PIA ON THE ELECTRONIC TRANSFER OF PRESCRIPTION RELEASE 1.1

For: National E-Health Transition Authority

15 DECEMBER 2010

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

1.1 BACKGROUND

The National E-Health Transition Authority (NEHTA) asked Information Integrity Solutions (IIS) to conduct a Privacy Impact Assessment on the new features of the Electronic Transfer of Prescription (ETP) Specification known as Release 1.1. The ETP is being developed as part of NEHTA's Electronic Medications Management (eMM) program and is one of five capabilities that NEHTA has identified as being necessary for comprehensive eMM.

A preliminary PIA on Release 1 of the ETP was conducted by Better Life ICT in June 2009. NEHTA has engaged IIS to conduct a second PIA, which is to build on the preliminary PIA by examining the new information flows resulting from the changes made by Release 1.1. In general terms Release 1.1 has moved from a system that supports existing paper based prescription in the primary care setting to one that extends this support to a paperless process in additional settings including hospitals and residential aged care across Australia. Also, four additional information flows have been introduced into the specifications:

- A cancellation of prescription process which includes dispense information going to the prescriber where medications have been dispensed before the prescription was cancelled.
- A new message flow from the dispenser to a specific prescriber requesting a prescription for medications dispensed based on an informal (e.g. verbal) order ('prescription owing').
- The notification to the prescriber from the dispenser of the situation where the consumer has exhausted the number of prescription repeats authorised by the prescriber. The aim being to prompt the prescriber to generate a new prescription if appropriate to maintain continuation of medications.
- The provision for agents managing medication on behalf of individuals to receive electronic notification of prescriptions (notification agent).

The key participants in the ETP are:

- The Prescription Exchange Service (PES);
- The Electronic Prescribing System (EPS); and
- The Electronic Dispensing System (EDS).

More details about the ETP and how it works are in Section 6 of the Report.

The scope of this PIA does not include an assessment of the whole of the ETP as outlined in Release 1.1. The aspects of the ETP that remain unchanged in Release 1.1 have already been assessed by the preliminary PIA. IIS was asked only to consider the additional information flows provided for in Release 1.1, and was asked to identify whether there are new privacy risks beyond those identified in the preliminary PIA. As a result, this PIA should be read in conjunction with the Preliminary PIA.

However, during consultations with stakeholders, the Australian Privacy Foundation (APF) raised some issues around the preliminary PIA, including the consent arrangements for the ETP. As a result

this PIA has some clarification and discussion around these issues that it would not otherwise have included.

1.2 PROCESS

In conducting the PIA IIS:

- Made contact with privacy and health consumer stakeholders and consulted them about the process for consultation;
- Read the documents provided by NEHTA, including stakeholder feedback on the public high level specification documents;
- Held meetings with relevant NEHTA staff;
- Conducted analysis;
- Prepared a draft report for NEHTA comment;
- Circulated the draft report to privacy and health consumer stakeholders;
- Revised the draft report on the basis of feedback from stakeholders and NEHTA
- Finalised the draft report.

1.3 FINDINGS

IIS considers that generally speaking the ETP Release 1.1 does not create any significantly greater risks than the current prescribing situations and has been designed in such a way that each party to the ETP (prescribers, dispensers and the PES) does not collect, use, or disclose any more information about an individual than is necessary for the purposes of the ETP or than is currently collected, used or disclosed in current paper prescribing purposes.

In relation to ETP generally, the process mirrors the current paper based processes for issuing and dispensing prescriptions including the current process for consent. The change to use of information technology to transmit prescription information does not warrant a requirement for explicit consent. The design, which involves the encryption of data held in the PES and which ensures that prescription information only becomes accessible when an individual provides the DAK to the dispenser, underpins this view. In response to concerns about the need for explicit consent raised by the Australian Privacy Foundation (APF) IIS considers this issue in detail in Section 10.1 of the PIA.

In relation to Release 1.1 there are two grey areas relating to consent. These are where:

- A dispenser discloses dispensing information to a prescriber when a dispense occurs before a prescription is cancelled; and
- A prescriber sends a prescription notification to a notification agent used by an aged care facility or public hospital.

IIS makes recommendations about these.

The APF raised some issues about information to be collected in the e-Prescription and IIS makes some recommendations about this.

IIS considers that the key issue will be ensuring that there are adequate accountability and governance mechanisms for the ETP. IIS has made recommendations about this.

IIS also considers some changes to the specifications suggested by stakeholders and makes one recommendation about this.

1.4 RECOMMENDATIONS

Recommendation 1: Business as usual – Transparency and e-Prescription notifications

IIS recommends that NEHTA include in its specifications for ETP that individuals should be entitled to receive an e-Prescription notification that includes all the personal information and clinical content on the e-Prescription. The specifications should require prescribers to offer the option of a paper notification. The notification should include information about where an individual can get more information about ETP.

Recommendation 2: Business as usual – Community awareness and education about ETP

IIS recommends that NEHTA ensures that before and after ETP comes into operation there is an extensive community awareness and education campaign about ETP and how it works. It should include online tools, as well as a brochure that can be handed to the individual at the time an e-Prescription is issued and when an e-Prescription is dispensed.

Recommendation 3: Technology – Gender in an e-Prescription

IIS recommends that there should not be a specific field for recording gender in an e-Prescription

Recommendation 4: Technology – Date of Birth in an e-Prescription

IIS recommends that an e-Prescription retains a field for recording age (years and /or months) but that specifications require that the field only be used when the individual is under the age of 12.

Recommendation 5: Technology – Configuration of ETP software

IIS recommends that ETP specifications require that ETP software that pre-populates e-Prescriptions only includes information that is necessary for the particular prescription being issued.

Recommendation 6: Business as usual – Transparency relating to disclosure of dispensing records

IIS recommends that should the notification of dispense on cancellation of prescription proceed protocols developed for participants in the ETP include specifications about how individuals are to be informed that dispensing information could be given to the prescriber and of the circumstances in which this could happen. It should be included in the education and awareness campaign conducted on the implementation of the ETP specifications.

Recommendation 7: Business as usual – Policies and procedures for consent to notify prescription

IIS recommends that NEHTA ensure that there are appropriate policies and procedures in place to ensure that a prescriber does not send, and an aged care facility or private hospital does not receive, prescription notifications unless the individual or their authorised representative has given the appropriate form of consent.

Recommendation 8: Business as usual and technology security and notification agents

IIS recommends that the same security mechanisms that will apply to prescribers, PES, and dispensers should also apply to Notification Agents.

Recommendation 9: Business as usual – Transborder data flows

IIS recommends that a PES provider should not be approved as meeting the NEHTA specifications if it proposes to transmit or store e-Prescription data outside Australia unless there has been a Privacy Impact Assessment including public consultation which establishes that the e-Prescription information can be protected to the level it would have if it remained in Australia.

Recommendation 10: Governance and accountability

IIS recommends that NEHTA advocates the need for there to be put in place an appropriate governance mechanism which provides:

- a mechanism for ongoing oversight of the operation of ETP as a whole;
- a mechanism for developing a consistent and coordinated approach to:
    - policy relating to the ETP;
    - information and transparency about how the ETP operates, the role of each participant and the information flows between the participants;
    - implementing audit and accountability mechanisms to ensure that all participants comply with the applicable privacy and security requirements and obligations – this should include independent audits and random inspections carried out on processes used by PES operators and dispensers;
    - providing access to information held by the participants where necessary or an emergency;
    - managing failure and complaints;
    - developing fair terms and conditions, if any, imposed on individuals in relation to the ETP;
    - monitoring and managing function creep;
- Public reporting on the operation of ETP in relation to each of these matters.

Recommendation 11: Undispensed e-Prescriptions

IIS recommends that NEHTA does not provide for the capability to include in records associated with an e-Prescription the information that a dispense was unsuccessful or the reasons why.

2 INTRODUCTION

The National E-Health Transition Authority (NEHTA) asked Information Integrity Solutions (IIS) to conduct a Privacy Impact Assessment on the new features of the Electronic Transfer of Prescription (ETP) Specification known as Release 1.1. The ETP is being developed as part of NEHTA's Electronic Medications Management (eMM) program and is one of five capabilities that NEHTA has identified as being necessary for comprehensive eMM.

3 SCOPE

A preliminary PIA on Release 1 of the ETP was conducted by Better Life ICT in June 2009. NEHTA has engaged IIS to conduct a second PIA, which is to build on the preliminary PIA by examining the new information flows resulting from the changes made by Release 1.1. In general terms Release 1.1 has moved from a system that supports existing paper based prescription in the primary care setting to one that extends this support to a paperless process in additional settings including hospitals and residential aged care across Australia. Also, four additional information flows have been introduced to the specification:

- A cancellation of prescription process which includes dispense information going to the prescriber where medications have been dispensed before the prescription was cancelled.
- A new message flow from the dispenser to a specific prescriber requesting a prescription for medications dispensed based on an informal (e.g. verbal) order ('prescription owing').
- The notification to the prescriber from the dispenser of the situation where the consumer has exhausted the number of prescription repeats authorised by the prescriber. The aim being to prompt the prescriber to generate a new prescription if appropriate to maintain continuation of medications.
- The provision for agents managing medication on behalf of individuals to receive electronic notification of prescriptions (notification agent).

The scope of this PIA does not include an assessment of the whole of the ETP as outlined in Release 1.1. The aspects of the ETP that remain unchanged in Release 1.1 have already been assessed by the preliminary PIA. IIS was asked only to consider the additional information flows provided for in Release 1.1, and was asked to identify whether there are new privacy risks beyond those identified in the preliminary PIA. As a result, this PIA should be read in conjunction with the Preliminary PIA.

However, during consultations with stakeholders, the Australian Privacy Foundation (APF) raised some issues around the preliminary PIA, including the consent arrangements for the ETP. As a result this PIA has some clarification and discussion around these issues that it would not otherwise have included.

4 STEPS IN CONDUCTING THE PIA

IIS took the following steps in conducting the PIA.

4.1 MADE CONTACT WITH EXTERNAL PRIVACY/HEALTH CONSUMER STAKEHOLDERS AND DEVELOP PROCESS

IIS made contact with the following stakeholders:

- Australian Privacy Foundation;
- Consumers Health Forum of Australia;
- Australian Council of Social Service (ACOSS).

These stakeholders reviewed and provided comments on the draft PIA.

4.2 READ DOCUMENTS

IIS read the following documents provided by NEHTA:

- Concept of Operations: Electronic Transfer of Prescription Release 1.1, Version 1.0 – 6 September 2010, Draft for consultation;
- Business Requirements Definition: ETP Release 1.1, Version 1.0 – 20100816;
- Electronic Transfer of Prescription: Detailed Requirements Definition v1.0;
- ETP Release 1.1: Solution Specification, Version 1.0 – 6/09/2010;
- Privacy Self-Assessment Checklist;
- Electronic Transfer of a Prescription: Preliminary Privacy Impact Assessment, 26/06/2009 (version 0.4);
- ETP R 1 Privacy Management Plan, Version 1.0 – 19/02/10;

IIS made a preliminary analysis, framed further questions and asked for further documents where necessary.

All but the last three documents have been publicly available since early September 2010 on the NEHTA website at http://www.nehta.gov.au/e-communications-in-practice/emedication-management.

4.3 MET WITH RELEVANT NEHTA PERSONNEL

IIS met with relevant NEHTA personnel as necessary including David Batch, Principal Privacy Officer, Toby Matheison (Program Director eMM) and Kieron McGuire (Project manager ETP) to discuss the ETP, including, the differences between Releases 1.0 and 1.1.

4.4 DETAILED ANALYSIS

During this phase IIS considered the new information flows, identified any privacy risks taking into account the National Privacy Principles (NPPs) and Information Privacy Principles (IPPs) as well as identified any other privacy risks that could arise that go beyond mere compliance with the law.

4.5 WROTE DRAFT REPORT

IIS prepared a draft report which it provided to NEHTA for comment and feedback. The draft report was also provided to stakeholders (as listed in Section 4.1) for comment.

4.6 WRITE FINAL REPORT

IIS then wrote the final report which took into account comments from NEHTA, feedback from NEHTA's public consultation on ETP 1.1 and feedback received from privacy/health consumer stakeholders.

5 BACKGROUND TO ETP

NEHTA's ETP package is being developed in response to a heightened need for national improvements in medication management. Adverse drug events jeopardise the health of patients and place a substantial burden on the healthcare system and the broader community. Attempts to reduce medications-related readmissions and/or related interventions are constrained by gaps in clinical awareness of relevant medication information across the continuum of patient care. The National E-Health Strategy, endorsed by the Australian Health Ministers' Advisory Council (AHMAC), recommends the establishment of a 'Prescriptions Service' as the highest priority initiative within eMM.

A number of commercial organisations within the ETP market are currently developing systems for electronic medications management, and some already support electronic transfer of prescription information. However, these services rely on paper prescriptions in order to obtain the prescriber's signature. The ETP is designed to ensure that consumers are able to have their medications dispensed at a pharmacy of their choice by providing mechanisms for achieving interoperability between medication management services.

NEHTA's ETP package is intended to build and foster the ongoing development of a series of national specifications and methods to support the structured electronic exchange of prescriptions and dispensed medication information between prescribers and dispensers. The ETP package aims to establish an agreed set of specifications providing for the timely, secure and consistent transfer of medication information between prescribers and dispensers, in order to:

- Improve the quality and safety of medication provision;
- Improve efficiency, particularly in pharmacies;
- Reduce the potential for errors of transcription and/or interpretation; and
- Build a technical foundation for improvements in the quality and safety of medication management.

These nationally agreed specifications will allow commercial organisations to develop software and hardware to implement products capable of transferring e-Prescriptions. Dispensers will benefit from the implementation of these products through the Fifth Community Pharmacy Agreement. This will provide a subsidy to dispensers that dispense e-Prescriptions generated and transmitted by software that complies with these specifications.

6 DESCRIPTION OF ETP

This section provides a brief overview of the ETP Release 1.1 package.

6.1 PARTICIPANTS AND THEIR ROLES

The following roles are played by the various elements in the ETP:

6.1.1 PRESCRIPTION EXCHANGE

The Prescription Exchange (PE) is a key feature of the ETP specification which will enable health consumers to have their prescription filled at a dispenser of choice. A PE has the following capabilities:

- It provides an indirect communication path between the prescriber and the dispenser(s) in which the dispenser(s) can be selected by the individual (or their agent) at any time after the prescription is created;
- It provides a single point of control for each prescription that allows the prescriber to cancel a prescription; and
- It manages the security of the records that it stores by requiring a 'document access key' (DAK) to be provided for any access.

There are already two private sector organisations running electronic prescription exchanges. These are eRx[1] and Medisecure[2] It is possible that other companies may enter this market once final specifications are released. Implementing the Prescription Exchange Service (PES) specifications within ETP 1.1 will enable these to be interoperable.

6.1.2 ELECTRONIC PRESCRIBING SYSTEMS

Electronic Prescribing Systems (EPS) systems interact with the PES to publish, cancel and retrieve e-Prescriptions. These systems would, for example, be used by prescribers such as a General Practitioners (GPs), specialists and hospitals to:

- Issue an e-Prescription and provide the DAK to the patient or their agent;
- Generate a DAK to go on a paper prescription; and
- Cancel a prescription.

6.1.3 ELECTRONIC DISPENSING SYSTEMS

The Electronic Dispensing System (EDS) interacts with the PES to:

- Retrieve e-Prescriptions and their associated dispense records (including repeat authorisations) prior to dispensing;
- Publish dispense records after dispensing; and, if necessary;

[1] https://www.erx.com.au/Default.aspx supported by the Pharmacy Guild.
[2] http://www.medisecure.com.au/index.html Supported by the Royal Australian College of General Practitioners [RACGP], the Australian General Practice Network [Division's peak body] and the Australian Association of Practice Managers.

- Terminate or reverse a previously initiated dispensing process.

The EDS will also:

- Generate a prescription request;
- Generate a notification for last supply.

This system would be used by a community or hospital pharmacy in their role as dispensers.

6.1.4 NOTIFICATION AGENT

A Notification Agent is a software agent operated by organisations to act on behalf of an individual with the individual's consent. The Notification Agent enables such organisations to be notified that a new electronic prescription for an individual is available from a PES. Healthcare providers such as an aged care facility, dispenser organisations or a private hospital may use a notification agent in circumstances where the individual is not in a position to manage the prescriptions for themselves. The ETP 1.1 specifications require that a notification agent allow these organisations to obtain a supply of medications on the individual's behalf.

6.1.5 FUTURE ETP SERVICE PARTICIPANTS

It is envisaged that future participants in the ETP could be:

- A Personally Controlled Electronic Health Record (PCEHR) including an index facility designed to support the ability to retrieve health records from distributed repositories;
- Approved Health research bodies for authorised projects or purposes.

The Concept of Operations document states that participation by these possible future consumers, would, for privacy reasons, need to be indirect and based on the individual providing consent. The Concept of Operations also states that ETP supports two possible mechanisms for sending information, with the individual's consent, to third parties. These mechanisms are:

- Prescribers and dispensers would supply the electronic prescription/dispense record directly to an approved external system (for example, a PCEHR). In this case prescribers and dispensers would send a copy to the PES and another copy to the external system;
- Prescribers and dispensers would send electronic prescription/dispense documents to the PES but add a 'cc-like' field to the meta-data. An external system would then receive these documents from the PES via a trusted gateway.[3]

However, the specifications provide that the technical capability is not to be activated as part of ETP. These future uses would require development though separate projects and involve the implementation of proper governance, consent and access control frameworks.

6.2 DOCUMENT ACCESS KEY

Each electronic prescription is identified by its own Document Access Key (DAK). A DAK is used to identify and secure a single medication to be prescribed to a single patient. When a prescriber such

[3] In a bulk transmission, the DAKs of all the records would be encrypted with the receiving organisation's public key.

as a GP generates a prescription the electronic prescribing system generates a DAK to be associated with this prescription and is provided to the patient or their agent. The patient or their agent grants access to the e-Prescription by providing the DAK to the pharmacist.

A DAK is a secret string of random text characters, plus the identity of the PE that stores the document. The DAK is used to derive two cryptographic keys:

- Retrieval key: which is a random number that is unique to a set of related clinical documents that are managed by the same PE service provider and
- Cipher key: which is a symmetric key (a random number) that is used to encrypt and decrypt the clinical content of the electronic prescriptions and dispense records.

The retrieval key is combined with the identifier of the PE service provider that manages the relevant prescription documents to create a qualified retrieval key. The PE service provider only receives the retrieval key. It does not receive the cipher key so it is unable to decrypt the clinical content of the e-Prescription.

The retrieval key is used by the electronic dispensing system to identify and receive the appropriate encrypted electronic prescription from the PE. The cipher key enables the electronic dispensing system to decrypt the relevant prescription and the associated records. PE records associated with one prescription are one e-Prescription and its associated dispense records including:

- Repeat authorisations;
- Prescription cancellations;
- Clinical notes.

NEHTA will specify a standard barcode format for the DAK, and the barcode (plus text string) will be printed on a paper notification given to the individual, or in the future, provided through other electronic means.

6.3 ETP AND NATIONAL INFRASTRUCTURE SERVICES

Participants in the ETP services will make use of National Infrastructure Services such as the Endpoint Location Service (ELS), the National Clinical Terminology and Information Service (NCTIS), the National Product Catalogue (NPC) and the National Authentication Service for Health (NASH). Most relevant to this PIA is that the ETP will use the Healthcare Identifier (HI) Services. ETP service participants will use the HI services to find the healthcare identifiers relevant to the particular participant's function.

6.4 PRESCRIBING AND DISPENSING PROCESS

In brief terms the following is the standard process provided for in the ETP.

1. The prescriber decides to issue a prescription using the EPS. The EPS generates an e-Prescription, its associated metadata and a paper prescription notification. The prescription notification includes the DAK represented as a barcode and as text. The e-Prescription also contains the DAK.

a. The E-prescription may contain, depending on legal requirements, the clinician's duty of care to ensure the right dosage and the settings on the clinicians software:

   i. person's Medicare number
   ii. individual health identifier
   iii. person's name
   iv. person's date of birth
   v. person's gender
   vi. person's address
   vii. information about the medication to be prescribed
   viii. clinical notes
   ix. name of prescribing doctor

b. The meta data is:
   i. the qualified retrieval key
   ii. the ID of the prescriber
   iii. the ID of the prescribing organisation
   iv. date and time prescribed
   v. the expiry date of the prescription
   vi. the number of repeats.

2. The EPS sends the e-prescription and associated metadata to the PES associated with EPS. The e-prescription is encrypted with the cipher key and the whole message is encrypted for transmission to the PES.

3. The PES receives the encrypted e-prescription and stores it in this encrypted form. The PES stores and uses the metadata, in unencrypted form.

4. The patient goes to their chosen pharmacy or dispenser and gives the pharmacist their paper prescription notification.

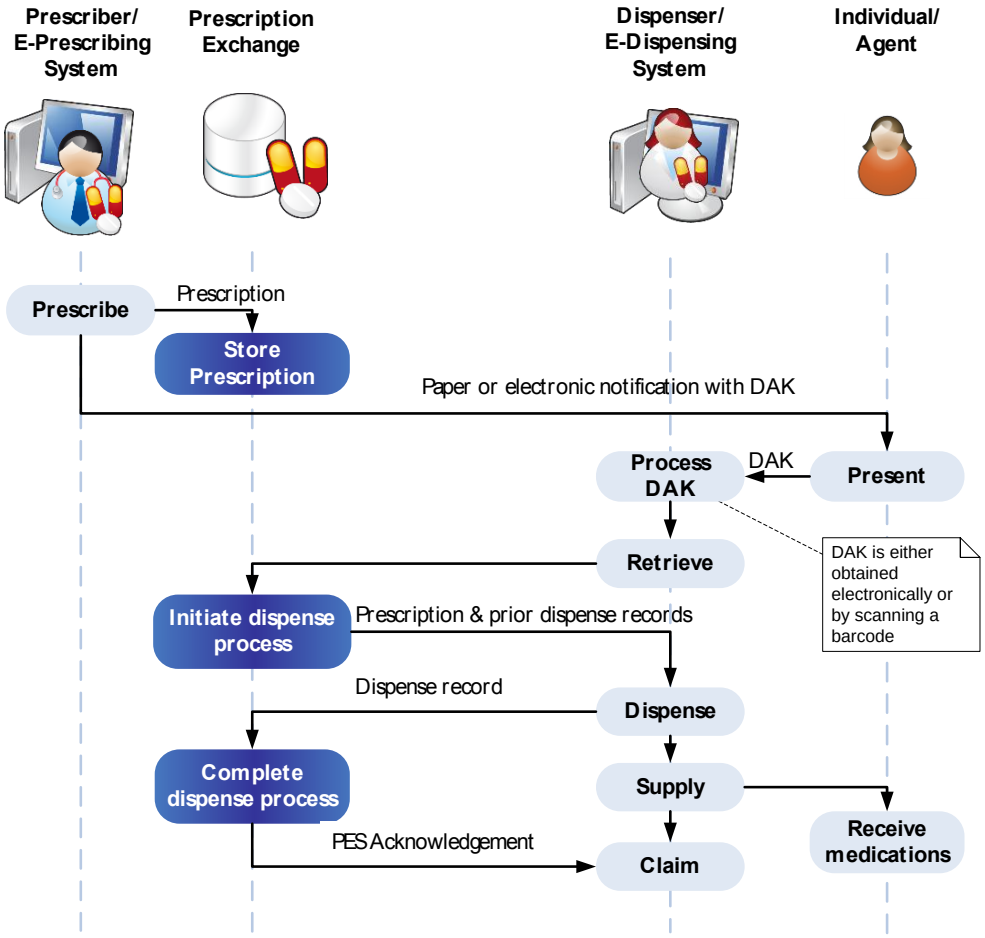
5. The pharmacist or other dispenser, with the patient's implied consent, uses the EDS and the DAK contained on the paper prescription to make a request for the prescription details from the relevant PES.

6. The PES uses the retrieval key on the DAK to find the right e-prescription record and then downloads the encrypted e-prescription record, including any associated records to the dispenser. The EDS uses the cipher key to decrypt the e-Prescription and associated records.

7. The dispenser dispenses the medication.

8. The dispenser uses the EDS to send an encrypted message to the PES to indicate that the medication has been dispensed.

Figure 1: Electronic prescribing and dispensing



7 ADDITIONAL INFORMATION FLOWS PROVIDED FOR IN ETP RELEASE 1.1

7.1 FULLY ELECTRONIC PROCESS

ETP Release 1.1 will support a fully electronic prescription process in which the full prescription details are transmitted electronically without the need for a piece of paper with the DAK on it to be issued to the medication recipient. However, initially, the most common process would be that the individual would receive a prescription notification which is likely to include the clinical details as well as the DAK. The prescriber will print out the e-Prescription and the prescriber will manually sign the printed copy. This will be the 'legal' prescription. This system will be used until such time as prescribers have access to an electronic digital signing system they can use to authenticate themselves.

Once NEHTA has developed rules for prescribers to digitally sign an e-Prescription and the federal Department of Health and Ageing has approved them, the electronic message digitally signed by the prescriber will become the legal prescription, and the paper form will become a copy that is used for convenience purposes. This is likely to happen in the not too distant future.

The final stage will enable the individual to choose to see the e-Prescription electronically and may not need paper at all. For example, the e-Prescription or just the DAK (as well as being sent to the

PE) could be sent to a person's PCEHR and be managed from there. However, paper will be available if the individual wants it. This is several years away at least.

However, ETP Release 1.1 will provide for a fully electronic prescribing system that can be used in circumstances where an organisation is obtaining medication on behalf of an individual with the individual's consent. These organisations will be able to authenticate themselves using their health identifier and NASH.

The following new information flows are also provided for ETP release 1.1.

7.2 CANCELLING PRESCRIPTION PROCESS

There may be circumstances where a prescriber may wish to cancel an e-Prescription. This could occur, for example, if new information comes to light that may cause a prescriber to consider that the medication or a dosage is no longer suitable or appropriate, or the individual is found to be a medication 'shopper'.

The ETP Release 1.1 provides a service by which the prescriber can cancel an e-Prescription. This involves the following steps:

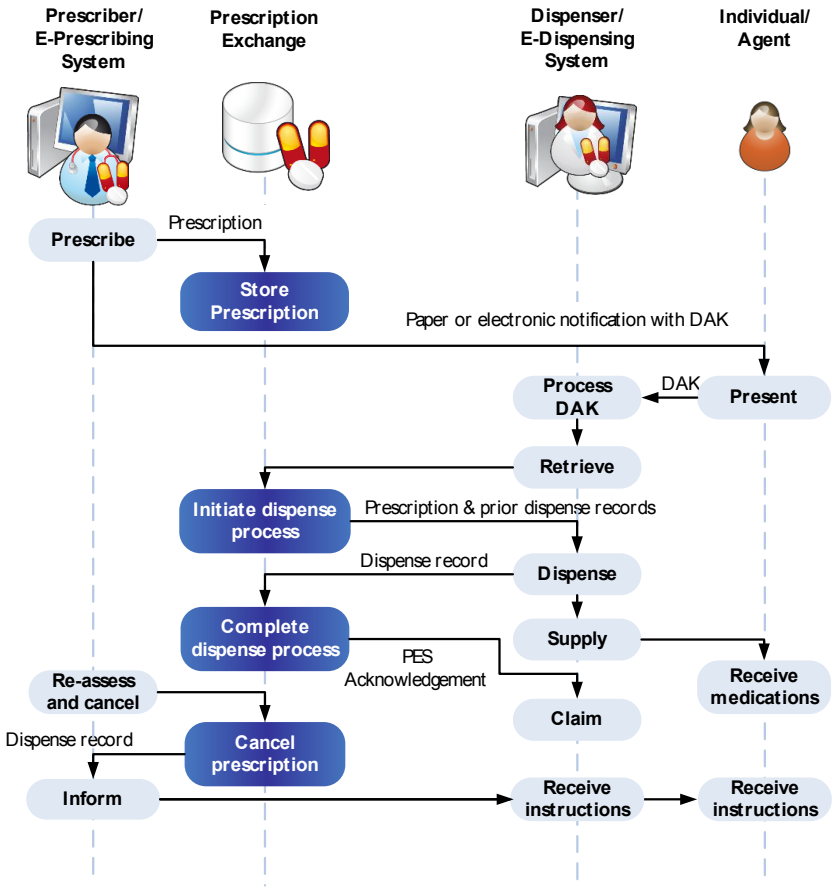
1. The prescriber (or any provider within the same organisation) uses their e-Prescribing system to send a cancellation message to the PES. A quite possible scenario that occurs when a prescriber cancels an e-prescription is that the medication has been dispensed before cancellation occurs, although unfilled repeats may remain.

2. The PES sends to the prescriber a list containing any dispense events that have happened before the e-Prescription was cancelled.

3. This enables the prescriber to manage this problem by contacting (by phone) the pharmacy or dispenser that dispensed the medication, and the pharmacy to contact the individual.

The specifications do not provide for a prescriber to amend an e-Prescription. The process to be followed is to cancel the current e-prescription and then to generate a new one with the necessary changes.

Figure 2: Cancelling prescription process where prior dispense



7.3 NOTIFICATION OF LAST DISPENSE

The ETP specifications provide a facility for the dispenser to notify the prescriber that the last repeat on a prescription has been dispensed and supplied. This would not occur via the PES. The message would be sent directly between the EDS and the EPS.

The specifications propose that this would not be an automatic feature, but rather be activated on a case by case basis and as a result of a conversation between the prescriber and the pharmacist.

This function is optional and assumes the dispenser has obtained the consumer's informal consent to notify a prescriber that the consumer has no repeats left. Use of this function would require there to be an overarching policy on its use.

7.4 PRESCRIPTION REQUESTS FOR 'OWING SCRIPTS'

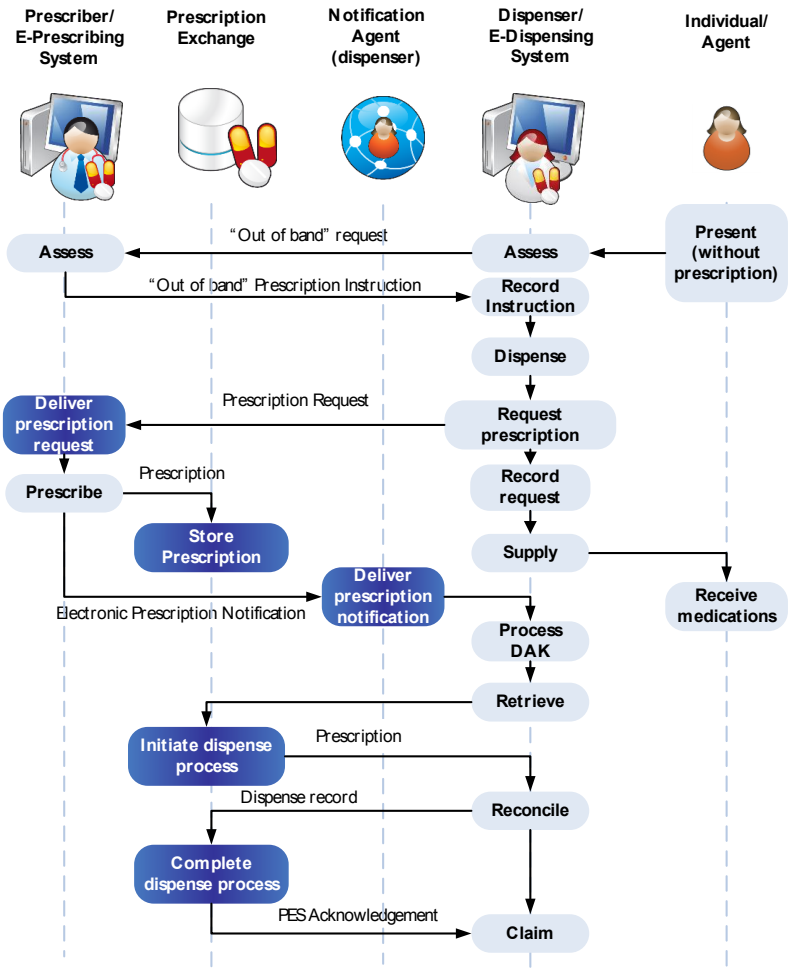
In some cases a pharmacist may find that a healthcare consumer arrives at the pharmacy in need of medication but without a prescription. For example, all their repeats on a drug they must take regularly may have run out and the consumer needs more of the medication. In such cases the pharmacist may phone the person's GP to ask whether or not to provide the medication and to confirm the type of medication.

On the basis of the phone conversation between the pharmacist and the GP, the pharmacist may supply the medication without a written or electronic prescription. This is called a 'script owing'

situation in which, to keep records up to date and to make a claim to the pharmaceutical benefits scheme, the dispenser must still receive an e-Prescription.

ETP Release 1.1 provides for a process by which the dispenser can electronically make a request to the GP or prescriber to provide an e-Prescription and the prescriber sending back an e-Prescription to the PES and a prescription notification to the pharmacist. Once the pharmacist receives the notification and reconciles the request with the medication dispensed, the pharmacist follows the standard electronic process of retrieving the e-Prescription records and returning a dispense record to the PES to complete the process.

Figure 3: Dispensing without an electronic prescription 'prescription owing'



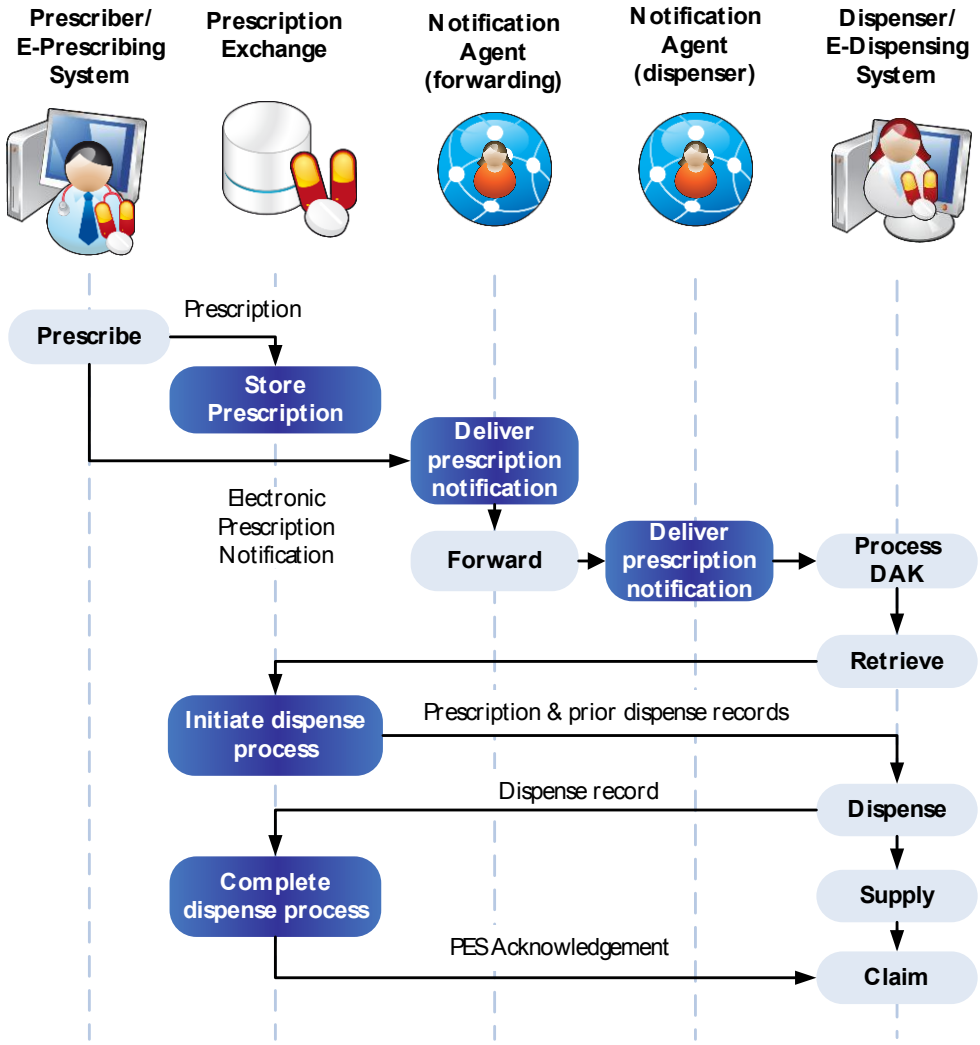
7.5 AGENT-MANAGED SUPPLY – NOTIFICATION AGENTS

There are a number of circumstances in which individuals are unable to attend a pharmacy or dispenser themselves to receive medication. They may have limited mobility, or be incapacitated for various reasons. In other cases, they may not be able to attend a GP personally to get a prescription. These individuals may be in an aged care facility or a private hospital. With the individual's consent these organisations may become the agent through which the individual receives medication. Where an aged care facility or private hospital takes on this role, the facility or hospital usually also has an established contractual relationship with a particular pharmacy or dispenser for the supply of medication.

For these cases, Release 1.1 provides for an electronic agent that the aged care facility or private hospital system can use to have prescription notifications for that individual delivered to them.

In this scenario, the prescriber initiates an e-Prescription as in the process described above. After this the prescriber then sends an electronic prescription notification, which includes the DAK, to the notification agent. Multiple notification agents may be involved in transferring a prescription notification to an electronic dispensing system. For example, where an aged care facility is involved, both the facility and the contracted dispenser may operate a notification agent. In the diagram below, the aged care facility notification agent forwards the prescription notification on electronically to the electronic dispensing system.

Figure 4: Information flow with agent managed supply and notification agents



8 APPLICATION OF PRIVACY PRINCIPLES

Public sector agencies and private sector organisations will be involved in using the ETP. The applicable privacy law and privacy principles vary depending on the jurisdiction and whether an entity is a private organisation or non-government organisation or a public sector agency. Federal public sector agencies are subject to the Information Privacy Principles (IPPs) in the Privacy Act 1988 (Cth). Private sector organisations involved in ETP, by virtue of the fact that they hold health

information will be subject to the National Privacy Principles (NPPs) in the Privacy Act 1988 (Cth). Some State public sector agencies and some private sector organisations such as those in Victoria will be subject to State privacy law and also State health privacy law. Most, but not all, State and Territory law is based closely on the NPPs.

This section analyses the new features of ETP Release 1.1 based, in broad terms, on the NPPs. The IPPs are structured differently, but most aspects can be fitted under the main headings of the NPPs. In broad terms the main difference between the two set of principles are:

- The IPPs do not require consent to collect sensitive, including health information.
- The IPPs do not cover direct marketing.
- The IPPs do not have an anonymity provision.
- The IPPs do not cover transborder data flows.

The NPPs are stronger than the IPPs on these matters and IIS has conducted the analysis on the basis that where the NPPs are stronger, the stronger principles should also apply to personal information in the public sector.

9 POSSIBLE PRIVACY RISKS ASSOCIATED WITH ETP RELEASE 1.1

This section outlines the possible privacy risks and issues that could be associated with ETP Release 1.1. This table only raises issues where IIS considers there could be a matter to discuss. The next section discusses the key privacy risks that are identified here and makes a finding about the issue.

Principle	Possible risk	Possible issue in relation to ETP Release 1.1
Collection limitation including anonymity NPP 1.1, NPP 8, IPP 1.1	Risk that process involves prescriber, dispenser, or PES collecting more information than necessary	Does ETP Release 1.1 result in the PES storing more information about an individual than it needs to? Does it result in the PES generating new audit logs about an individual's interactions with the ETP system? Is it necessary for its function or activity for a prescriber to store the DAK generated by an e-Prescription? Is it necessary for its function or activity for a prescriber to receive dispensing information about an individual when a prescription is cancelled and medication has already been dispensed? Is it necessary for its function or activity for a prescriber to receive information about the last dispense of an individual's prescription?
Consent to collect sensitive information NPP 10	Risk that health information is collected without consent of the individual	Is the individual's consent required for a dispenser to collect prescription cancellation information and for a prescriber to collect dispense information where a dispense has occurred before the cancellation? Is the individual's consent required for the prescriber to receive information that all repeats have been dispensed? Is the individual's consent required for the notification agent to collect prescription notifications on behalf of an individual?

Principle	Possible risk	Possible issue in relation to ETP Release 1.1
Notice and transparency NPPs 1.3, 1.4, 5 and IPP 2	Risk that individuals are not sufficiently aware that information about them is collected, used and disclosed in relation to the ETP Release 1.1 processes	Are individuals likely to be sufficiently aware of what happens to their information during ETP Release 1.1? For example, are individuals likely to be aware that a dispenser may disclose dispense information, or information that repeats have been exhausted may be disclosed to a prescriber? Are individuals likely to be aware of the role of the notification agent? Is there a risk that individuals do not have the necessary understanding of how a fully electronic and paper free ETP system works and the parties involved?
Use and disclosure NPP 2 and IPPs 10 and 11 Including use and disclosure for direct marketing Function creep	Risk that an entity participating in the ETP Release 1.1 uses or discloses prescription or dispense information for a purpose that is not directly related to the purpose for which it was collected and that the individual would not reasonably expect, or for which consent has not been obtained.	Is there an increased risk that a PES service provider might use or disclose e-Prescription records, including dispense information for purposes that an individual might not reasonably expect or agree to? Is there a risk that a prescriber might use dispense information, or repeat exhaustion information for purposes that an individual would not reasonably expect or agree to? Is there an increased risk that a notification agent might use prescription or dispense information about an individual for purposes that an individual might not reasonably expect or agree to? Does ETP Release 1.1 create an increased risk of function creep?
Data Quality NPP 3 and IPPs 7 and 8	Risk that the prescription or dispense information ETP entities collect, use, or disclose about individuals is not accurate complete or up-to-date.	Does ETP Release 1.1 and a fully electronic prescribing system increase the risk that the E-prescription or dispense information is not accurate, complete or up-to-date?

Principle	Possible risk	Possible issue in relation to ETP Release 1.1
Data Security NPP 4.1 and IPP 4	Risk that information collected, stored or transmitted in relation to ETP Release 1.1 is accessed by someone who does not need to see it, or inappropriately accessed by staff or external parties, possibly with malicious intent.	Does ETP Release 1.1 increase the risk of inappropriate or malicious access to E-prescription or dispense information or E-prescription records about an individual? Is there a risk of inappropriate or malicious access to information held by a notification agent? Is the barcode on a piece of paper with numbers under it sufficiently secure
Destruction, or de-identification of data when no longer needed NPP 4.2 and IPP 7	Risk that participants in ETP Release 1.1 hold information about individuals when it is no longer needed.	Does ETP Release 1.1 increase the risk that the PES holds DAK and E-prescription records for longer than it needs to? Is there a risk that a prescriber holds DAK or dispense information for longer than necessary?
Access and correction NPP 6 and IPPs 6 and 7	Risk that individual's cannot access personal information about them stored in relation to ETP Release 1.1	Does ETP Release 1.1 increase the risk that individuals cannot access E-prescription or dispense information or logging information held by participants.
Identifiers	Risk of unauthorised use or disclosure of Commonwealth identifier.	Does ETP Release 1.1 increase the risk of unauthorised adoption, use of disclosure of Commonwealth identifiers?
Transborder data flows NPP 9		Does ETP Release 1.1 increase any risks relating to transborder data flows?
Safety-net for individuals when ETP fails	Risk that if something goes wrong with an ETP process the individuals may have difficulty working out who	Does ETP Release 1.1 increase the risk that individuals will not know who to approach if they experience a problem with an ETP process, or that there is no

Principle	Possible risk	Possible issue in relation to ETP Release 1.1
	to approach to have the problem rectified, and finding someone who will take responsibility to coordinate any cross ETP entity problems to ensure the problem is fixed.	one to take responsibility among the participants for handling such a problem?
Unfair allocation of risk	Risk that terms and conditions relating to ETP Release 1.1 processes place unfair burden of responsibility on individuals to ensure accuracy, security or other privacy measures.	Do the terms and conditions of ETP Release 1.1 place an unfair burden of responsibility for its successful security and functioning on individuals rather than on the other participants such as the prescriber, the PES or the dispenser?

10 DISCUSSION OF RISKS AND RECOMMENDATIONS

10.1 CONSENT, CONTROL AND ETP GENERALLY

In commenting on the Preliminary PIA on the ETP and on this PIA the APF recommended that specific informed consent must be given by a patient prior to an e-Prescription being issued and that the privacy implications of the difference between paper and electronic format must be fully explained as part of the consent process. The Consumers Health Forum did not specifically raise the issue of explicit consent in this context, but said it would welcome measures to strengthen the elements of ETP that relate to disclosure and consent. ACOSS referred IIS to its submission on the Health Identifiers Bill 2010 which indicated a preference for the choice to 'opt-in rather than opt-out' and emphasised the importance of consumer choice and control of their personal health information.

IIS did not consider this specific issue in relation to ETP as a whole in its draft PIA as the Preliminary PIA had considered this issue and made an assessment that that 'the individual does not need to provide explicit consent that would be recorded on the PES to permit the use of e-Prescriptions.'

In the light of the APF's recommendation and the general views expressed by the Consumers Health Forum and ACOSS, IIS has considered the issue taking into account the following factors.

NEHTA says it has addressed a number of imperatives in designing the ETP. These include the need to avoid bogging clinicians down with additional consent obligations when issuing an e-Prescription and to enable individuals to take their e-Prescription to the pharmacy of their choice. At the same time, it has sought to ensure that an individual keeps control over his or her personal information and that the ETP does not create any new privacy risks for the individual. It therefore sought to mirror as closely as possible current arrangements for issuing paper prescriptions. This included enabling the current approach to consent which consists of the act of the individual going to a clinician and asking for relevant treatment including a prescription if necessary.

The designers considered that the main privacy risk would arise if the design of ETP involved new disclosures of personal information about an individual other than to the pharmacy of the individual's choice. Giving the individual choice, at any time of the day or night, about which pharmacy to use, without having advanced notice of which pharmacy the individual might choose, required having a central repository of some sort, such as the PES provided for in the ETP design.

To remove the privacy risks associated with the disclosure to a third party such as a PES, NEHTA designed the system so that there was no effective disclosure of e-Prescription information to the third party PES. It did this by encrypting the e-Prescription and giving the individual control over who gets to see it by providing the individual with the decryption key (the DAK). This means that apart from the prescriber who issued the prescription, the only way anyone can get access to the e-Prescription is if the individual exercises their choice to give the key to a dispenser. This mirrors the current arrangement whereby an individual provides a paper copy to the dispenser.

This is an improvement on the current private sector PES providers who have less stringent protections in place relating to third party disclosure and access. Once NEHTA's ETP specifications are finalised and approved, PES providers will be encouraged to comply with these specifications.

IIS considers that the proposed approach to consent and the ETP is appropriate on the basis that:

- The proposed process mirrors the current process for issuing and filling prescriptions except for use of information technology to transmit the information;
- There is no new disclosure to a third party because the information is encrypted on the PES and not accessible to the provider of the PES;
- The individual controls who has access to the e-Prescription by having control over the DAK;
- The clinician has the option of issuing a paper prescription (in which case the prescription will be fully handled manually including the repeats).

In addition, it will be an improvement on current private sector PES providers which are currently operating with less stringent measures in place.

However, the key to gaining patient trust will be transparency and education about how the ETP works. This is a process which must be taken seriously and to which significant resources should be devoted. This should include the ability to provide a range of options about how an individual will be notified that an e-Prescription has been issued. This means that an individual receiving an e-Prescription should also be entitled to receive a paper **notification** of the e- Prescription which includes all the information contained in the prescription as well as the DAK. This would not add any extra work for clinicians as they already enter information into their clinical applications and provide a printed copy to the individual. Such information should also be included in the future when e-Prescription notifications might be sent to an individual's PCEHR.

Recommendation 1: Business as usual – Transparency and e-Prescription notifications

IIS recommends that NEHTA include in its specifications for ETP that individuals should be entitled to receive an e-Prescription notification that includes all the personal information and clinical content on the e-Prescription. The specifications should require prescribers to offer the option of a paper notification. The notification should include information about where an individual can get more information about ETP.

Recommendation 2: Business as usual – Community awareness and education about ETP

IIS recommends that NEHTA ensures that before and after ETP comes into operation there is an extensive community awareness and education campaign about ETP and how it works. It should include online tools, as well as a brochure that can be handed to the individual at the time an e-Prescription is issued and when an e-Prescription is dispensed.

10.2 Collection must be necessary and loss of anonymity justified

10.2.1 The principles

Privacy principles[4] say that an organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

Privacy principles[5] require organisations, wherever it is lawful and practical, to give individuals the option of not identifying themselves when entering a transaction.

[4] National Privacy Principle 1.1 and Information Privacy Principle 1.1.
[5] National Privacy Principle 8 and Information Privacy Principle 1 collection limitation implies this.

10.2.2 Information collected in an e-Prescription

The APF in its comments on the Preliminary PIA and the draft PIA raised the question of whether some of the information indicated as being included in an e-Prescription is necessary for the purpose of filling a prescription. In particular it raised the question of whether it is necessary to include an individual's date of birth and clinical notes. The APF also raised the question of whether the prescription should include a confidentiality tag and the need to clarify what it might mean.

Once again, IIS did not consider this specific issue in relation to ETP as a whole in its draft PIA as this was a matter to be considered by the Preliminary PIA.

IIS inquired further into this issue and understands that all the fields provided for an e-Prescription in ETP are optional in the sense that they are not configured as compulsory fields. However, some information is required by law, for example, the Medicare number. Others are related to the clinician's duty of care, for example, to ensure that the pharmacy provides the correct dosage. IIS understands that date of birth, or age, is mainly required as a matter of best practice and duty of care where an individual is under the age of 12 years and liver function may be changing rapidly. In this case, dosage may vary significantly according to the weight of the individual. However, once an individual is 12 years or over, dosage becomes more stable and date of birth is much less significant.

IIS understands that date of birth is not currently used to identify the holder of a prescription currently. Indeed no identification is required at all apart from production of the prescription and this will remain so for the dispensing of an e-Prescription.

This appears to indicate that there does need to be a field in the e-Prescription for age, or possibly date of birth, but that it should not be compulsory and indeed should not be included as a matter of course unless the individual is under the age of 12.

IIS also inquired about the need for gender to be included as a field for an e-Prescription and was told that there does not appear to be any need for gender to be included.

On the question of clinical notes, IIS understands that this specification will no longer will be a field called clinical notes. There will be a field called 'reasons for medication' and then another field called 'other comments'. IIS understands that the 'other comments' section would be used for situations where further instructions are needed. An example could be where the GP would like the dispenser to put the medication into a dosage aid, or where the GP would like the dispenser to remind the individual to have their blood tests done.

This information is often included in paper prescriptions and IIS considers that where needed, it should be possible to include it in an e-Prescription. On the other hand, it should not be compulsory to include it and as a matter of compliance with NPP 1.1 should only be collected if necessary. IIS considers that the privacy risk is managed by the fact that such information is encrypted on the PES and only accessible to a dispenser when the individual provides them with the DAK.

Further protection would be provided if e-Prescription notifications include all information on the e-Prescription including reason for medication and any other comments. This will ensure that individuals are aware of the information held in an e-Prescription and to take action to correct it if they think it is wrong. **Recommendation 1** addresses this issue.

Recommendation 3: Technology – Gender in an e-Prescription

IIS recommends that there should not be a specific field for recording gender in an e-Prescription

Recommendation 4: Technology – Date of Birth in an e-Prescription

IIS recommends that an e-Prescription retains a field for recording age (years and /or months) but that specifications require that the field only be used when the individual is under the age of 12.

Recommendation 5: Technology – Configuration of ETP software

IIS recommends that ETP specifications require that ETP software that pre-populates e-Prescriptions only includes information that is necessary for the particular prescription being issued.

10.2.2.1 CONFIDENTIALITY TAG

A confidentiality tag is included as a standard in HL7 of the Clinical Document Architecture Standard. NEHTA says it is aware of the problems of interpreting the meaning of the tag as identified in the Preliminary PIA and will ensure that to gain approval as meeting the ETP specifications an ETP system must have the tag set to 'no value'. IIS considers that this adequately meets the issue raised by the APF.

10.2.3 INFORMATION STORED IN THE PES

IIS considers that the specifications ensure that the PES only receives and stores information that is necessary for it to play its role in the ETP system. For example, it only receives and stores the retrieval key component of the DAK and the metadata associated with the e-Prescription. Because the clinical content is encrypted with the cipher key which the PES does not have, the PES does not have access to the clinical content.

10.2.4 ARE MORE LOGS GENERATED?

ETP Release 1.1 will result in the PES knowing the additional information about an e-Prescription:

- That an e-Prescription has been cancelled and by whom.
- That a particular dispenser has dispensed a medication before the prescription was cancelled.

The PES will not know that a prescription is being sent to an identifiable notification agent. This is only known by prescribing system and the agent.

The PES will not know that a dispenser has asked a prescriber to issue a prescription owing. This is only known by the electronic dispensing system and prescribing systems.

Also, as with the previous release, the PES will not have access to such information as who the message is about or their Health Identifier or any clinical details such as what medication is involved, the dosage etc.

All this information is encrypted and the PES is unable to decrypt it. Given the absence of identifiable information attached to these logs, IIS considers the privacy risk remains low.

Under the previous release, the PES would be able to identify pockets of non-prescribing or pockets of non-dispensing. Under the Release 1.1, the PES would be able to identify pockets of cancelled

prescriptions. But in the absence of access to identifiable information about individuals, IIS considers this remains of low privacy risk.

10.2.5 Prescriber storage of DAK

Under ETP Release 1.1, the prescriber's electronic prescription system stores the DAK for each prescription issued. The new prescription cancellation information flow requires the EPS to retain the retrieval key component of the DAK to enable the PES to identify which e-Prescription has been cancelled. The specifications also provide for the prescriber to retain the DAK so that he or she can reissue the prescription notification (if the patient loses it, for example) or to enable the prescriber, for some undefined reason, to retrieve the e-Prescription from the PES. This could include to reassure him or herself that the e-Prescription has the right information in it, particularly when he or she first starts using the EPS.

IIS considers that a prescriber having the DAK does not create a significant new privacy risk because the DAK does not allow the prescriber to have access to any information which he or she would not otherwise have. When the prescriber enters the DAK to view a prescription he or she only gains access to the same information that was on the original prescription. The DAK does not give a prescriber general access at any time to associated records such as dispense records. So, for example, the GP cannot use a DAK to look, as a matter of interest, at whether a medication has been dispensed or not.

Specifically the system does not allow a prescriber to query the PES using other information about a person to find a prescription or a number of prescriptions. The only way a prescriber can find a particular prescription is to have the particular DAK for that prescription.

10.2.6 Prescriber access to dispense information

As described above, once a prescriber has cancelled an e-Prescription, the PES will send the prescriber dispense records relating to the cancelled prescription in the circumstance where the medication has been dispensed before the e-Prescription was cancelled.

The reason for providing the dispense records where a dispense has occurred before cancellation is to enable the Doctor to take any clinical action that might be necessary where a person's health is threatened, for example, because the wrong drug or the wrong dosage has been prescribed.

In the current manual handling of prescriptions, there would generally be little point in cancelling a prescription as very often there would be no obvious dispenser to notify. A prescriber would not get information about whether a medication has been dispensed. The ability to cancel a prescription is a new function and it enables a prescriber to get information about dispensing that he or she would not have been able to get before.

On the assumption that the ability to cancel a prescription has been identified as being useful and legitimate, it would appear that in some circumstances there are legitimate clinical reasons for providing dispense records to a prescriber and so could be regarded as meeting the requirement to be 'necessary' for a function or activity. As long as prescriber access to dispense records is only in the circumstance of cancellation of a prescription, and only where dispense has occurred before cancellation, IIS does not consider there is any significant privacy risk arising from unnecessary collection.

There may be other risks arising from the individual's knowledge and consent, and these are discussed under the relevant privacy principles below.

10.2.7 NOTIFICATION OF LAST DISPENSE

The notification of last dispense function would result in the prescriber getting information about the status of a prescription and the number of repeats an individual has had filled. For the function to have been activated, the prescriber would know the dispensing pharmacy, and it would mostly be in circumstances where an individual, or an aged care facility or private hospital acting on their behalf with the individual's consent, has a regular relationship with the pharmacy. This kind of notification may already happen off line, and is simply allowing it to be done electronically.

The exchange of this kind of information would appear to be a function closely related to the functions and activities of both pharmacies and prescribers and does not raise any significant privacy risk relating to unnecessary collection.

There may be other risks arising from the individual's knowledge and consent, and these are discussed under the relevant privacy principles below.

10.3 NEED TO GAIN CONSENT TO COLLECT SENSITIVE INFORMATION

10.3.1 THE PRINCIPLE

Privacy principles[6] say that an organisation must not collect sensitive information about an individual unless the individual has consented or an exception applies.

10.3.2 CANCELLATION OF PRESCRIPTION

ETP Release 1.1 involves the following new collections of sensitive (health) information about an individual:

- In relation to cancellation of e-Prescription process:
    - the dispenser collects information that an e-Prescription has been cancelled;
    - the prescriber may receive dispense records relating to the cancelled prescription if dispense has occurred before cancellation;
- In relation to notification of last dispense, the prescriber receives notification that the repeats relating to an individual's prescription has been exhausted;
- A notification agent collects notifications of prescriptions relating to an individual and this includes the DAK which will give the agent access to identifying information about the individual and the clinical content of the prescription.

The application of privacy principle consent requirements in the context of the transfer of medical and health information between clinicians and other closely related practitioners has always been a fluid and grey area. In practice, what has occurred is a close adherence to what most individuals would reasonably expect to happen to their information with implied or express consent in general terms at the time the individual interacts with the GP or other clinician.

[6] National Privacy Principle 10 but not the Information Privacy Principles. Where States or Territories have privacy law, they require consent to collect sensitive information including health information.

Rather than get bogged down in technical legal analysis, IIS considers that the best approach to dealing with consent is to consider what an individual would reasonably expect as an appropriate consent mechanism taking into account the sensitivity of the information and the circumstances and what is practical in the circumstances. This approach may need back up with strict legal advice if necessary.

10.3.2.1 Dispenser collecting cancellation information

IIS considers that a dispenser collecting information that an e-Prescription has been cancelled is directly related to e-Prescribing and likely to be within the expectations of an individual. It is unlikely to require any significant further steps to gain consent than insertion as an item in the consent notices that most GPs and other clinicians provide an individual when they visit. This should be supplemented by more general information about how ETP works to be discussed below in Section 10.3.

10.3.2.2 Prescriber collecting dispense records

IIS considers that an individual is unlikely to expect a prescriber to have general access to their medication dispense records. Although not necessarily good for health outcomes, an individual may nevertheless not want their GP to know on a routine basis whether they have had a prescription filled, or the pharmacy they have attended to fill the prescription. This is could be the case with regard to parts of the population that are on the move, such as seasonal workers and the 'grey nomad' population, neither of which may have any loyalty to any health service at all, possibly seeing any particular service only once in their lifetime. On the other hand, these or other populations on the move may have a real need for this.

When cancelling a prescription, the prescriber has a duty of care to contact the patient to tell them to not take or to stop taking the medication. When the prescriber is unable to contact the patient, they may be able to obtain more up to date contact information from the last pharmacist that dispensed the prescription. Limiting the information in the message to just the fact of dispense and the time of dispense is unlikely to be a solution. To be useful for any kind of follow up action, the message would have to include the location at which the dispense took place.

This would be an extension of current practice which creates some, but not a significant privacy risk.

Getting explicit or even implied consent at the time the prescription is cancelled is difficult because the individual will not be in contact with either the pharmacy or the prescriber at the time the dispense records are sent to the prescriber and an individual is unlikely to have any idea that their prescription has been cancelled. Getting explicit consent in advance in case it does happen at the time of prescription would defeat the whole approach taken in the ETP to consent as discussed in Section 10.1. The options appear to be:

- Not including this functionality at this stage and instead seeking to include it in a later release once trust in and knowledge about the system is more established; or
- Relying on intensive education and awareness and hoping that this will be adequate to address any consumer concerns.

IIS does not consider that there is a high privacy risk in providing this functionality. . IIS considers that individuals are more likely to accept that a prescriber should get such information if there is a good medical reason for it. The limited circumstances in which a prescriber receives this information

in ETP Release 1.1 are likely to be acceptable to most individuals. On the other hand, cancellation after dispense is also likely to be a rare event and so the safety issue is not a pressing one. Given the concerns expressed by the APF, Consumers Health Forum and ACOSS about the importance of disclosure and consent it may be wise to postpone the inclusion of this functionality at this stage. However, should NEHTA decide to include the functionality there should be measures taken to inform individuals about the disclosure of dispensing records to a prescriber in the circumstances of cancellation.

Recommendation 6: Business as usual – Transparency relating to disclosure of dispensing records

IIS recommends that should the notification of dispense on cancellation of prescription proceed protocols developed for participants in the ETP include specifications about how individuals are to be informed that dispensing information could be given to the prescriber and of the circumstances in which this could happen. It should be included in the education and awareness campaign conducted on the implementation of the ETP specifications.

10.3.2.3 Notification agents

IIS considers that the relevant consents for a notification agent to receive prescription information should be obtained. These are easily obtained, and are probably already obtained in relation to paper prescriptions, by the aged care provider at the time that the individual appoints the aged care facility or private hospital to act on their behalf. However, the prescriber may not necessarily know that an aged care facility has that consent. IIS understands that current practice is for the prescriber to send all the paper prescriptions he or she has issued to individuals resident in the aged care facility and the aged care facility works out which residents have given consent and which have not. This appears to be a grey area and IIS considers that it is not appropriate for this practice to carry on into the ETP environment.

Recommendation 7: Business as usual – Policies and procedures for consent to notify prescription

IIS recommends that NEHTA ensure that there are appropriate policies and procedures in place to ensure that a prescriber does not send, and an aged care facility or private hospital does not receive, prescription notifications unless the individual or their authorised representative has given the appropriate form of consent.

10.3.2.4 Notification of last dispense

IIS considers that a pharmacy or prescriber should gain the consent of the individual for last dispense information to be sent to the prescriber. Again, this particularly applies in the case of mobile populations. This could be done informally at the time the prescriber issues the prescription to the individual, or when the individual (or their representative) first goes to, or interacts with, the pharmacy to have the prescription filled.

10.4 Need to ensure that individuals know about and understand about ETP and shared information

10.4.1 The principles

Privacy principles[7] require an organisation to be transparent about a range of information handling matters including the fact that it is collecting information, the purpose for which it collecting the

[7] National Privacy Principles 1.3, 1.4 and 5 and Information Privacy Principle 2. The IPPS require agencies to publish a digest of information they hold rather than provide a general privacy policy.

information and to whom it might disclose the information. An organisation must also make available, if asked, a general policy about the organisation's information handling practices. These obligations apply to organisations collecting information directly from a patron such as licensed venues, or the ID scanning technology provider who may be collecting the information indirectly from the patron.

The preliminary PIA identified the need to ensure that individuals can easily access the applicable privacy policies associated with the ETP. The same issue arises in relation to the new information flows proposed by ETP Release 1.1. NEHTA has identified that it considers the responsibility for notice and transparency lies with prescribers and dispensers and that the ETP specifications are designed to support current clinical practice.

However, in the context of an electronic system where there are a number of different parties communicating in new ways, some of which are not immediately apparent to an individual, for example the role of the PES, there is a much greater need for a consistent approach to providing notice and privacy policies. The approach should also give the individual a picture of how the system operates as a whole. How this should be achieved is a governance issue and is discussed further in Section 11.3 below.

10.5 Need to limit use and disclosure of ID scanning information to primary and related purpose

10.5.1 The principles

In general terms, privacy principles[8] limit the use and disclosure of personal information an organisation collects to the primary purpose of collection, purposes that are related (or in the case of health information directly related) to that purpose and within the individual's reasonable expectations, or those for which a person has given their consent.

There are provisions that allow use of personal information collected for the secondary purpose of direct marketing in certain circumstances and also for some specified law enforcement purposes.

10.5.2 The PES

The new information flows will increase the amount of 'header' information accessible on the PES, but not more information about individuals, because the personal information is encrypted and not accessible to the PES. On this basis, IIS considers the new information flows do not increase the risk of information about individuals held in the PES being used for unrelated or unauthorised purposes.

10.5.3 Prescribers

Having some dispense records and some prescription repeat exhaustion information in electronic form may add slightly to the richness of data about an individual held by prescribers but not sufficiently to add to the risks of unauthorised use or disclosure already identified in the Preliminary PIA. The key here will be audit and accountability mechanisms and this is discussed in Section 11.3.

10.5.4 Dispensers

The only additional information a dispenser will have is that a prescription has been cancelled. IIS considers that this does not add significantly to the possible risk that dispensers may use the electronic information they hold about e-Prescription for unrelated or unauthorised purposes, such as direct marketing.

[8] National Privacy Principle 2 and Information Privacy Principles 10 and 11.

Once again the key here will be audit and accountability mechanisms and this is discussed in Section 11.3.

10.5.5 Notification agents

As a result of ETP Release 1.1 notification agent capability, aged care facilities and private hospitals will have (with the individual's consent) more information in an electronic format about an individual's prescriptions and medications than was held in paper format before. This could make it easier to use or disclose this information for unrelated or unauthorised purposes.

Once again the key here will be audit and accountability mechanisms and this is discussed in Section 11.3.

10.6 Need to ensure information is accurate complete and up to date

10.6.1 The principles

Privacy principles[9] require an organisation to take reasonable steps to make sure that the personal information it collects uses or discloses is accurate, complete and up-to-date.

10.6.2 Discussion

IIS considers that ETP release 1.1 does not increase the risk that information collected, used, or disclosed using the ETP is not accurate, complete or up-to-date. If anything, it reduces such a risk by providing the capability to cancel prescriptions and then issue new ones.

10.7 Need to keep data secure and delete when no longer needed

10.7.1 Security

10.7.1.1 The principles

Privacy principles[10] require an organisation to take reasonable steps to protect the personal information it collects, uses and discloses from misuse and loss and from unauthorised access, modification or disclosure.

10.7.1.2 Bar code

There may be some security issues around the bar code and the fact that there are numbers under the bar code that could be used in a way separate from the person who holds the piece of paper with the bar code on it. The numbers are designed to allow a dispenser to access the prescription when the barcode fails to scan. This is convenient, but increases the ease with which a person could seek to gain access to medication using someone else's prescription. IIS considers that this is not ideal, but only marginally increases the existing risk that someone steals or uses someone else's prescription.

According to NEHTA, this risk will be difficult address until such time as individuals have access to an electronic signing process of the kind that health care providers and dispensers have in relation to electronic access.

10.7.1.3 Discussion

On the information IIS has, ETP Release 1.1 does not appear to increase the risk of inappropriate or malicious access to E-prescription or dispense information held in electronic prescription or electronic dispensing systems.

[9] National Privacy Principle 3 and Information Privacy Principle 7 and 8.
[10] National Privacy Principle 4.1 and Information Privacy Principle 4.

Depending on the security of the systems on which notification agent software is installed ETP Release 1.1 does potentially create a risk that personnel of aged care facilities or private hospitals could misuse could inappropriately access, use or disclose prescription information including HI information on the prescription. Similarly sensitive information is already held on aged care and hospital systems and appropriate security measures should already be in place.

The preliminary PIA raised the issue of appropriate use of DAKs and access to prescription information. The measures NEHTA proposes to address this issue, including requirements for the acceptable use of DAKS should apply to Notification Agents. Measures should also include audit and logging mechanisms that are provided for in relation to the PES, prescribers and dispensers.

Recommendation 8: Business as usual and technology security and notification agents

IIS recommends that the same security mechanisms that will apply to prescribers, PES, and dispensers should also apply to Notification Agents.

10.7.2 NEED TO DESTROY OR DE-IDENTIFY INFORMATION IF NO LONGER NEEDED

10.7.2.1 THE PRINCIPLES

Privacy principles[11] require an organisation to 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 use and disclosure limitation principles.

10.7.2.2 DISCUSSION

ETP Release 1.1 provides that prescription and dispense information is available in the PES for one month after the expiry of the prescription. It is a legal requirement that prescription and dispense information is available on the PES for 12 months, and then under ETP Release 1.1 it becomes unavailable. The Release 1.1 specification does not require that the information be deleted after that time: it just becomes unavailable to prescribers and dispensers.

The rationale for not deleting the information once it is no longer available is that all the personal information on the PES is encrypted and not accessible to PES administrators or others and so there is no strong reason to delete the information from the point of view of PES security. The information is in also stored in backups in encrypted form. NEHTA says that a requirement for a PES to delete all the information, rather than make it unavailable could increase the costs of operation extensively.

IIS considers that given that all the personal information held in the PES is encrypted and not accessible the proposal not to delete the information is reasonable from a security point of view. However, while the information is kept, even in encrypted form, there is potential for the information to be used for new purposes of a kind that might be regarded as unacceptable function creep even if indirectly transferred. The issue of function creep is discussed in Section 11.1.

[11] National Privacy Principle 4.2 and Information Privacy Principle 7.

10.8 Need to give patients access to personal information held about them

10.8.1 The principles

Privacy principles[12] require an organisation, on request, to give an individual access to information it holds about him or her and to correct the information if it is wrong unless one of the exceptions applies.

10.8.2 Discussion

ETP Release 1.1 does not enable an individual to access directly information about them held in the PES. However, as long as they have the relevant DAK the individual could access particular prescription information via their prescriber's electronic prescribing system or via their dispenser to their dispense records for that particular prescription. In the future, some people may want to draw this information into their PCEHR, and if so, this should be possible. Although a technical interpretation of the privacy principles could entitle an individual to have direct access to information about them held on the PES, in practical terms, this is generally unlikely to be asked for.

Furthermore, establishing a mechanism for an individual to achieve this is likely to create security and access vulnerabilities that far outweigh any privacy benefit. In the short term, by far the best mechanism is transparency about the information about them contained in an e-Prescription (on paper and/or in the future through their PCEHR) and for an individual to approach the prescriber or the dispenser who can identify the individual and is in a position to address any inaccuracies or other issues relating to the content of the records.

However, sometimes failure could occur in the PES, and if so, there should be an emergency mechanism by which any problems with records can be handled. This is likely to be rare, but there should be a governance mechanism that covers this contingency. The issue of governance is addressed in Section 11.3.

10.9 Limitations on the use of Commonwealth identifiers

10.9.1 The principles

Privacy principles[13] say in general terms that an organisation must not adopt as its own identifier an identifier assigned to an individual by a State of Commonwealth government agency. It also says that an organisation must not use or disclose such an identifier unless it is necessary for the organisation to fulfil its obligations to the agency, there are law enforcement related reasons, or there are regulations which allow it to.

10.9.2 Discussion

The key Commonwealth identifiers used for ETP are the Medicare number and the Individual Health Identifier. ETP Release 1.1 does not appear to raise any new risks relating Commonwealth identifiers.

10.10 Need to protect information moving across borders

10.10.1 The principles

NPP 9 prescribes the circumstances in which an organisation may transfer personal information about an individual to a foreign country. The IPPs do not have such a principle. Where State or

[12] National Privacy Principle 6 and Information Privacy Principle 6 and 7.
[13] National Privacy Principle 7 but not the Information Privacy Principles.

Territories have privacy law, it generally prescribes the circumstances in which information about an individual can transfer information across borders.

10.10.2 Discussion

ETP 1.1 does not appear to raise any immediate risks in relation to the movement of ETP information to overseas jurisdictions. However, it could be that a PES provider or an online pharmacy might seek to operate off shore in the future. This could raise privacy risks that are not currently able to be addressed within the current Australian or International privacy regulatory framework. The APF also raised concerns about the privacy risks associated with the flow of e-Prescription information sent or stored off shore. IIS considers that it is not appropriate in the current environment for PES operators to be able to operate offshore, or for e-Prescription information to be transmitted overseas. However, the ability to adequately protect information off shore may change in the future.

Recommendation 9: Business as usual – Transborder data flows

IIS recommends that a PES provider should not be approved as meeting the NEHTA specifications if it proposes to transmit or store e-Prescription data outside Australia unless there has been a Privacy Impact Assessment including public consultation which establishes that the e-Prescription information can be protected to the level it would have if it remained in Australia.

11 OTHER RISKS

11.1 Function creep

11.1.1 The issue

When any new technology is being implemented involving personal information, there is always a risk that uses for the technology will be extended and people will seek to use the information collected for new purposes. Whether or not such expansions are welcome or accepted or seen as unwelcome 'function creep depends on their nature and how they are made. The difference may simply be the speed of introduction, the degree to which the community is taken into confidence and other subtle matters.

At other times, the difference is more real and will never be considered as anything but function creep because it is seen as an inappropriate invasion of privacy, for example if changes are introduced with insufficient surrounding governance mechanisms such as transparency and accountability mechanisms to ensure abuse or unintended consequences do not happen.

11.1.2 Discussion

There is clearly envisaged in the future that information about individuals held in the PES might be used in identifiable form for secondary purposes such as:

- Inclusion in a Personally Controlled Electronic Health Record (PCEHR) including in an index facility designed to support the ability to retrieve health records from distributed repositories;
- For approved research by approved Health research bodies.

The specifications include the capacity for such activities in the future but also indicate that it is expected that this would only occur with the individual's consent. However, as yet, there is no indication of how this consent might be obtained or what process might be followed before use for such secondary purpose was allowed to proceed. There could be a push from some quarters to dispense with individual consent on the grounds that it is too time consuming, expensive or cumbersome.

A further complication is that organisations operating a PES could be private sector organisations. The only other way, besides individual consent for secondary use to occur would be if it was authorised or required by law. Because of the way the ETP is designed, if the law allows it, this would involve the prescriber allowing its release each time he or she makes a new prescription and this process would have to occur via a trusted an authorised third party whose public key is included in the DAK. There is no capacity for bulk release of e-Prescription data from a PE. This means that a PES could not on its own make a decision to release e-Prescription data to third parties. If release has not been provided for at the time of the prescription, there is no technical way for e-prescription information to be released in bulk to third parties because they do not have access to the DAK.

Use of e-Prescription information for new purposes could be acceptable to members of the community, but there should be a mechanism for ensuring that these secondary uses do not occur without a proper assessment process, including a PIA and comprehensive community consultation.

This requires there to be an adequate governance process for ETP. This is discussed in Section 11.3.

11.2 Safety-net when things go wrong and unfair burden of risk

11.2.1 The issue

A key problem with many new technologies is that while they may of great assistance in managing the risks of the organisation, they very often shift significant risk to the individual. Particularly where there are a number of organisations involved, it can be difficult to identify the source of the problem and who is responsible for fixing the problem and restoring the individual to their previous situation. It is very common for no one to be prepared to accept responsibility, for the individual to be treated as the cause of the problem, and for the individual to be passed from one organisation to another.

This may be further exacerbated by terms and conditions that place unfair burden on individuals to protect their security and place minimal responsibility on the other participants.

11.2.2 Discussion

IIS considers that given that there are a number of participants in the ETP process there is scope for an individual to fall between the cracks if something goes wrong. Problems could arise in relation to any one of the participants such as the PES, the electronic prescription system, or the electronic prescribing system and each one of these could seek to avoid responsibility for any failures.

The individual could be left being not sure who to approach or how to have the problem resolved. Although some of the participants may be private sector and some may be public sector there should be a mechanism for ensuring that where individuals experience problems with the ETP there is a responsive mechanism for handling the problem and ensuring that there is a coordinated approach to resolving issues. Once again this is matter of ensuring that there is adequate governance of the ETP process.

11.3 NEED FOR STRONG GOVERNANCE INCLUDING ACCOUNTABILITY

IIS considers that the key risk associated with ETP Release 1.1 is that there will be an inconsistent and uncoordinated approach to a number of matters relevant to the privacy of individuals and their trust in the system. IIS considers that the risks are sufficiently significant that they cannot simply be left to the operation of general privacy law. Issues identified above which relate to governance and accountability include:

- That there may not be a consistent and adequate approach to consent to collect health information by prescribers and by dispensers.
- That there may not be a comprehensive and consistent approach to transparency and informing individuals about how the ETP operates as a whole, including the role of the PES and the kinds of information being exchanged between participants.
- That there may not be adequate accountability mechanisms to ensure that all participants are complying with requirements in the ETP specifications, requirements and protocols or the requirements of privacy law.
- That there may not be a coordinated approach to handling access to ETP information, including emergency access to PES information should this be necessary.
- That there may not be a coordinated approach between the PES, a prescriber and a dispenser to handling individual complaints where problems or failure occurs and no one to take responsibility to ensure the complaint is resolved or the problem fixed.
- There may be no mechanism for monitoring or managing function creep and ensuring that significant change that affects individual privacy does not occur without appropriate steps including PIAs and community consultation.

Recommendation 10: Governance and accountability

IIS recommends that NEHTA advocates the need for there to be put in place an appropriate governance mechanism which provides:

- a mechanism for ongoing oversight of the operation of ETP as a whole;
- a mechanism for developing a consistent and coordinated approach to:
    - policy relating to the ETP;
    - information and transparency about how the ETP operates, the role of each participant and the information flows between the participants;
    - implementing audit and accountability mechanisms to ensure that all participants comply with the applicable privacy and security requirements and obligations – this should include independent audits and random inspections carried out on processes used by PES operators and dispensers;

- providing access to information held by the participants where necessary or an emergency;
- managing failure and complaints;
- developing fair terms and conditions, if any, imposed on individuals in relation to the ETP;
- monitoring and managing function creep;

- Public reporting on the operation of ETP in relation to each of these matters.

12 ISSUES RAISED IN OTHER FEEDBACK ON ETP DOCUMENTS

This section discusses the feedback that NEHTA has received on the ETP specification documents it released for public comment on 6 September 2010[14]. Feedback has raised the following matters that have privacy implications. In this section IIS considers the privacy implications, and, where necessary makes a recommendation.

12.1 UNDISPENSED E-PRESCRIPTIONS

ETP Release 1.1 currently only allows a dispenser to include notes about a successful dispense. Some feedback has suggested that dispense records associated with an e-Prescription should include any refused or rejected dispensing and possibly the reason for the refusal or rejection. The rationale appears to be that this would prevent prescription shopping, or someone from seeking to accumulate a hoard of certain kinds of drugs.

However, this inclusion would create a number privacy issues. For example, including information that a dispense was unsuccessful or rejected, without including the reason, may lead to inappropriate inferences to be drawn. The dispenser seeing that the previous attempt was unsuccessful might conclude that there is something suspicious when there are a number of reasons why a dispense could be unsuccessful. This could include:

- That the dispenser has made a professional judgement that the prescription should not be issued, for example, a mistake has been made;
- A belief that the prescription was gained fraudulently;
- That the particular medication was out of stock.

The key privacy risk is that a dispenser would be making a decision of the basis of information that may not be accurate, complete or up-to-date in breach of NPP 3.

On the other hand, including reasons for failure to dispense could lead to a wide range of information about an individual being included in ETP data, some of it likely to be inaccurate, discriminatory or prejudicial. This could also be in breach of NPP 3 and create a time consuming and costly onus on dispensers to ensure that the information they include is accurate complete and up-to-date. It would also complicate the system further by requiring a much greater emphasis on access to ETP records and a right of correction as required by NPP 6.

[14] http://www.nehta.gov.au/e-communications-in-practice/emedication-management

In either scenario, it would raise complicated issues of consent.

The proposal would also take the ETP away from its core function which is to simplify and make more accurate and efficient the dispensing of medication, into secondary areas of catching people who use prescriptions in inappropriate or illegal ways.

Recommendation 11: Undispensed e-Prescriptions

IIS recommends that NEHTA does not provide for the capability to include in records associated with an e-Prescription the information that a dispense was unsuccessful or the reasons why.

12.2 Inclusion of Close the Gap annotation

One stakeholder has suggested that it should be possible for a prescriber to include in the e-Prescription an indication that the prescription was issued under the Indigenous Close The Gap program by adding the letters CTG in the notes section of the e-Prescription. This enables the Indigenous person to get medication at a lower than normal cost.

This information is currently included in paper prescriptions and IIS understands that it is governed by Medicare regulations. This facility seems to be simply implementing existing practice and does not appear to raise any privacy risks than were already in existence. IIS makes no recommendation about this.