access the information is more complex as this is not recorded on the PES record. Any HPI-O that has the PDP.token will appear to be a legitimate access. An audit function may show irregularities, i.e. when a PES record has been access more than is necessary.
- 7) As with (6) above the EDS could have records of the PDP.tokens presented. Any list of PDP.tokens that was accessed by unauthorized parties would have the same risks. PDP.tokens would need to be kept as secure as any personal information. An HPI-O making access to the PES using a list of PDP.tokens would be challenging to effectively audit.

A risk analysis assessing each of these points is provided in the next section.

### 13.2 Risk Analysis

An international standard Risk Analysis Matrix is utilised which combines a Likelihood rating and an Impact rating.

Likelihood	Rare (1)	Unlikely (2)	Possible (3)	Likely (4)	Almost Certain (5)
<b>Impact</b>					
<b>Catastrophic (5)</b>	5	10	15	20	25
<b>Major (4)</b>	4	8	12	16	20
<b>Moderate (3)</b>	3	6	9	12	15
<b>Minor (2)</b>	2	4	6	8	10
<b>Insignificant (1)</b>	1	2	3	4	5

The following table explains the legend used in the risk analysis matrix together with the example recommended Required Actions for each risk level.

Risk	Required Actions
<b>High Risk</b>	<b>Significant Risk</b> — Immediate treatment required, i.e. should be addressed as soon as practicable.
<b>Medium Risk</b>	<b>Moderate Risk</b> — Treatment required as medium priority, i.e. should be

	addressed within the next few months.
<b>Low Risk</b>	<b>Accepted Risk</b> — Manage by specific monitoring or response procedures, i.e. policies and procedures should be in place within a year.
<b>Negligible Risk</b>	<b>Rejected Risk</b> — Manage and monitor by routine internal procedures, i.e. no special action is required while it remains at this level.

The preliminary risk associated with the PDP.token for the ETP project is summarised in the following tables:

Risk	Likelihood	Impact	Risk Level	Mitigation Strategy
1) the printed token is read or copied;	Possible (3)	Minor <sup>1</sup> (2)	Low (6)	Care with the paper prescriptions (as per current practice) and try to ensure they can not be readily photocopied or scanned
2) the token can be guessed at random or generated in sequence;	Rare (1)	Minor (2)	Rare (2)	Ensure a robust and reliable random number generator is used with a true random seed
3) the token can be predicated;	Rare (1)	Minor (2)	Rare (2)	Ensure a robust and reliable random number generator is used with a true random seed
4) the random number seed could be intercepted.	Rare (1)	Major <sup>2</sup> (4)	Low (4)	Use an internal seed generator rather than an externally sourced seed. Ensure robust security and breach software is in place
5) the token could be misread by the bar code reader or mistyped when using manual entry;	Unlikely (2)	Catastrophic <sup>3</sup> (5)	Medium (10)	Provisions for Sum Checks, Typed Entry and Dispensing using the paper prescription only, i.e. without using PES.
6) the token(s) can be located on the Electronic Prescribing System (EPS);	Possible <sup>5</sup> (3)	Catastrophic <sup>4</sup> (5)	High (15)	Strong policy of not keeping lists of PDP.tokens. Ensure robust security and breach software is in place
7) the token(s) can be located on the Electronic Dispensing System (EDS).	Unlikely <sup>5</sup> (2)	Catastrophic <sup>4</sup> (5)	Medium (10)	Strong policy of not keeping lists of PDP.tokens. Ensure robust security and breach software is in place

**Notes on the classifications assigned above:**

<sup>1</sup> Access to a single prescription has been classified as having minor impact to the eMM systems as a whole.

<sup>2</sup> Access to a set of prescriptions involving more than one individual associated with a single HPI-O has been classified as major impact.

<sup>3</sup> The impact of a prescription not being issued or the wrong one being issued could have a catastrophic impact on a given individual.

<sup>4</sup> Access to sets of prescriptions involving many individuals associated with a many HPI-Os has been classified as having a catastrophic impact on the viability of the ETP system.

<sup>5</sup> The prescribing system (e.g. a G.P. clinic) is considered to be a higher security risk than the dispensing system (e.g. a Pharmacist) based on the typical technical knowledge of the different organisations.

**Recommendation:** Ensure robust mechanisms are employed for generating PDP.tokens (and the PDP.id / PDP.key) in a secure and dependable manner.

## 14 Management Recommendations

This PIA has developed a number of recommendations. The main focus has been on the impact that the electronic system will bring over the existing paper-based systems. They have been prioritised to reflect the importance on the effects over the ETP designs currently under development, to include:

### 14.1 As a High Priority:

The recommendations included in this High Priority section could have a significant impact on privacy and have either a high impact on the ongoing design or may take longer than the other recommendations to resolve. Therefore, addressing these recommendations should commence as soon as possible and not longer than 3-4 months.

- Resolve the issue of consent for Dispense Notification by referring to the appropriate reference groups. This has been detailed in Section 6.2.2. 'Dispense Notifications'.
- Provide clear definitions on the confidentiality indicators and their use. This may need consultation across NEHTA to adopt a common approach. As an interim measure the confidentiality indicator should be specified as 'reserved' and clearly stated that this is reserved for future application and cannot be assigned any value. This has been detailed in Section 5.5. 'Information Confidentiality'.
- Ensure robust mechanisms are employed for generating PDP.tokens in a secure and dependable manner. The PDP.token was identified as central to many of the privacy requirements. A detail analysis was provided in Section 12, 'The risks with the PDP.token'. Therefore, the reliability for generating dependable tokens and the perceived risks associated with token generation should be addressed through an independent review by an external third party such as QUT's Information Security Institute.

### 14.2 As a Medium Priority:

The recommendations included in this Medium Priority section could have a moderate to high impact on privacy and a moderate impact on the ongoing design, e.g. addressing these recommendations should ideally commence within 3-6 months and no longer than 6-9 months.

- Develop methods and policies that minimise the risk associated with the creation of lists of previously assigned PDP.tokens. Any HPI-O that has the PDP.token will appear to be a legitimate access as detailed in Section 7.1 'Disclosing to Third parties'. An audit function that records which HPI-O has

accessed which PES record may be necessary as a deterrent. Reviewing the access controls that would minimise this risk is also recommended.

- Standardise the terminology used in the ETP project associated with the various sub-systems and encryption keys. The terminology is changing as the business requirements and standard document templates evolve. Due to the new approach proposed for security (Section 9 'Data security') it is important to ensure that the various team members and others in NEHTA clearly understand what is being proposed. Hence, the recommendation is to standardise, as soon as realistically possible, the terminology used. This will help minimise privacy risks resulting from any misunderstanding of the data security protections proposed.
- Provide the Prescriber with the discretion of choosing what information will be entered in the mandatory fields on the PES to accommodate situations when an individual has special circumstances, see section 5.8, 'Can individuals choose what information they supply?'

### **14.3 As a Lower Priority:**

The recommendations included in this Lower Priority section also have a moderate to high impact on privacy but are unlikely to have a high impact the ongoing design, e.g. addressing these recommendations should ideally commence within 12 months and no longer than 18 months.

- Include specifications of the back-up and audit functions of the PES to ensure that personal data is only stored in encrypted form which is protected by the proposed PDP.key. This has been detailed in Section 9.1.1 'Backup and Audit'.
- Ensure that individuals can readily access the applicable privacy policies associated with eMM and wherever possible provide these policies in other commonly used languages, in line with Government practice (e.g. Medicare and Centrelink). This has been detailed in Section 5.4., 'Can other languages be used?'
- Provide suitable access mechanisms (e.g. via the Prescriber or Dispenser) that permits individuals to exercise their right to access any personal information stored electronically and to request corrections to errors if necessary). This has been detailed in Section 8.1., 'Access and Correction'.

## Appendix

### Questions addressed in the PIA Information Mapping

The following represents a full list of questions that were addressed for a PIA information flow mapping. The ETP project will be following current legislation and best working practice for paper records. The focus will be on any aspect that has changed as a result of the introduction of the proposed electronic system.

#### 1 Collection

When considering collection, describe:

- how the collection relates to the agency's functions or activities;
- what public interest justifies the collection;
- why the personal information, including the particular data items and kinds of data, is necessary for the project;
- whether the information can be collected in a de-identified or anonymous manner; and
- whether individuals can choose not to provide some or all of the personal information sought.

##### 1.1 Scope of collection

Describe:

- the personal information, including the data items to be collected (e.g. name, address, occupation, identification numbers);
- where the information is to be collected from (e.g. from the individual directly, from other individuals, from other agencies or organisations, from publicly available sources);
- whether the information will be paid for or exchanged for something else of value;
- how the circumstances of the individuals involved will be taken into account when the personal information is being collected, e.g. cultural diversity, hearing impairment, languages other than English;
- why each element of the information is being collected (e.g. identify whether some data items are collected for some purposes and other data items for different purposes);
- whether the information to be collected is of a sensitive nature (including, for example, financial information, political or religious beliefs, health, sexual practices, biometric or genetic information);
- any statute, authority or requirement the agency is relying upon to collect the information; and

- alternatives to collection that have been considered and rejected (e.g. using de-identified data).

## 1.2 Notice

Personal information should be handled in a transparent way so there are no surprises for the individual. Identify and describe what information is given to the individual about the collection, and how it is given, including:

### (a) Purpose and authority

- the purpose for which the personal information is being collected;
- whether the collection is authorised or required by law (and, if so, which law?);

### (b) Use and disclosure

- uses or disclosures that the agency considers consistent with the purpose for collection;
- the people, bodies or agencies to which the collecting agency usually or sometimes discloses personal information (and any further uses and disclosures by those people, bodies or agencies);
- proposed uses or disclosures for purposes other than the purpose of collection; and

### (c) Choice

- do individuals know they have a choice about the handling of their personal information where these choices exist? Has the agency told them?

## 1.3 Method of collection

Identify and describe:

- how often the personal information is to be collected (e.g. only on one occasion or ongoing);
- any potentially sensitive or intrusive methods of collection (including photographs, fingerprinting, iris scanning, drug testing and the collection of genetic information, for example, through buccal swabs);
- any covert methods of collection, such as surveillance, and why they are necessary and appropriate (e.g. some website cookies and surveillance devices including electronic listening devices and cameras); and
- whether the technology is privacy enhancing or privacy invasive, and why.

## 2 Use

### 2.1 Use

Identify and describe:

- all the uses of the personal information (including ones which may be expected but uncommon);
- how all these uses relate to the purpose for which the personal information was collected;
- any changes to the purpose for using the information after the information is collected; and
- measures in place to prevent use for secondary purposes.

### 2.2 Secondary purposes

If the information collected may be used for an additional or secondary purpose, identify and describe:

- whether consent is required for the secondary use;
- if the use is directly related to the purpose of collection;
- whether an individual can decline the secondary use and still be involved in the project; and
- if new, unplanned purposes for handling personal information arise in the life of the project, the extent to which individuals will be involved in decisions about these new purposes.

### 2.3 Data linkage / matching

Aggregation or the bringing together of diverse groups of personal information collected for different purposes, either in the agency or by another agency or organisation, has privacy risks. For example, it may reveal personal information not previously available, or it may reveal information not necessary for the purpose at hand.

Identify and describe:

- any intention or potential for the personal information to be linked, matched or cross-referenced to other information held in different databases (held by the agency or by other agencies or organisations);
- how this linkage, matching or cross-referencing might be done;
- any decisions affecting the individual that are to be made on the basis of such data-matching, linking or cross-referencing;
- what safeguards will be in place to limit inappropriate access, use and disclosures of the resulting information;

- what mechanisms will be in place to ensure audit trails and appropriate back-ups; and
- what protections are in place to ensure the accuracy of the data linkage and that individuals will not be adversely affected by erroneous data matching; for example, have individuals been informed of the data linkage?

### 3 Disclosure

Generally speaking, “disclosure” refers to the process of releasing personal information outside the control of an agency.

Identify and describe:

- to whom and under what circumstances the personal information will be disclosed and why;
- whether the personal information disclosed to others outside the agency will be protected from privacy risks in the same way as information held by the agency (e.g. covered by the Privacy Act, or by a similar privacy law);
- if the information is to be published, or disclosed to a register, e.g. a public register;
- whether the individual has been told about the disclosure and what choices they have (including about the publication or suppression of their information); and
- whether the disclosure is authorised or required by law, specifying the relevant provisions.

### 4 Access and correction

Identify and describe:

- how an individual can access their personal information (including any costs incurred by the individual); and
- how the individual can have the information about them corrected, or annotations made, if necessary.

### 5 Data Security

Describe:

- what security measures will be taken to protect the personal information from loss, unauthorised access, use, modification, disclosure or other misuse, including how data is transferred between sites;
- what security measures will be taken to protect personal information where its handling will be or has been outsourced to external agencies or organisations;
- who will have access to the information, and who authorises those access rights;

- the systems in place to prevent and detect misuse of, or inappropriate access to, the personal information; and
- what action will be taken if there is a security breach (e.g. informing individuals of the breach).

## 5.1 Retention and destruction

Identify and describe the retention and destruction practices to be employed in the project, including:

- when personal information is to be de-identified or destroyed;
- how this is to be done and whether it will be done securely;
- whether a data retention policy and destruction schedule is in place; and
- how compliance with the data retention policy and any relevant legislation relating to record destruction will be measured.

## 6 Data quality

Identify and describe:

- the consequences for individuals if the personal information is not accurate or up-to-date (e.g. the kinds of decisions made on the basis of the information; the risks to the agency and the individual posed by inaccurate information);
- how information will be kept up-to-date;
- the processes to ensure that the data is only used or disclosed when it is relevant, up-to-date and complete; and
- the updates and modifications to personal information which will be disseminated to others outside the agency to whom personal information has been disclosed.

## 7 Identity Management

Agencies handling personal information may require identity management systems and processes robust enough to identify, to an appropriate level of confidence, the individuals whose personal information they are dealing with.<sup>12</sup>

Identify and describe:

- to what extent the project can proceed through the handling of anonymous or de-identified information;
- whether it is necessary to authenticate identity, and to what degree of confidence (e.g. taking into account a consideration of the value of the transaction);
- how evidence of identity is to be authenticated;
- whether the project involves the issuing of a new identification number to individuals, and its purpose;

this includes whether the new identification number could potentially be used for other purposes or adopted by other agencies or private sector organisations, and, if so, what protections could be put in place to address this;

- any expected uses and disclosures of this or other identification numbers (by any agency or organisation); and
- individual attributes, other than identity, that need to be authenticated (e.g. that an individual has a certain qualification).

# National Privacy Principles (NPPs)

## 1. Collection

1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of:

- (a) the identity of the organisation and how to contact it; and
- (b) the fact that he or she is able to gain access to the information; and
- (c) the purposes for which the information is collected; and
- (d) the organisations (or the types of organisations) to which the organisation usually discloses information of that kind; and
- (e) any law that requires the particular information to be collected; and
- (f) the main consequences (if any) for the individual if all or part of the information is not provided.

1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.

1.5 If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in subclause 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

[Back to Top](#)

## 2. Use and disclosure

2.1 An organisation must not use or disclose personal information about an individual for a purpose (the **secondary purpose**) other than the primary purpose of collection unless:

(a) both of the following apply:

- (i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;
- (ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or

(b) the individual has consented to the use or disclosure; or

(c) if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:

- (i) it is impracticable for the organisation to seek the individual's consent before that particular use; and
- (ii) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and
- (iii) the individual has not made a request to the organisation not to receive direct marketing communications; and
- (iv) in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications; and
- (v) each written direct marketing communication by the organisation with the individual (up to and including the communication that involves the use) sets out the organisation's business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the organisation can be directly contacted electronically; or

(d) if the information is health information and the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety:

- (i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and
- (ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph; and
- (iii) in the case of disclosure—the organisation reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information; or

(e) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent:

- (i) a serious and imminent threat to an individual's life, health or safety; or
- (ii) a serious threat to public health or public safety; or

(ea) if the information is genetic information and the organisation has obtained the genetic information in the course of providing a health service to the individual:

(i) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety (whether or not the threat is imminent) of an individual who is a genetic relative of the individual to whom the genetic information relates; and

(ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95AA for the purposes of this subparagraph; and

(iii) in the case of disclosure—the recipient of the genetic information is a genetic relative of the individual; or

(f) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or

(g) the use or disclosure is required or authorised by or under law; or

(h) the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

Note 1: It is not intended to deter organisations from lawfully co-operating with agencies performing law enforcement functions in the performance of their functions.

Note 2: Subclause 2.1 does not override any existing legal obligations not to disclose personal information. Nothing in subclause 2.1 requires an organisation to disclose personal information; an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: An organisation is also subject to the requirements of National Privacy Principle 9 if it transfers personal information to a person in a foreign country.

2.2 If an organisation uses or discloses personal information under paragraph 2.1(h), it must make a written note of the use or disclosure.

2.3 Subclause 2.1 operates in relation to personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation's primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.

2.4 Despite subclause 2.1, an organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual if:

(a) the individual:

(i) is physically or legally incapable of giving consent to the disclosure; or

(ii) physically cannot communicate consent to the disclosure; and

(b) a natural person (the **carer**) providing the health service for the organisation is satisfied that either:

(i) the disclosure is necessary to provide appropriate care or treatment of the individual; or

(ii) the disclosure is made for compassionate reasons; and

(c) the disclosure is not contrary to any wish:

(i) expressed by the individual before the individual became unable to give or communicate consent; and

(ii) of which the carer is aware, or of which the carer could reasonably be expected to be aware; and

(d) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (b).

2.5 For the purposes of subclause 2.4, a person is **responsible** for an individual if the person is:

(a) a parent of the individual; or

(b) a child or sibling of the individual and at least 18 years old; or

(c) a spouse or de facto spouse of the individual; or

(d) a relative of the individual, at least 18 years old and a member of the individual's household; or

(e) a guardian of the individual; or

(f) exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health; or

(g) a person who has an intimate personal relationship with the individual; or

(h) a person nominated by the individual to be contacted in case of emergency.

2.6 In subclause 2.5:

**child** of an individual includes an adopted child, a step-child and a foster-child, of the individual.

**parent** of an individual includes a step-parent, adoptive parent and a foster-parent, of the individual.

**relative** of an individual means a grandparent, grandchild, uncle, aunt, nephew or niece, of the individual.

**sibling** of an individual includes a half-brother, half-sister, adoptive brother, adoptive sister, step-brother, step-sister, foster-brother and foster-sister, of the individual.

### 3. Data quality

An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.

### 4. Data security

4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2.

### 5. Openness

5.1 An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.

5.2 On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

### 6. Access and correction

6.1 If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that:

(a) in the case of personal information other than health information—providing access would pose a serious and imminent threat to the life or health of any individual; or

(b) in the case of health information—providing access would pose a serious threat to the life or health of any individual; or

(c) providing access would have an unreasonable impact upon the privacy of other individuals; or

(d) the request for access is frivolous or vexatious; or

(e) the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings; or

(f) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(g) providing access would be unlawful; or

(h) denying access is required or authorised by or under law; or

(i) providing access would be likely to prejudice an investigation of possible unlawful activity; or

(j) providing access would be likely to prejudice:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or

(iii) the protection of the public revenue; or

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders;

by or on behalf of an enforcement body; or

(k) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

6.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

Note: An organisation breaches subclause 6.1 if it relies on subclause 6.2 to give an individual an explanation for a commercially sensitive decision in circumstances where subclause 6.2 does not apply.

6.3 If the organisation is not required to provide the individual with access to the information because of one or more of paragraphs 6.1(a) to (k) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

6.4 If an organisation charges for providing access to personal information, those charges:

(a) must not be excessive; and

(b) must not apply to lodging a request for access.

6.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up-to-date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up-to-date.

6.6 If the individual and the organisation disagree about whether the information is accurate, complete and up-to-date, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete or up-to-date, the organisation must take reasonable steps to do so.

6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.

## 7. Identifiers

7.1 An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

- (a) an agency; or
- (b) an agent of an agency acting in its capacity as agent; or
- (c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.

7.1A However, subclause 7.1 does not apply to the adoption by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before those matters are prescribed: see subsection 100(2).

7.2 An organisation must not use or disclose an identifier assigned to an individual by an agency, or by an agent or contracted service provider mentioned in subclause 7.1, unless:

- (a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency; or
- (b) one or more of paragraphs 2.1(e) to 2.1(h) (inclusive) apply to the use or disclosure; or
- (c) the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before the matters mentioned in paragraph (c) are prescribed: see subsection 100(2).

7.3 In this clause:

**identifier** includes a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. However, an individual's name or ABN (as defined in the *A New Tax System (Australian Business Number) Act 1999*) is not an **identifier**.

## 8. Anonymity

Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

## 9. Transborder data flows

An organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country only if:

- (a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles; or
- (b) the individual consents to the transfer; or
- (c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or
- (d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or
- (e) all of the following apply:
  - (i) the transfer is for the benefit of the individual;
  - (ii) it is impracticable to obtain the consent of the individual to that transfer;
  - (iii) if it were practicable to obtain such consent, the individual would be likely to give it; or
- (f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the National Privacy Principles.

## 10. Sensitive information

10.1 An organisation must not collect sensitive information about an individual unless:

- (a) the individual has consented; or
- (b) the collection is required by law; or
- (c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:
  - (i) is physically or legally incapable of giving consent to the collection; or

(ii) physically cannot communicate consent to the collection; or

(d) if the information is collected in the course of the activities of a non-profit organisation the following conditions are satisfied:

(i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities;

(ii) at or before the time of collecting the information, the organisation undertakes to the individual whom the information concerns that the organisation will not disclose the information without the individual's consent; or

(e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

10.2 Despite subclause 10.1, an organisation may collect health information about an individual if:

(a) the information is necessary to provide a health service to the individual; and

(b) the information is collected:

(i) as required or authorised by or under law (other than this Act); or

(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

10.3 Despite subclause 10.1, an organisation may collect health information about an individual if:

(a) the collection is necessary for any of the following purposes:

(i) research relevant to public health or public safety;

(ii) the compilation or analysis of statistics relevant to public health or public safety;

(iii) the management, funding or monitoring of a health service; and

(b) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and

(c) it is impracticable for the organisation to seek the individual's consent to the collection; and

(d) the information is collected:

(i) as required by law (other than this Act); or

(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or

(iii) in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph.

10.4 If an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must take reasonable steps to permanently de-identify the information before the organisation discloses it.

10.5 In this clause: **non-profit organisation** means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims.