Maddocks

Lawyers
Level 1
40 Macquarie Street
Barton ACT 2600 Australia

Telephone 61 2 6120 4800
Facsimile 61 2 6230 1479

info@maddocks.com.au
www.maddocks.com.au

Australian Capital Territory Health Directorate

Digital Health Record Solution

Privacy Impact Assessment

Date of Analysis: April 2021
Date Finalised: March 2022

Contents

Part A EXECUTIVE SUMMARY

1. Introduction

1.1 The Australian Capital Territory Health Directorate (**ACT Health**) has procured a digital health record solution (**DHR Solution**) from a third party software vendor, Epic Systems Melbourne Pty Ltd (**Epic**), to provide a solution that will deliver a comprehensive medical record for Patients (a **Patient's DHR**) that will support the delivery and management of all publicly funded facilities in the Australian Capital Territory (**Territory**) including the three public hospital facilities (Canberra Hospital, Calvary Public Hospital Bruce, University of Canberra Hospital), all public mental health facilities, community health centres, Walk-in Centres and community based care (**Health Services**).

1.2 A Patient's DHR will be a 'person-centred' electronic medical record. It will maximise access to clinical information by the treating team at the point of care, so health practitioners providing health care in a Health Service (**Clinicians**) to a Patient will no longer have to search multiple clinical systems and paper records to find the information needed to provide safe and high-quality care.

1.3 ACT Health has commissioned this privacy impact assessment (**PIA**) to consider the privacy impacts of implementing the DHR Solution and to inform the design of the DHR Solution.

1.4 This PIA:

1.4.1 considers the impact of the implementation of the DHR Solution, which will result in the creation of Patient DHRs. In this context, this PIA does not examine all associated business processes (such as policies associated with, or procedures used by Clinicians or other staff in connection with, the provision of a health service to a Patient where personal health information is obtained);

1.4.2 considers compliance with the *Health Records (Privacy and Access) Act 1997* (ACT) (**Health Records Act**), including the Privacy Principles contained in the Act (referred to as '**HPPs**' in this PIA report), and, to the extent relevant, the *Information Privacy Act 2014* (ACT) (**Information Privacy Act**), including the Territory Privacy Principles (**TPPs**);

1.4.3 sets out the information flows, which help to highlight privacy risks and areas for improvement in terms of risk mitigation;

1.4.4 is intended to help ACT Health manage identified privacy risks and impacts, in respect of the DHR Solution;

1.4.5 is intended to provide ACT Health with guidance on privacy risks, and potential privacy enhancing measures to inform the design of the DHR Solution;

1.4.6 may serve to inform ACT Health and other stakeholders about the privacy elements of the DHR Solution; and

1.4.7 considers the safeguards that have been, or should be, put in place to secure personal information from misuse, interference or loss, or from unauthorised access, modification or disclosure.

2. Summary of findings

2.1 We consider that ACT Health has shown a genuine appreciation of the importance of properly considering and addressing privacy risks associated with the implementation of the DHR Solution. In this respect, we see the conduct of this PIA at this early stage of implementation of the DHR Solution as demonstrating ACT Health's commitment to incorporating 'privacy by design' into its processes.

2.2 Overall, based on the information available to date on the implementation of the DHR Solution, our analysis has not identified any significant privacy risks.

2.3 In our view, the implementation of the DHR Solution includes some **privacy enhancing features**, such as:

2.3.1 an enhanced ability for Patients to be able to access their own records through the Patient Portal;

2.3.2 strong security requirements and contractual protections for the DHR Solution (to mitigate the potential privacy risk associated with consolidation of all information currently located in multiples sources into a single record, thereby providing motivated intruders with a single source of personal information to attack); and

2.3.3 enhanced ability to track access to personal information about Patients (including personal health information) (**Patient Information**) (through logs and audits of access to a Patient's DHR), to identify any unusual or unauthorised access (which may not be possible with paper-based records).

2.4 We have however identified some **potential privacy risks** related to the implementation of the DHR Solution. These include privacy risks associated with:

2.4.1 the potential for a Patient's DHR to be inappropriately accessed by persons who, although authorised to access the DHR Solution, do not have an appropriate need or reason for accessing a particular Patient's DHR (the DHR Solution does not appear to use technical measures to restrict or limit access within a role, e.g. to the treating team members for a Patient);

2.4.2 Patients may be unaware that their personal health information has been collected in their DHR, particularly in relation to any clinical photographs, information from medical devices, or information from other 'consumer wearable devices' (**Wearables**); and

2.4.3 noting the potential for the DHR Solution to be flexible and for its design to be significantly further developed and enhanced in the future, the potential risk that privacy factors may not be appropriately considered at the time that the extended functionalities are approved or implemented.

2.5 These risks are further discussed and considered throughout this PIA report. A number of recommendations set out in paragraph 3 of this **Part A** are designed to address the identified risks.

2.6 We also make the followings **observations**:

2.6.1 Health Services are delivered in partnership between the Territory Government and a range of different providers, including Calvary Health Care ACT Limited, the largest health service provider in the Territory. Providers have different organisational structures and requirements, and are subject to different arrangements that reflect the different services provided. Calvary has a separate contractual relationship that governs the relationship between Calvary and Territory.

2.6.2 The introduction of the DHR Solution is a key shift in the way Health Services are to be provided in the Territory and the continued provision of quality, safe, effective and efficient Health Services in the Territory is therefore dependent on the continued partnerships with those providers and requires consideration of the different arrangements documented with these partners.

2.6.3 The extent to which the personal health information in a Patient's DHR is handled appropriately will depend to a large extent on Users understanding their existing obligations under the Health Records Act. We note in this respect that ACT Health, as part of its planning for the implementation of the DHR Solution, has identified training of Users as paramount to the success of the DHR Solution. This training includes training on the User's privacy obligations. As is the case now, Health Services are responsible for ensuring their staff are appropriately trained and will continue to be responsible for ensuring staff understand their privacy obligations. As best practice, privacy training should be refreshed on a regular basis, which we understand will be the case for Users.

2.6.4 The introduction of the DHR Solution will more readily facilitate the sharing of personal health information between Health Service locations (including those operated by entities that are contracted by the Territory to provide public health services, such as at Calvary Public Hospital Bruce, which will ensure that persons receiving public health services in the Territory will have access to more up-to-date information to inform clinical decision making. This sharing of relevant personal health information between Health Services is already provided for under current legislative and policy frameworks, and the implementation of the DHR Solution does not itself introduce any new privacy risks in this regard. We note, for example, access to Calvary Public Hospital Bruce patient records by other Health Services is supported by a number of HPPs in the Health Records Act and that implementing **Recommendation 9**, in relation to the arrangements for the provision of services at Calvary Public Hospital Bruce, may strengthen the basis on which the DHR Solution is used in the Territory. The arrangements in relation to Calvary Public Hospital Bruce are discussed in more detail at section 14 of Part D.

2.6.5 ACT Health's Identity and Access Management Services will be an even more critical part of the implementation of the DHR Solution. For example, it will be necessary to ensure that persons who cease providing public health services within the Territory (for example, where a locum contract ceases) do not continue to have access to the DHR Solution. This may not be a significant risk if the DHR Solution is only accessible at a Health Service location by persons with security access to that location, but the potential risk of unauthorised access to the DHR Solution will be increased if persons can access the DHR Solution on mobile devices outside of a Health Service location, and that person's access to the DHR Solution is not removed.

2.6.6 The Health Records Act may not now represent current medical practice and advances in technology, such as the ability to have a patient-centred electronic medical record. In our view, many of the HPPs are difficult to rationalise, particularly in situations where the TPPs still have some operation. The Territory may wish to consider, as part of its broader work, whether the implementation of the DHR Solution is an opportune time to review the Health Records Act to assess whether it continues to meet the objectives for which it was enacted, particularly given the Information Privacy Act and the proposed review of the *Privacy Act 1988* (Cth).

2.7 In addition, the recommendations in paragraph 3 of this **Part A** also include suggestions for ways in which ACT Health could further enhance privacy protections associated with the DHR Solution, and/or further strengthen ACT Health's compliance with the HPPs and TPPs.

3. Recommendations

3.1 This PIA makes the following recommendations in relation to the DHR Solution:

Recommendation 1 **Governance measures**	**Relevant Privacy Principles**
We **recommend** that ACT Health ensure that it has suitable governance processes in place in relation to the further functionality or enhancement of the DHR Solution, which will ensure any privacy implications of the new or changed functionality which might affect the information flows identified in this PIA are considered and addressed before any extended functionalities are approved or implemented. This could include: • ensuring that examination of privacy implications is a standing item/issue that must be addressed in any change documentation; and • treating this PIA as a 'living document' which is reviewed and updated as further enhancements are considered, including undertaking further updates or supplementary PIA processes as required.	**All**

ACT Health Response:	**Agreed** ACT Health has established a governance framework for the Digital Health Record Program which has been approved by the Digital Health Record Program Board. Processes for approving workflow adoption or changes in the system will consider whether there are any privacy impacts, and will escalate through this governance structure for impact analysis and mitigations as required. Primary responsibility for assessment of this function will be raised into the already established Security, Privacy and Access Working Group which will report to the Technical Steering Committee and the CIO. ACT Health will be specifically tasked to brief the Digital Health Record Program Board as required.

Recommendation 2	**Further promote openness and transparency about the handling of personal information in connection with the DHR Solution**	**Relevant Privacy Principles**
To ensure that personal information is managed in an open and transparent way, we **recommend** that ACT Health consider: • publishing this PIA, or a summary form of its findings and recommendations, on its website; • ensuring that information on the DHR Solution is included on its, and/or Canberra Health Services, websites so persons understand how their personal information in the DHR Solution will be handled (i.e. by whom personal information will be accessed, for what purpose, and how it will be used and disclosed). This information could include a suitable privacy notice; and • when implementing the DHR Solution, include as part of the work program that any relevant admissions forms be updated to refer to the website. Information (for example, in the form of pamphlets) containing information about the DHR Solution could also be prepared and made available when a person presents at a Health Service.		**TPP 1**
ACT Health Response:	**Agreed** ACT Health will publish this PIA and any additional supporting information on the ACT Health website at https://www.health.act.gov.au/privacy and will provide the PIA to Health Services to publish on its websites. ACT Health will also establish a dedicated contact point for any consumer or health provider enquiries in relation to privacy and the DHR.	

Recommendation 3	**Mitigating against misuse of personal health information**	**Relevant Privacy Principles**
We **recommend** that ACT Health give further consideration to whether it is feasible to implement additional technical measures for the DHR Solution, in addition to the current strategies of requiring compliance with policies and procedures, to mitigate the risk of Users accessing a Patient's DHR where they have no business need to do so. For example, measures that could be considered might include: • the DHR Solution's capabilities being used to identify any unusual or unexpected access to a Patient's DHR (for example, if a User accessed a Patient's DHR where that person had not recently interacted with a Health Service)**;** • the DHR Solution including a mechanism for a Clinician who is a User to be advised that they need to be a member of the relevant Patient's treating team before being able to access a Patient's DHR (or perhaps the Clinician could be required to confirm this) – noting that the benefits of this privacy protection would need to be balanced against any operational inconvenience for Clinicians; and/or		**HPP 4.1**

• DHR Solution screens that allow Users to search for a Patient's DHR could include a prominently displayed statement that 'Persons are only authorised to access a record where they have a business need to do so. Your access will be logged and is auditable'. Alternatively, if the above is not practical, we **recommend** as a privacy enhancing feature that ACT Health ensure that the training provided to Users before access is granted to the DHR Solution includes training on their privacy obligations, including when they may or may not use or disclose Patient Information.	
ACT Health Response:	**Agreed, and ACT Health intends to implement the measures outlined in dot points one and two.** ACT Health will be defining during the implementation of the DHR audit report requirements on access to records and will consider what message will display each time a user logs into the system to remind them of their privacy obligations. The example in dot point three is not a practical process to implement due to the impost it would cause to the workflow. However, ACT Health will ensure that mandatory training for all privacy aspects is completed before access is given to the DHR Solution.

Recommendation 4	**Notice to be provided to Patients about the collection of information from Wearables**	**Relevant Privacy Principle**
For Wearables, we **recommend** that consideration be given to ensuring that either: • the DHR Solution will give a notice to the Patient before their Wearable is linked to the DHR Solution and their Patient Information is uploaded; or • ACT Health implements policies and procedures so that it is satisfied that the provider of the Wearable will issue such a notice before the linking occurs. The notice should explain to Patients that linking will cause their personal health information to be collected by ACT Health and stored in their Patient DHR, and be accessible to ACT Health staff who provide Health Services to the Patient.		**HPP 2**
ACT Health Response:	**Agreed** ACT Health will develop appropriate guidance material and consumer consent prior to the connection of any Wearables in the following circumstances: 1. Consumer owned devices to be connected to the DHR; 2. materials to review and refer to when coming into the hospital in the event that Wearables are used in the course of a hospital stay; and 3. Health Service issued devices where a Wearable is used for an outpatient appointment (i.e. Holter Monitor, Insulin Pump etc).	

Recommendation 5	**Collection of Patient Information in the form of clinical images**	Relevant Privacy Principles
We **recommend** ACT Health consider supporting existing policies and procedures that are designed to ensure compliance with HPP 2, by considering whether it is feasible from a technical and operational perspective for the DHR Solution to display a prompt to a User who is seeking to upload a clinical photograph of a Patient to the Patient's DHR. Such a prompt could advise (or perhaps require the User to acknowledge) that the Patient has given their verbal consent to the image being taken and then stored in the Patient's DHR.		**HPP 2**
ACT Health Response:	**Agreed** The DHR solution can be configured to capture a user acknowledgement that the patient has consented (written or verbally) for the clinical image to be uploaded to the DHR.	

Recommendation 6	**Confirm that DHR Solution specifications facilitate compliance with certain HPPs**	**Relevant Privacy Principles**
We **recommend** that ACT Health confirm that the design specifications for the DHR Solution contain functionality to: • maintain a register of records that have been destroyed or transferred as required by HPP 4.2; • allow Health Services to destroy or de-identify a Patient's DHR if it is no longer needed, as required by HPP 4.3; • deal with alterations to a Patient's DHR in the manner set out in HPP 7. That is, the DHR Solution should not allow a user to delete information from a Patient's DHR but be able to make appropriate corrections or additions if information is found or claimed to be inaccurate, or permit creation of a separate record with the incorrect information in the circumstances permitted by HPP 7; and • allow for destruction or de-identification of personal information about external Users when that information is no longer required, in compliance with TPP 11.2.		**HPP 7**
ACT Health Response:	**Agreed** Processes for the above DHR functionality will be documented, and necessary registers will be configured as part of the DHR Solution implementation.	

Recommendation 7	**Processes for granting access to external Users other than Patients (e.g. external health providers, Carers, ICT service providers of support for the DHR Solution)**	**Relevant Privacy Principles**
We **recommend** that, when designing the processes to be used to grant access to the DHR Solution for external Users, ACT Health take into account that: • only the minimum personal information required to identify the person should be solicited (for example, information about their political associations would not be relevant or necessary and should not be collected); and • a suitable TPP 5 collection notice covering the TPP 5 matters is provided to the User at the time they are registering or otherwise applying for access to the DHR Solution.		**TPP 3**
ACT Health Response:	**Agreed** ACT Health will take into account the above-mentioned points when granting externals Users access to the DHR Solution. The process for external Users to apply for access to the DHR will incorporate a collection and privacy notice at the time of application.	

Recommendation 8	**Seeking consent for specific purposes**	**Relevant Privacy Principles**
We **recommend** in accordance with best practice that: • specific consent be obtained from a Patient if their photograph will be uploaded to the Patient's DHR so that it can be used by Users to assist them in identifying that person in the future (we do note that the consent could be obtained orally, if appropriate); and • provide a Patient with the option to 'opt-out' of the Patient's DHR being used for the purposes of identifying potential candidates for participation in approved research projects. Where a Patient so opts-out, that Patient should not be included in any lists generated to identify potential candidates for research.		**TPP 3**
ACT Health Response:	**Agreed** Throughout the system configuration process, the capture of consent and opt out processes will be defined and implemented.	

Recommendation 9	**Protecting and strengthening privacy in arrangements with third parties**	**Relevant Privacy Principles**
We **recommend** that any contractual or other arrangements with another organisation to provide public health services in the Territory, where that other organisation will have access to, and use, the DHR Solution: • include a specific requirement to comply with any relevant policies, including those dealing with records and/or the handling of personal information; • include an express requirement to comply with the Health Records Act and the Information Privacy Act at all times in connection with the delivery of the Health Services; and • provide clear rights and obligations in relation to the access and use of records when delivering the Health Services, including the use of the DHR Solution. We suggest that this recommendation could be implemented through review and (if necessary) updating of existing contractual arrangements, or by supplementing those arrangements with agreed ancillary governance documents.		**All**
ACT Health Response:	**Agreed** ACT Health will ensure that express contractual terms are incorporated in relation to privacy requirements for any new arrangements. For existing arrangements, ACT Health will work with the other party to the arrangement to determine whether contractual arrangements require updating or whether ancillary governance documents are required to support the DHR Solution .	

Part B METHODOLOGY AND ASSUMPTIONS

4. Our methodology

4.1 This PIA has been conducted in accordance with the *Privacy Impact Assessment Guide* (**PIA Guide**) issued by the OAIC, using the following methodology.

Stage	Description of steps
1.	**Plan for the PIA:** We have reviewed relevant background material provided by ACT Health (as set out in **Attachment 2**), and were provided with briefings by officers from ACT Health. We discussed the policy intent behind the collection of personal information through the DHR Solution and clarified our understanding of the technical and other arrangements for the DHR Solution. We discussed and agreed the scope of this PIA generally.
2.	**Stakeholder consultation:** When undertaking our analysis and forming our views about privacy risks, we have taken into account: • feedback provided by ACT Health; and • our research about reasonable community expectations of privacy. For example, the *Australian Community Attitudes to Privacy Survey 2020* commissioned by the OAIC contains useful information regarding current community expectations, including about the level of trust in government agencies' handling of personal information, including personal health information. ACT Health also undertook stakeholder consultation with consumers and representatives of consumer groups . The feedback from of this consultation process is set out below.
3.	**Privacy impact analysis and compliance check:** In this step we focussed on compliance against each TPP and privacy best practice. The analysis set out in this PIA is consistent with the Information Privacy Act, which outline the mandatory requirements of the TPPs. We also considered compliance with the Health Records Act, which applies to personal health information (as discussed further in **Part D**)
4.	**Privacy management and addressing risks:** We considered existing mitigation strategies in place and further potential mitigation strategies that could reduce or remove the privacy impacts and risks identified during the previous step.
5.	**Recommendations:** From the steps referred to above, we developed our recommendations, designed to remove or reduce privacy risks.
6.	**Draft report:** We prepared a draft version of this PIA report.
7.	**Further refinement of draft PIA report**: Following review of the draft report by ACT Health, we further refined our analysis and potential mitigation strategies as required to ensure that privacy risks were appropriately considered and addressed. We also refined the draft PIA report to take into account feedback received by ACT Health during its consumer consultation process.
8.	**Final Report**: We finalised this PIA report, including incorporation of ACT Health's responses to our recommendations.

Consumer Consultation

4.2 To ensures that consumer perspectives informed this PIA report, ACT Health approached the Heath Care Consumers' Association (**HCCA**), the peak health consumer organisation in the Territory, and a number of individual consumers. A draft of the PIA report was provided to consumers nominated by the HCCA and feedback was obtained by the ACT Health from these consumers at a meeting.

4.3 The consumers consulted were generally positive about the implementation of the DHR Solution, acknowledging the benefits that a DHR will provide to consumers and Clinicians.

4.4 Consumers, however, raised the following specific concerns:

4.4.1 consumers were concerned about a Patient's mental health history being available to treating team members when it was not relevant to the health service being provided (for example, the provision of physiotherapy service);

4.4.2 consumers were concerned that a Patient's medical history would be accessible to any Clinician with access to the DHR Solution, even where they ceased to be a treating team member. Consumers wanted to understand the sanctions that would apply to a Clinician accessing a Patient's DHR where the Clinician is no longer a treating team member and how any sanctions will be enforced;

4.4.3 consumers sought confirmation that there will be a proxy for access to a Patient's DHR for Patients with severe mental health issues, compliant with law; and

4.4.4 consumers considered it important that Patients be able to consider whether to participate in research on a case-by-case basis, that is, consumers may want to be included in some research projects but not others.

4.5 We note that some of the concerns related to issues broader than the implementation of the DHR Solution. For example, consumers raised some concerns about the processes used for considering research projects which will not be directly impacted by the implementation of the DHR Solution, although the DHR Solution may facilitate the ability to undertake particular forms of research more readily. However, we address the concerns raised in our analysis against the HPPs and TPPs.

4.6 A glossary of defined terms and acronyms is at **Part G** of this PIA report.

5. Assumptions and qualifications

5.1 We have conducted our analysis on the basis that the factual information provided by ACT Health (as set out in **Part C** of this PIA report) is up-to-date, correct and complete.

5.2 We have assumed that the current ACT Health and the Canberra Health Services' policies provided to us are consistent with all legislative requirements.

5.3 This PIA does not analyse or examine any information flows, or associated privacy risks or compliance issues, that are not described in **Part C** of this PIA report.

Part C PROJECT DESCRIPTION AND INFORMATION FLOWS

6. Overview of the ACT Health Digital Health Record Solution

6.1 ACT Health has procured the DHR Solution, to provide a solution that will deliver a comprehensive medical record to support the delivery and management of Health Services.

6.2 The DHR Solution will deliver a 'person-centred' electronic medical record for Patients. It will:

6.2.1 include the following information about Patients:

(a) Patient administration data; and

(b) their clinical records; and

6.2.2 be hosted on a hybrid cloud environment.[1]

6.3 The objectives of the DHR Solution are to:

(a) improve the quality, safety, effectiveness and efficiency of health care services by providing enabling technology to support the implementation of the Territory-wide Health Services;

(b) provide a real-time patient clinical record that can be accessed by all members of the treating team regardless of physical location or organisational affiliation;

(c) capture all clinical interactions performed in the one central repository;

(d) deliver improved clinical decision support with global best practice advanced tools and a more complete view of patient information;

(e) support research initiatives and clinical care innovations through access to high quality data, identification of patients that match studies and supporting collection of informed consent;

(f) standardise data capture of core activities;

(g) provide capabilities to support achievement of Healthcare Information and Management Systems Society (HIMSS) Electronic Medical Record Adoption Model (EMRAM) of Level 6 by 2023/24 and Level 7 by 2026/27; and

(h) replace the ACTPAS patient administration system, to provide improved patient scheduling and administration as well as building the foundations for patient self-service.

6.4 The DHR Solution will record all interactions between Patients and Health Services. These will include interactions in major hospitals (i.e. the Canberra Hospital and the Calvary Public Hospital Bruce), community health centres and 'walk-in centres' in the Territory. Currently, across the Health Services, data is captured electronically in a number of separate systems as well as in paper records. The DHR Solution will consolidate many of those clinical systems and information into a single record. The DHR Solution is not intended to be used by the Health Protection Service.[2]

[1] We understand this to be a mixture of technical hardware and Territory-controlled environment.
[2] The Health Protection Service is responsible for preventing public health incidents, as well as monitoring and enforcing public health regulations and providing public health advice.

6.5 Health Services are primarily delivered in the ACT by:[3]

6.5.1 Canberra Health Services (**CHS**), a separate administrative unit to ACT Health under the *Public Sector Management Act 1994* that is responsible for health services and facilities operated by the Territory government; and

6.5.2 Calvary Health Care ACT Limited (**Calvary**), engaged by the Territory to provide public hospital services at Calvary Public Hospital Bruce.[4]

6.6 Each Patient who accesses services at a Health Service will have a health record created for them in the DHR Solution (referred to as a **Patient's DHR** in this PIA report). The personal health information collected in the DHR Solution will include sensitive health information regarding services accessed in relation to mental health, sexual health and justice health.[5] At a basic level, a Patient's DHR represents a single health record for that Patient across the Health Services.

6.7 Health records must be kept in a manner that complies with the Health Records Act. The Health Records Act does not require the consent of a Patient to create a health record.

6.8 A Patient's DHR will be accessible by their health care team at any Health Service location. The intent is that this will allow staff to have faster access to information, which will improve care and reduce errors. A Patient's DHR will also be able to be accessed by the Patient (or their Carer) through a secure website or a mobile app.

6.9 ACT Health will be responsible for the implementation the DHR Solution, together with Epic and NTT Australia Pty Ltd (**NTT**), who will provide the hosting solution and subsequent operation to support the Health Services.

7. The DHR Solution

7.1 The DHR Solution, at a high level, will:

7.1.1 facilitate the collection, use, disclosure and storage of personal information, including personal health information of Patients, in real time, across the Territory;

7.1.2 enable real time monitoring to take place, by receiving and processing personal health information from a number of other sources, including medical devices and earlier treatment information or medical history, in the course of services being provided at a Health Service; and

7.1.3 allow Patients to access and view a subset of information held on their Patent's DHR.

7.2 The DHR Solution will create a single database built up of many modules, each covering one or more areas of the clinical workflow. Broadly, the modules cover inpatient services, ambulatory services, speciality systems, patient administration and bed management, mobile devices (to provide medical staff with access to patient information), population health management tools and external provider communication, patient engagement (including a patient portal); and business intelligence tools.

[3] We note that the Territory has also engaged a private organisation to provide health services at the Tresillian Queen Elizabeth II Family Centre. This PIA report focuses on the provision of public health services by CHS and Calvary, as the providers of the key public health services within the Territory. However, the commentary in this PIA report about the provision of public health services provided by Calvary (a private entity) will apply to any private entity engaged by the Territory to provider public health services within the Territory.
[4] Calvary also runs a private hospital, however, this PIA report only deals with the provision of public hospital services by Calvary.
[5] For example, health services accessed while in correctional facilities.

7.3 A Patient's DHR will be accessible by Clinicians, administrative and other staff providing services at Health Services. As part of the DHR Solution, staff profiles will be built relying on ACT Health's Identity Access Management services, that will result in staff becoming authorised users of the DHR Solution (**Users**).

7.4 The DHR Solution will operate on User based permissions. Under the model, Users will have permission to amend a Patient's DHR based on their role (for example, while administrative staff may be able to view a Patient's DHR, they will not be able to amend clinical information). Audit functions are available to ensure that access is appropriate to the role the User is performing. The DHR Solution can, if required, restrict certain records (VIPs, Employee records, sensitive records such as concerning sexual health and mental health, forensic testing, young adult records transitioning from parental care etc), with additional processes required to view the information (this is referred to Epic's 'Break the Glass' functionality). Work is continuing, which will be informed by consultations with a range of stakeholders, on what records will be restricted and only able to be viewed through the 'Break the Glass' functionality.

7.5 Access to information in the DHR Solution will depend on the role of the User and the implementation of policies based on the need to access the information. For example, all Clinicians in Health Services can access the DHR Solution and all Patients' DHRs. However, under the policy, only treating team members should access a Patient's DHR (unless they are otherwise accessing a Patient's DHR for the purposes of the management, funding or quality of the relevant health service).

7.6 In practice, a treating team can include current and referring Clinicians for a particular episode of care. For example, where a Patient nominates a particular General Practitioner (**GP**) on hospital admission, the GP is considered as a member of the treating team.

7.7 A Patient's DHR will be able to be accessed by Users through a number of channels, including kiosks, mobile devices (such as, smart phones and tablet, including on personal devices), patient bedside terminals, and computers.

7.8 The DHR Solution will integrate with about 100 ACT Health systems, for example the pharmacy inventory management system.

7.9 The DHR Solution will have the ability to 'push' information to treating team members who are not Health Services staff (for example, discharge summaries, letters and results relating to a Patient may be sent to their GP).

7.10 The DHR Solution also has the ability for external health care providers (i.e. those providers outside of Health Services) to be provided with access to the DHR Solution. However, the processes and procedures that would be used to do this (i.e. the information that would be collected about the User in order to establish their profile) is not yet known.

7.11 The DHR Solution will also include a "**Patient Portal**". This portal will allow the Patient (and any Carer that is authorised) to access the Patient's DHR. Access to the Patient Portal will be through a mobile app or a web browser.

7.12 Epic and NTT will have access to the DHR Solution only for the purposes of providing the contracted support services, and are subject to contractual requirements to keep information secure and confidential.

7.13 The DHR Solution will include an "**Electronic Data Warehouse**" (**EDW**). The EDW will store all Patient Information, and will hold all data that is captured not only by the DHR Solution but all related healthcare services and systems. Extracts from the EDW will be used for the purposes of providing information to external registries or for analysis in third party systems. The DHR Solution will record what is extracted from the EDW.

7.14 Health Services also currently has a "**ACT Health Data Repository**", and we understand that data stored and used in this repository that captures longitudinal data sets may be integrated to the DHR Solution, at a later date.

8. Collection of Personal Information

8.1 **Overview**

8.2 We have set out below the separate instances by which personal Information (including personal health information) will be collected by the DHR Solution. In summary, personal information (including personal health information) is **collected**:

8.2.1 about an external health service provider at the time of registration for access to the DHR Solution;

8.2.2 about a Patient (and Carer if relevant) by an administrative Health Services' staff member to create a Patient's DHR;

8.2.3 about a Patient (and their Carer, if applicable) when they register to access the Patient Portal;

8.2.4 about a Patient through the Patient Portal;

8.2.5 about a Patient by a Clinician or Health Services' administrative staff when they enter information into the DHR Solution;

8.2.6 about a Patient by a Clinician using an ACT Health system integrated with the DHR;

8.2.7 about a Patient by an external health care provider where the information is sent to the DHR Solution;

8.2.8 about a Patient received from other systems that will be integrated with the DHR Solution, such as ICT systems used by pathology or radiology laboratories; and

8.2.9 about a Patient by a system or device that automatically collects Patient Information, such as medical devices or Wearables, where that system or device will be integrated with the DHR Solution.

8.3 **Details of collections**

Personal information is collected about an external health service provider at the time of registration for access to the DHR

8.4 External health service providers will be able to be provided with access to the DHR Solution. The process to register an external health service provider to gain access to the DHR Solution has not yet been determined and may rely on Health Services' provider index. Whatever process is ultimately used, ACT Health will need to collect personal information about individual health service providers at the time of registering them for access to the DHR Solution, in order to decide whether or not to provide them with access.

Patient Information (and Carer information) is collected to create a Patient's DHR in the DHR Solution

8.5 Where a Patient presents at a Health Service or is referred to a Health Service by an external health service provider, administrative staff will search for the Patient on the DHR Solution by entering a range of search terms, including Patient's name and Date of Birth (**DOB**). If there is an existing Patient DHR, further verification steps will be taken to verify the Patient. These verification steps will be set out in a Patient Identification Policy, which is yet to be determined.

8.6 If the Patient does not already have a Patient DHR, administrative staff will create a Patient DHR for the Patient. In this process they will collect from the Patient, at least the following information:

8.6.1 the full name of the Patient;

8.6.2 address;

8.6.3 DOB;

8.6.4 contact number;

8.6.5 next of kin details; and

8.6.6 Medicare card number for Australians.[6]

8.7 A unique reference number (**URN**) will be assigned to the Patient.

8.8 Consideration is currently being given to using the Individual Healthcare Identifier (**IHI**) for a Patient to be used as the identifier in the DHR Solution. The IHI is a unique 16-digit number used to identify an individual for health care purposes. The DHR Solution will collect the IHI at least for the purposes of disclosing summary information in a Patient's DHR to their My Health Record.

8.9 Consideration is also being given to including a photograph of a Patient on the Patient's DHR for identification purposes. The process for doing this has not yet been determined but is anticipated that a photograph may be taken (i.e. collected) when a person attends at a Health Service. However, the DHR Solution does not require that a photograph be included in a Patient's DHR.

8.10 We note in this context where a Patient has a Carer, the DHR Solution will also collect information about the Carer. Health Services have established processes for authorising Carers for a Patient. Consideration is currently being given to how the DHR Solution can facilitate these processes.

Patient (and their Carer) registers to access the Patient Portal

8.11 The DHR Solution will collect information about Patients and any relevant Carers when they register to access the Patient Portal. The process for this registration is yet to be determined, but we understand it may involve the use of the Patient's ACT Digital Account.[7]

Patients (or their Carers) add information through the Patient Portal

8.12 The DHR Solution will collect Patient Information thorough the Patient Portal if Patients (or Carers) enter information to be included in the Patient's DHR. For example, responses to questionnaires, feedback provided, or uploading any advance care planning documents.

[6] We note that additional information may also be required to be collected at this point, but further details are not yet available.
[7] Consideration of the operation of ACT Digital Account is outside the scope of this PIA.

Patient Information is entered by Clinicians or ACT Health administrative staff

8.13 Patient Information will be collected by the DHR Solution when Clinicians or administrative staff within Health Services directly enter information to a Patient's DHR.

8.14 For completeness, we note that the DHR Solution will involve the migration of personal health information in existing Health Services systems to establish a Patient DHR, for those Patients that have already interacted with the Health Services. This will not be a new collection of that information but will be a **use** of personal health information that Health Services already holds about Patients.

Patient Information is collected by Clinician using an ACT Health system integrated with the DHR Solution

8.15 The DHR Solution will integrate with a number of other ACT Health systems. Work is currently being undertaken as to how the data will be exchanged between the DHR Solution and these other systems.

Patient Information is collected when external health care provider sends information to the DHR

8.16 External health providers, including GPs, will collect Patient Information in the course of creating bookings and through referral services.

8.17 The existing external messaging provider "**Healthlink**" provides services to connect information from the GP's system to the DHR Solution.

8.18 We understand that, in later phases of the implementation of the DHR Solution, external health providers will be given access to the DHR Solution in order to upload Patient Information to the DHR Solution.

Patient Information is collected through the integration of other systems to the DHR Solution

8.19 The DHR Solution will allow Patient Information to be uploaded (and therefore collected) from other ICT systems that are integrated with the DHR Solution, such as ICT systems used by pathology or radiology laboratories

8.20 For example, upon receiving a service at an appropriate pathology laboratory, Patient Information (including results and reports) will be able to be uploaded to DHR Solution, which will ensure that the Patient Information is included in the Patient's DHR, where it can be accessible to the Patient's treating team (including external health providers, if applicable).

8.21 This would provide a seamless way for information to be included in a Patient's DHR without manual handling of results (which could result in inputting errors).

Patient Information is collected through medical devices on site at Health Services

8.22 Patients at Health Services may be fitted with a medical device that passively collects Patient Information (such as heart rate monitors, dialysis machines, ultrasound technology, or infusion pumps at a Patient's bedside).

8.23 The DHR Solution will enable such Patient Information to be uploaded to a Patient's DHR, where it will be able to be viewed by relevant Clinicians.

Patient Information is collected through Wearables

8.24 Patients of Health Services may also have other Wearables which passively collect Patient Information (such as a 'fitbit' or similar device).

8.25 The DHR Solution will in future allow Patients to choose to link their Wearables with the DHR Solution, so that their Patient Information collected by that device is uploaded to the Patient's DHR. However, specific details about how this will occur are yet to be determined.

9. Use of Patient Information

9.1 **Overview**

9.2 We have set out below instances of how personal information (including personal health information) will be **used** in connection with the DHR Solution.

9.3 In summary, personal information in the DHR Solution will be **used** by Health Services in the following ways:

9.3.1 for the provision of direct clinical care of a Patient of a Health Service;

9.3.2 for administrative management of a Patient of a Health Service;

9.3.3 to respond to a Patient's request for information about themselves;

9.3.4 for the operation and support of the DHR Solution, including the operation of the in-built machine learning functionality, maintaining the relevant ICT infrastructure, and other system improvements;

9.3.5 for other 'business as usual' purposes of the relevant Health Service, including for operational purposes such as quality improvement, audit activities and reporting.

9.4 The above points are discussed in more detail below at paragraphs 9.7 to 9.14.

9.5 We note that Patient Information in the DHR Solution is also **used** by a range of other entities and persons as follows:[8]

(a) by an external health care provider to provide care to a Patient or in connection with the provision of care to a Patient (including where the external provider is engaged to support the relevant Health Service, e.g. for send-away pathology or radiology tests, or transcription of letters).

(b) by a Patient to manage their own healthcare; and

(c) by a Carer to manage the healthcare of a Patient.

9.6 ***Patients receiving clinical care at a Health Service***

9.7 When a Patient receives care at a Health Service, those Clinicians providing care will login to the DHR Solution and search for a Patient's Individual DHR.

9.8 When searching the DHR Solution, a Patient's DHR will be searched by entering a range of search terms, including Patient's name and Date of Birth (**DOB**).

[8] We note that these uses also correspond to a **disclosure** by ACT Health through the DHR Solution, as discussed below.

9.9 Clinicians will then have access to the Patient Information in the Patient's DHR.

9.10 The Patient Information will be **used** by Clinicians to deliver health care services to the Patient.

Administrative management of a Patient of a Health Service

9.11 Administrative staff will access and **use** Patient Information for the purposes of amending Patient Information, facilitating care, or facilitating the delivery of business as usual functions within the relevant Health Service, including clinical coding and billing.

Responding to Patient's request for information about themselves

9.12 The DHR Solution will be **used** to respond to the requests from Patients to access their health record (i.e. Patient's DHR).

Operation and support of the DHR Solution

9.13 Patient Information in the DHR Solution will be used for the operation and support of the DHR Solution, such as:

9.13.1 by ACT Health ICT support staff when they access Patient Information required to maintain the proper operation of the DHR Solution infrastructure; and

9.13.2 through the application of artificial intelligence and machine learning capabilities to identify improvements that will improve the quality of service, for example, frequently used buttons.

Business as usual operations

9.14 Users will be able to access information in the DHR Solution to continue to undertake the normal administrative and operational functions of the relevant Health Services. This might include accessing and using information in the DHR Solution (including Patient Information in a Patient's DHR):

9.14.1 to respond to requests by Patients (or their Carers or legal representatives) for access to a medical record (in accordance with current policies and processes);

9.14.2 for medico-legal purposes, including seeking legal advice;

9.14.3 for the management, funding, or quality of the Health Service, including informing best clinical practice and identifying potential research candidates;

9.14.4 to prepare statistical reports;

9.14.5 undertaking or facilitating approved research activities; and

9.14.6 other functions or activities authorised or required by law.

10. Disclosure of Patient Information in the DHR Solution

10.1 **Overview**

10.2 We have set out below instances of when personal information (including personal health information) may be **disclosed** from the DHR Solution. In summary, personal information in the DHR Solution may be **disclosed** by Health Services to:

10.2.1 a Patient or Carer;

10.2.2 to external health care providers (including those engaged to support the relevant Health Service);

10.2.3 My Health Record; and

10.2.4 potentially, to other entities in the context of 'business as usual' operations (for example, to respond to medico-legal requests, such as to the coroner).

10.3 ***Disclosure to Patient or Carer***

10.4 Patient Information in the Patient's DHR will be disclosed to Patient or Carer through the Patient Portal.

10.5 Patient Information in a Patient's DHR may also be disclosed through other means to Patients and Carers when responding to a request for access to a Patient's health record, including in hard copy.

10.6 ***Disclosure to external health care providers***

10.7 Patient Information in a Patient's DHR may be disclosed to external health care providers:

10.7.1 when an external health care provider is given access to the DHR Solution; or

10.7.2 when a Health Service receives a request to provide Patient Information to an external health care provider (e.g. a request showing the Patient had consented to the transfer of all of their Patient Information to another external health care provider, the User may cause the DHR Solution to send the relevant information to the external health care provider.[9]

10.8 For completeness, it is intended that the disclosure of Patient Information for clinical/medical purposes to external health care providers may be potentially facilitated through:

10.8.1 Epic's "**EpicCare Link**" application, which is a web-based application that provides external health care providers with secure access to real-time Patient Information held in the DHR Solution; and

10.8.2 Epic's "**EpicCare Everywhere**" platform, which facilitates the exchange of a Patient's DHR (that is, the whole record) with another organisation that also has an Epic digital health record system.

10.9 As the potential deployment of EpicCare Link and EpicCare Everywhere is at a very early stage of consideration at the time of drafting this PIA Report, we have set out at **Attachment 3** high level guidance on issues for ACT Health to consider before deciding whether to share information in the DHR Solution with external entities using these Epic products.

Business as usual operations

10.10 Users will be able to access information in the DHR Solution to continue to undertake the normal administrative and operational functions of the relevant Health Services. This might include accessing and disclosing information in the DHR Solution (including Patient Information in a Patient's DHR):

10.10.1 to entities in response to medico-legal requests, such as to Executors in relation to deceased estates; or

10.10.2 to entities as required by law, such as responding to a Court Order.

[9] We understand that, as per current processes, no Patient Information would be sent unless and until the Health Service is satisfied that the Patient's consent had been provided, and a record review had been undertaken in relation to the request (to determine if the information is available, and to ensure that no exemptions that prevent the release of the Patient Information apply).

11. Information flow

11.1 A simplified diagram outlining the information flows is provided at **Attachment 1** to this PIA report.

Part D KEY CONCEPTS

12. Applicable Privacy Principles

12.1 The Information Privacy Act applies to ACT public sector agencies and contracted service providers (including subcontractors). The Information Privacy Act includes 12 TPPs in Schedule 1 which are modelled on the Australian Privacy Principles (**APPs**) in the *Privacy Act 1988* (Cth). The Health Records Act includes 14 HPPs that apply to persons providing health services in the Territory.

12.2 ACT Health and CHS are subject to the TPPs under the Information Privacy Act as well as the HPPs under the Health Records Act. As a contracted service provider, Calvary in delivering Calvary Public Hospital Bruce is also subject to the TPPs and HPPs.[10]

12.3 The Information Privacy Act applies to 'personal information'. The definition of 'personal information' excludes 'personal health information' as defined in the Health Records Act[11]:

> (1) For this Act, ***personal information***—
>
> (a) means information or an opinion about an identified individual, or an individual who is reasonably identifiable—
>
> (i) whether the information or opinion is true or not; and
>
> (ii) whether the information or opinion is recorded in a material form or not; but
>
> (b) does not include personal health information about the individual.
>
> (2) In this section: ***personal health information***—see the *Health Records (Privacy and Access) Act 1997*, dictionary.

12.4 The Health Records Act defines 'personal health information' as:

> **personal health information**, of a consumer, means any personal information[12], whether or not recorded in a health record—
>
> (a) relating to the health, an illness or a disability of the consumer; or
>
> (b) collected by a health service provider in relation to the health, an illness or a disability of the consumer.[13]

12.5 The Health Records Act further defines 'health record' as

> **health record** means any record, or any part of a record—
>
> (a) held by a health service provider and containing personal information; or
>
> (b) containing personal health information.[14]

[10] We also understand that Calvary is also subject to the *Privacy Act 1988* (Cth) as it is a 'organisation' as defined in that Act.
[11] Information Privacy Act, s 8.
[12] The Health Records Act defines 'personal information' for the Act in relation to a consumer as ' any information, recorded or otherwise, about the consumer where the identity of the consumer is apparent, whether the information is—(a) fact or opinion; or (b) true or false.
[13] Health Records Act, Dictionary.
[14] Health Records Act, Dictionary.

12.6 It is relatively clear that a Patient's DHR will be a 'health record' within the meaning of the Health Records Act, as the Patient's DHR will contain information relating to a person's health, illness or disability. Accordingly, compliance against the HPPs need to be assessed in relation to the implementation of the DHR Solution.

12.7 However, the DHR Solution also includes, more broadly, matters and processes about persons other than Patients, such as use of information about Health Services personnel to provide access to the DHR Solution, and collection and use of personal information about external health care providers to provide them with access to the DHR Solution. These processes deal with personal information about those individuals that is subject to the TPPs.

13. Key terms in the Health Records Act

13.1 The HPPs in the Health Records Act impose obligations on various persons: 'collectors', 'health service providers' and 'record keepers'. ACT Health, Calvary, CHS and Users are all subject to the HPPs in different ways.

Meaning of 'collector'

13.2 The Health Records Act defines 'collector' in the Dictionary at Schedule 1 as *a 'person who, in the course of his or her profession, employment or official duty, collects personal health information'*. Although the *Legislation Act 2001* (ACT) provides that a general reference to a person includes a reference to a corporation as well as an individual, the phrasing of the definition, which refers to 'his or her profession' etc, suggests an intention that a collector is an individual.

13.3 In the context of the DHR Solution, 'collectors' will be Users in the Health Services who collect information from a Patient, for example, when a Clinician takes notes as part of a consultation with a Patient or administrative staff member that obtains information from a Patient for the purposes of updating their Patient DHR.

Meaning of 'health service provider'

13.4 The Health Records Act defines 'health service provider' in the Dictionary at Schedule 1 as *'an entity that provides a health service'.* **'**Entity' is defined broadly under the *Legislation Act 2001* (ACT) to include '*an unincorporated body and a person (including a person occupying a position)'.*

13.5 In the context of the DHR Solution, a 'health service provider' will include a Clinician providing a health service but can also refer (depending on the context and the relevant HPP) to the Health Service that is providing the health service.

Meaning of 'record keeper'

13.6 The Health Records Act defines 'record keeper' in the Dictionary at Schedule 1 as **'***an entity that has possession or control of a health record'*. The words 'possession' and 'control' are not further defined.

13.7 In our view, 'possession or control' of a record is equivalent to the concept that applies where an agency 'holds' personal information for the purposes of the TPPs under the Information Privacy Act. The Information Privacy Act defines 'holds' at s 16 as:

> a public sector agency ***holds*** personal information if the agency has possession or control of a record that contains the personal information.

13.8 We note OAIC's APP Guidelines, while relevant to the APPs under the *Privacy Act 1988* (Cth), do provide useful guidance on the interpretation of the TPPs (and by extension is illustrative when interpreting the Health Records Act).

13.9 The APP Guidelines clarifies that the term 'holds' extends beyond physical possession of a record to include a record that an entity has the right or power to deal with:

> 'Whether an APP entity 'holds' a particular item of personal information may therefore depend on the particular information collection, management and storage arrangements it has adopted. For example, an APP entity 'holds' personal information where:
>
> - It physically possesses a record containing the personal information and can access that information physically or by use of an electronic device (such as decryption software)
>
> - It has the right or power to deal with the personal information, even if it does not physically possess or own the medium on which the personal information is stored. For example, the entity has outsourced the storage of personal information to a third party, but it retains the right to deal with it, including to access and amend that information.'[15]

13.10 That is, the question is whether an entity has effective control over the personal information. This is an objective test requiring assessment of the particular factual circumstances.

13.11 For example, in the OAIC's investigation of the data breach associated with the DonateBlood.com.au site, the OAIC found that the Australian Red Cross Blood Service (**ARCBS**) which did not physically hold the personal information in the relevant data file (as this was stored on its contractor's systems), nevertheless retained effective ownership of the data given the nature of the contractual relationship with its contractor. The OAIC found that both the ARCBS and its contractor held the personal information in the data file and therefore had relevant obligations under the Privacy Act. However, the OAIC's publicly available report does not outline the specific provisions of the contractual arrangement between the ARCBS and its contractor which gave rise to its finding about who was 'holding' the relevant information.[16]

13.12 In the context of the DHR Solution, it is relatively clear that Calvary and CHS (as the entities that primarily provide the Health Services) are each record keepers for the purposes of the DHR Solution as their staff can deal with the personal health information in a Patient's DHR, for example, to amend records.

13.13 However, ACT Health is also likely to be considered a 'record keeper' for the purposes of the Health Records Act as the DHR Solution (and Patient DHRs) will be held in ACT Health controlled ICT environment so ACT Health will have possession of the health records and it can control the management of the information in the DHR Solution, through its contractual arrangements with Epic and NTT.

13.14 We have also considered whether Epic and NTT will also be 'record keepers' for the purposes of the Health Records Act. The APP Guidelines provides useful guidance on this as well. That guidance provides the following as indicators of whether an agency maintains 'effective control' over personal information, rather than an ICT or other service provider:

13.14.1 a binding contract between the entity and the contractor, which requires the contractor only to handle the personal information for these limited purposes;

13.14.2 provisions in the contract, which give the entity effective control of how the information is handled by the contractor. Issues to consider include:[17]

(a) whether the entity retains the right or power to access, change or retrieve the information;

(b) who else will be able to access the information and for what purposes;

[15] APP Guidelines, Chapter B, paragraph B.81
[16] https://www.oaic.gov.au/privacy/privacy-decisions/investigation-reports/donateblood-com-au-data-breach-australian-red-cross-blood-service/
[17] APP Guidelines, Chapter B, paragraph B.144

(c) the security measures that will be used for the storage and management of the personal information;

(d) whether the information can be retrieved or permanently deleted by the entity when no longer required or at the end of the contract; and

(e) provisions in the contract which require any subcontractors to agree to the same obligations.

13.15 In our view, considering the guidance above, Epic and NTT should not be analysed as 'record keepers' under the Health Records Act even though they may have access to information in the DHR Solution for the purposes of providing support services, because ACT Health retains effective control of any personal information that Epic and NTT may have to provide their services.

Meaning of 'treating team' and 'episode of care'

13.16 As set out above, at section 7.5 of Part C, while all Clinicians in Health Services can access the DHR Solution and all Patients' DHR, as a matter of policy, only 'treating team' members should access a Patient's DHR (unless they are otherwise accessing a Patient's DHR for the purposes of the management, funding or quality of the relevant health service). This is an important concept for the purposes of the Health Records Act.

13.17 The Act sets out the circumstance where another person besides a Patient can access a health record. For example, this includes at HPP 6 where a health service provider who is a member of a treating team requires access to provide a health service to the Provider (this is discussed in more detail below in Part E).

13.18 A 'treating team' in relation to a Patient is defined in the Health Records Act as:

> 'health service providers involved in diagnosis, care or treatment for the purpose of improving or maintaining the consumer's health for a particular episode of care, and includes —
>
> a. if the consumer named another health service provider as his or her current treating practitioner—that other health service provider; and
>
> b. if another health service provider referred the consumer to the treating team for that episode of care—that other health service provider.'

In practice, a treating team can include current and referring Clinicians for a particular episode of care. For example, where a Patient nominates a GP on hospital admission, the GP is considered as a member of the treating team.

13.19 The phrase 'episode of care' is not defined in the Health Records Act. We note that it appears that the phrase is most commonly used in the context of admitted patient episodes of care in the context of hospital funding. For example, *Mosby's Dictionary of Medicine, Nursing & Health Professions* (revised third Australian and New Zealand Edition) provides the following definition for 'episode of hospital care' (there is no definition provided for 'episode of care' in this dictionary):

> 'the services provided by a hospital in the continuous course of care of a patient with a health condition. It may cover a sequence from emergency through inpatient to outpatient services'

13.20 The Australian Institute of Health Welfare appears to provide the following broad definition for 'episode of care': '*a period of health care with a defined start and end*'.[18] In the context of the Health Records Act, we take 'episode of care' to have a broad meaning which covers care for particular purpose or condition (for example, it can cover the spectrum from admission in a hospital following an accident, to screening services at walk-in-centre where results are potentially provided to a person's GP).

13.21 We note that by necessity, whether something forms part of a particular episode of care will be highly context dependent. We acknowledge that who forms part of a 'treating team' may change quickly as a Patient's needs change, for example where a matter has to be referred to a specialist within a hospital setting.

13.22 Generally, if a Clinician within a Health Service in providing a health service to a Patient reasonably believes they require access to a Patient's DHR, taking into account their professional obligations such as the *Good Medical Practice: A Code of Conduct for Doctors in Australia*,[19] it is likely that they would be able to satisfy the requirements relating to accessing information for the purposes of an episode of care.

Meaning of 'management, funding or quality of a health service received'

13.23 The Health Records Act also provides that:

> If a person reasonably requires access to personal health information about a consumer for the purpose of the management, funding or quality of a health service received, or being received, by the consumer, the person may have access to the extent necessary for that purpose without the consumer's consent.[20]

This means that the Health Records Act acknowledges that access to personal health information may be required by persons in circumstance other than providing a health service for a particular episode of care.

13.24 The phrase 'purpose of the management, funding or quality of a health service received' is not defined and is used in a number of the HPPs. In our view the phrase also can be interpreted broadly. Again, whether an activity falls within the meaning of the phrase will need to be determined on a case by case basis. Some examples of activities that may come within the phrase include:

13.24.1 reviewing a Patient's DHR to determine whether the Patient should be managed under a Clinician's speciality;

13.24.2 booking and scheduling of Patients;

13.24.3 triaging; and

13.24.4 ensuring proper functioning of the ICT systems supporting the health services, such as system administration functions and ICT support (but only to the extent that such activities require access to personal health information).

[18] https://meteor.aihw.gov.au/content/index.phtml/itemId/268978
[19] https://www.medicalboard.gov.au/Codes-Guidelines-Policies/Code-of-conduct.asp
[20] HPP 6.1 in the Health Records Act.

14. Sharing of patient medical records between CHS and third parties contracted to provide public health services in the Territory

14.1 We note that with the implementation of the DHR Solution, there will be in practical terms an ability for staff of third party entities contracted to provide public health services in the Territory (such as Calvary staff at the Bruce, ACT location or staff of the operator of the Tresillian Queen Elizabeth II Family Centre) to access information about a Territory Patient receiving Health Services (i.e. public health services), which was inputted by a member of staff of Canberra Health Services (and vice versa).

14.2 Health records have generally been considered to be 'owned' by the person or organisation that authored them, with persons to whom the record relates having a right of access to them. Indeed, the explanatory memorandum to the *Health Records (Privacy and Access) Bill 1997* provided that the intention of the Bill (now the Health Records Act) '*is to increase consumers' access to their own health information without unnecessary bureaucratic processes being put in place'.*[21]

14.3 We understand that the view that the Territory has previously taken is that access to Calvary Public Hospital Patient records is supported by a number of HPPs in the Health Records Act. For example, through consent of the consumer (HPP 10(2)(c)); reasonable expectation of the consumer (HPP 10(2)(b)); in appropriate cases where the disclosure of the information is necessary for the management, funding or quality of the health service received, or being received, by the consumer (HPP 10(2)(f)); or where the information is being shared between members of a treating team for the consumer only to the extent necessary to improve or maintain the consumer's health or manage a disability of the consumer (HPP 10(2)(a)). HPP 6 and 9 may also be relevant in circumstances.

14.4 We note that the Calvary Network Agreement, which sets out Calvary's obligations in relation to the provision of public hospital services at Calvary Public Hospital Bruce, provides at clause 36.1, in the context of intellectual property, that '*Ownership of all Health Records vests on its creation in Calvary'*. The remainder of clause 36 does not specifically give the Territory (or Canberra Health Services as part of the Territory) the right to use or access the health records created by Calvary in performing its public health services.

14.5 The DHR Solution will effectively be a shared infrastructure for Health Services, with different Clinicians across CHS and Calvary (and potentially other entities that are engaged to provide public health services in the Territory) providing input into a Patient's DHR depending on a particular health event or related to an episode of care. Documenting the intentions around the use of the DHR Solution may assist in clarifying the intended creation and use of health records in relation to public patients in the Territory.

14.6 In our view, it is reasonable that CHS staff and Calvary staff have the same level of access to a Patient's DHR for the purposes of providing public health services in the Territory (with User based permission controls depending on a staff member's role). This would seem to further the commitment reflected in Recital D of the Calvary Network Agreement that:

> *'The parties have a shared commitment to the delivery of high-quality public health services in the Territory and have agreed that Calvary will operate the Public Hospital as a Network Service Provider integrated into the Territory's public health system.'*

14.7 This is also reflected in the provisions in the body of the Calvary Network Agreement. Without the DHR Solution being able to be accessed consistently by CHS and Calvary Public, in our view, this integration is unlikely to be realised.

14.8 We also note that the Calvary Network Agreement does not provide a great amount of detail about the handling of personal information in delivering the public health services. For

[21] Explanatory Memorandum, https://www.legislation.act.gov.au/View/es/db_17070/19971113-19511/PDF/db_17070.PDF

example, it does not include a specific requirement for Calvary to comply with any CHS policies, and refers to outdated requirements (such as that 'each party must comply with the 'Information Privacy Principles' set out in the *Privacy Act 1988* (Cth) as if they were provisions of this Agreement' at clause 35.3 instead of the Information Privacy Act and the Health Records Act 1997).

14.9 We also note that CHS and Calvary are separate entities. When a User in CHS uploads information about a Patient to a Patient's DHR and that information is accessed by a User at Calvary, there will technically be a disclosure from CHS to Calvary in relation to that information (even though the same shared infrastructure the DHR Solution is being used by both entities).

14.10 To realise the benefits of the DHR Solution, in our view it would be beneficial for the Calvary Network Agreement to be updated to reflect the intended practices, or alternatively for the Calvary Network Agreement to be supplemented by agreed ancillary governance documents between Calvary and the Territory.

14.11 Although we have not reviewed agreements with other third party entities that have been engaged to provide public health services in the Territory, the principles above apply equally to the entry of Patient information by, and the disclosure of Patient information to, those other third party entities.

14.12 We therefore **recommend** that any contractual or other arrangement with another organisation to provide public health services in the Territory, where that other organisation will have access to, and use, the DHR Solution:

14.12.1 include a specific requirement to comply with any relevant policies, including those dealing with records and/or the handling of personal information;

14.12.2 include an express requirement to comply with the Health Records Act and the Information Privacy Act at all times in connection with the delivery of the public health services; and

14.12.3 provide clear rights and obligations in relation to the access and use of records when delivering the public health services**,** including the use of the DHR Solution

(**Recommendation 9**)

14.13 We suggest that this recommendation could be implemented through review and (if necessary) updating of existing contractual arrangements, or by supplementing those arrangements with ancillary governance documents.

14.14 We note that during stakeholder consultation, Calvary expressed the view that the current drafting of the Calvary Network Agreement remains appropriate, but that it is possible that 'Practice Notes' or a 'Partner Network Access Agreement' (similar to one developed for the sharing of pathology and imaging results) could be developed, and the relevant Patient consent forms reviewed and updated as appropriate. Calvary also stressed the importance of recording the location of the episode of care that the Patient is receiving, and how that information can be shared with the other party in the 'digital age'. We believe that having agreed ancillary governance documents would be consistent with **Recommendation 9**.

14.15 We note that as part of implementing **Recommendation 2**, any information or collection notice should clearly provide that information will be accessible to all providers of public health services within the Territory, noting that this would help support the view that Patients should reasonably expect this to occur.

14.16 We also make the **observation** that the Health Records Act may not now represent current medical practice and advances in technology, such as the ability to have a patient-centred electronic medical record. In our view, many of the HPPs are difficult to rationalise, particularly in situations where the TPPs still have some operation. The Territory may wish to consider, as part of its broader work, whether the implementation of the DHR Solution is an opportune time to review the Health Records Act, to assess whether it continues to meet the objectives for which it was enacted, particularly given the Information Privacy Act and the proposed review of the *Privacy Act 1988* (Cth).

15. Approach to undertaking our analysis

15.1 In undertaking our analysis, we have taken into account:

15.1.1 ACT Health's draft DHR principles – which articulate ACT Health's approach to decision making in relation to the implementation of the DHR Solution (including putting patients first; clinical quality and excellence, coordinated, patient centred care);

15.1.2 OAIC's *Guide to health privacy* – though this guidance is to assist health service providers understand their obligations under the *Privacy Act 1988* (Cth), it provides useful general guidance on how to embed good privacy practice in a health service setting;

15.1.3 current consumer views on privacy, for example, as set out in OAIC's *Australian Community Attitudes to Privacy Survey 2020*. Relevantly the Survey found:

> Australians trust health service providers the most with their personal information.[22]
>
> Over a third (36%) of Australians are comfortable with government agencies sharing their personal information with other Australian Government agencies, while 40% are uncomfortable with this. Australians are far less likely to be comfortable with government agencies sharing their personal information with businesses in Australia (15% comfortable, 70% uncomfortable) and businesses sharing their personal information with other Australian organisations (13% comfortable, 70% uncomfortable)
>
> Only a quarter (24%) of Australians feel the privacy of their personal information is well protected and 40% feel it is poorly protected
>
> The vast majority (83%) of Australians would like the government to do more to protect the privacy of their data[23]

15.2 As discussed above, both the HPPs and TPPs apply to the DHR Solution. However, at this initial stage of the project, the development of the DHR Solution is focussed on the development of the DHR Solution by Epic and significantly the establishment of Patient DHRs (which are heath records for the purposes of the Health Records Act) within the DHR Solution. In **Part E,** we have therefore focussed on ACT Health's compliance with the HPPs in relation the establishment of the DHR Solution and Patient DHRs in relation to these matters.

15.3 However, the TPPs will also apply to the handling of personal information in the DHR Solution to the extent it deals with personal information that is not personal health information. For example, the handling of external healthcare provider personal information for the purposes of registering access to the DHR Solution. Given that at this stage details of how this is to be managed is not yet determined, we have provided high level guidance to assist ACT Health ensure compliance with the TPPS in **Part F** to inform design of the DHR

[22] OAIC, Australian Community Attitudes to Privacy Survey 2020 infographic: https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/acaps-2020-infographic/
[23] OAIC, *Australian Community Attitudes to Privacy Survey 2020*, p 65

Solution, we note that as work progresses on the DHR Solution, compliance against the TPPs will need to be further considered.

15.4 We also consider that the TPPs cover important principles relevant from a whole of system perspective, in particular TPP 1. We consider that members of the public would generally expect the DHR Solution will be developed by ACT Health in a manner consistent with privacy best practice and be underpinned by principles which are designed to ensure that personal information is managed in accordance with best practice. We therefore consider the application of the TPPs at **Part F** from a principles based perspective to the DHR Solution as a whole.

Part E HEALTH RECORDS ACT PRIVACY PRINCIPLES COMPLIANCE

Set out below is our analysis of the HPPs as it relates to the 'health record' that is, the Patient DHR aspect of the DHR Solution.

1. HPP 1 – Manner and purpose of collection of personal health information

Text of HPP 1

Principle 1: Manner and purpose of collection of personal health information

1 A collector must not collect personal health information for inclusion in a health record or in a generally available publication unless—

(a) the information is collected for a lawful purpose that is directly related to a function or activity of the collector; and

(b) the collection of the information is necessary for or directly related to that purpose.

2 A collector must not collect personal health information by unlawful or unfair means.

3 Where personal health information or health records are required to be collected by someone as part of his or her employment for the management, funding or quality of a health service received by the consumer, then that person is allowed access to the information only for those purposes, unless these principles otherwise provide.

Analysis of compliance with HPP 1

1.1 HPP 1 provides that personal health information must only be collected for a lawful purpose that is directly related to, and necessary for, the collector's function or activity.

1.2 We note that HPP 1 has limited applicability to the implementation of the DHR Solution, because it relates to what is required at the time personal health information is collected for inclusion in a health record. This PIA does not consider the policies followed or processes used by administrative staff or Clinicians to collect personal health information from Patients for inclusion in a health record (e.g. what Patients are told at the time of collection). Such practices of Clinicians and other persons collecting personal health information will not be impacted by the implementation of the DHR Solution.

1.3 We do note that the data entry fields in screens that are displayed to Users who will be collecting Patient Information should only contain fields for pieces of Patient Information (administrative information or clinical information) that are necessary for, or directly related to, the provision of the relevant health services to the Patient. Similarly, fields that are displayed to Patients through the Patient Portal should also solicit Patient Information that is relevant for their care. We understand that this will be the case.

Medical Devices and Wearables

1.4 The DHR Solution will include collection of personal health information from medical devices (where the Patient is located on a Health Services site) and Wearables. In our view these collections are directly related to the function of the provision public health services by Health Services to a Patient, as information from these sources will inform decisions on the healthcare to be provided to Patients.

1.5 A collection of personal information is lawful if it is not contrary to law. Conversely, a means of collection will not be lawful if a law, legal order or legal principle prevents that means of collection. For example, a collection will be unlawful if it is:

1.5.1 in breach of legislation, such as computer hacking, using telephone interception or a listening device except under the authority of a warrant, or requesting or requiring information with, or for the purposes of, an act of discrimination;

1.5.2 by a means that would constitute a civil wrong, such as by trespassing on private property or threatening damage to a person unless information is provided; or

1.5.3 contrary to a court or tribunal order, such as an injunction issued against the collector.[24]

1.6 A "fair means" of collecting personal information is one that is not oppressive, does not involve intimidation or deception, and is not unreasonably intrusive. Whether a collection uses unfair means would depend on the circumstances.[25]

1.7 In our view, the collection of personal health information:

1.7.1 passively from medical devices would be fair and therefore compliant with HPP 1 if Patients are informed of this (see our discussion at HPP 2); and

1.7.2 from Wearables, where the Patient opts to link this to their Patient DHR, would be fair and compliant if Patients are notified about the collection and use of the information (see our discussion at HPP 2).

Individual Healthcare Identifier

1.8 We note for completeness that ACT Health also discussed the potential collection and use of the IHI as an identifier for the DHR Solution with us. The collection and use of the IHI is governed by the *Healthcare Identifiers Act 2010* (Cth) (**HI Act**). In our view, Health Services, as 'healthcare providers' as defined in the HI Act, are authorised by law to collect and use the IHI, including adopting the IHI as its own identifier.[26]

[24] APP Guidelines, Chapter 3, paragraphs 3.60 – 3.61.
[25] APP Guidelines, Chapter 3, paragraph 3.62 – 3.63. We note that HPP 1 (2) is relevant to the collection of clinical images, which we have discussed in our analysis of HPP 2 below.
[26] *Healthcare Identifiers Act 2010* (Cth), ss 14 and 16.

2. HPP 2 – Purpose of collection of personal health information to be made known

Text of HPP 2

Principle 2: Purpose of collection of personal health information to be made known

1. Subject to clause 2 of this principle, where—

   (a) a collector collects personal health information for inclusion in a health record or in a generally available publication; and

   (b) the information is solicited by the collector from the consumer concerned;

   the collector must take such steps (if any) as are reasonable in the circumstances to ensure that, before the information is collected or, if that is not practicable, as soon as practicable after the information is collected, the consumer is generally aware of—

   (c) the purpose for which the information is being collected; and

   (d) if the collection of the information is required or authorised by law—the fact that the collection of the information is so required or authorised; and

   (e) unless it is obvious from the circumstances of any health service provided—the identity of all members of the treating team who will have access to the consumer's personal health information; and

   (f) the identity of any person to whom, or agency to which, the collector would, in accordance with the collector's usual practice, disclose the information for inclusion in a health record or in a generally available publication; and

   (g) if it is, to the knowledge of the collector, the usual practice of any such person or agency to pass on such information to other persons or agencies—the identity of each of those other persons or agencies.

2. The collector is not required to notify the consumer of the identity of individuals, or classes of individuals, who are employed by the collector and who are required for the management, funding or quality of the health service received by the consumer to handle health records or personal health information as part of their employment.

Analysis of compliance with HPP 2

2.1 HPP 2 provides that the collector must take reasonable steps to ensure that the consumer knows why the information is being collected, who will have access to it, and if relevant, that collection of the information is required or authorised by law.

2.2 Similarly to HPP 1, HPP 2 has limited applicability to the implementation of the DHR Solution as it relates to what is required to be made known to a consumer (i.e. Patient) at the time personal health information is collected for inclusion in a health record, or as soon as practicable after. Again, the usual practice of Clinicians and other persons collecting personal health information will not be impacted by the implementation of the DHR Solution.

Medical Devices and Wearables

2.3 As discussed at HPP 1, the DHR Solution will include collection of personal health information from medical devices (where the Patient is located on a Health Services site) and Wearables. We note that HPP 2 deals with information that is 'solicited' by ACT Health.

2.4 The OAIC's guidance is that an entity 'solicits' personal information where it 'requests' the information. A 'request' is an active step taken by an entity to collect personal information, and may not involve direct communication between the entity and an individual.[27]

[27] APP Guidelines, Chapter B, at 3.6

2.5 In our view, it is relatively clear that the passive collection of information from the medical devices is solicitation of the information from ACT Health. We also consider the functionality of being able to 'link' a Wearable to a Patient's DHR also amounts to solicitation of that information by ACT Health. While we understand that the Patient will need to consent to linking their Wearable and take active steps to do so, the offering of the functionality in our view amounts to 'soliciting' the information.

2.6 In order to meet HPP 2, Patients need be made aware that their personal health information has been collected through these means.

2.7 We understand that currently, when a medical device is attached to a Patient within a Health Service and any readings are recorded in handwritten clinical notes, the Patient is not expressly told that their personal health information from such a medical device is being collected (though they would be aware in the context this is happening). With the passive collection of personal health information from medical devices into a Patient's DHR, there is a risk that persons may not be aware that such information is being collected. In our view if **Recommendation 2** (as discussed under TPP 1) is implemented, this would assist in addressing this risk.

2.8 For Wearables, Patients will need to be informed about the collection of their personal health information at the time they link the Wearable to the DHR Solution.

2.9 We **recommend** that consideration be given to ensuring that either:

2.9.1 the DHR Solution will give a notice to the Patient before their Wearable is linked to the DHR Solution and their Patient Information is uploaded; or

2.9.2 ACT Health implements policies and procedures so that it is satisfied that the provider of the Wearable will issue such a notice before the linking occurs.

2.10 The notice should explain to Patients that linking will cause their personal health information to be collected by ACT Health and stored in their Patient DHR, and be accessible to ACT Health staff who provide health services to the Patient (**Recommendation 4**).

Clinical photographs

2.11 We note that ACT Health raised with us the specific issue of photographs that may be taken at a Health Service (for example through a smartphone or tablet) and the inclusion of the image on a Patient's DHR and to what extent consent is required for the taking and storing of the image on the DHR Solution. In our view such images would be 'personal health information' within the meaning of the Health Records Act as they would be linked to a Patient's DHR, persons would be readily identifiable. We set out below our consideration on the issue.

2.12 OAIC provides guidance on the obligations of health service providers when taking photos of patients.[28] While OAIC's guidance is in the context of the *Privacy Act 1988* (Cth) it does provide important relevant points to note and consider in the context of the DHR Solution.

2.13 The OAIC considers that a health service provider will usually need to ensure that they have the appropriate consent to collect, use and/or disclose a photographs of a Patient's injury or visible illness. There may be exceptions, such as it is unreasonable or impracticable to obtain the individual's consent to the collection, use or disclosure; and the agency reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of an individual, or to public health or safety.

2.14 The OAIC Guide to Health Privacy provides, at Chapter 2, a health service provider may collect health information about a patient, if:

[28] https://www.oaic.gov.au/privacy/privacy-for-health-service-providers/taking-photos-of-patients/

2.14.1 the patient consents (expressly or impliedly) to a health service provider collecting it; and

2.14.2 the information is reasonably necessary for the activities (which would generally be providing a health service to that patient).

2.15 The Australian Medical Association (**AMA**) has also prepared a guide to 'clinical images and the use of personal mobile devices' which sets out a decision making process for collecting, using and storing clinical images and which we consider to be best practice approach to the dealing with the taking of photographs in a health service setting.[29]

2.16 In summary, applying the AMA guidance:

2.16.1 Patients have the right to consent (or refuse), the collection, use and disclosure of clinical images.

2.16.2 Only Patients with capacity can provide valid consent, however, where a Patient lacks decision-making capacity, consent should be sought from a Patient's authorised guardian.

2.16.3 Clinicians should discuss with their patients the following information to ensure the patient can provide fully informed consent:

(a) the purpose(s) of the clinical image i.e. why the clinical image is being taken;

(b) how the clinical image may be used (e.g. a Patient's images will be included in the Patient's DHR);

(c) who will have access to the image (i.e. ACT Health and potentially external health care providers if the Patient agrees);

(d) whether it might be shared and disclosed to other, and for what purposes;

(e) whether it will be de-identified (which is not relevant for the DHR); and

(f) how and where it will be stored.

2.17 The AMA notes that many hospitals and health departments have implemented clinical image policies, but there is evidence that not all doctors are aware of or follow these policies. While we are not aware of any such policy applying in the ACT Health, we consider that the design of the DHR Solution could assist persons to comply with HPP 2.

2.18 We therefore **recommend** ACT Health consider, as an assurance measure that HPP 2 is being complied with, the DHR Solution include a prompt when images are uploaded to the DHR that the uploader acknowledges that the person has given consent to the image being taken and has been informed of how it may be used and stored (**Recommendation 5**). This will also assist in ensuring compliance with HPP 1.2.

[29] https://ama.com.au/sites/default/files/1/FINAL_AMA_Clinical_Images_Guide.pdf

3. HPP 3 – Solicitation of personal health information generally

Text of HPP 3

Principle 3 Solicitation of personal health information generally

Where—

(a) a collector collects personal health information about a consumer for inclusion in a record or in a generally available publication; and

(b) the information is solicited by the collector;

the collector must take such steps (if any) as are reasonable in the circumstances to ensure that, having regard to the purpose for which the information is collected—

(c) the information is relevant, up to date and accurate; and

(d) the collection of the information does not intrude to an unreasonable extent upon the personal affairs of the consumer.

Analysis of compliance with HPP 3

3.1 HPP 3 provides that the collector must take reasonable steps to ensure that the information collected is relevant, up to date and accurate. Requests for information should not be unreasonably intrusive.

3.2 Similarly, to HPP 1 and HPP 2, HPP 3 has limited applicability to the implementation of the DHR Solution as it relates to what is required at the time of collection. The relevant policies and the usual practices of Clinicians and other persons collecting personal health information will not be impacted by the implementation of the DHR Solution.

3.3 We do not consider that additional steps are required to ensure compliance with HPP 3.

4. HPP 4.1 – Storage, security and destruction of personal health information—safekeeping requirement

Text of HPP 4.1

Principle 4.1 — Storage, security and destruction of personal health information—safekeeping requirement

1. A record keeper who has possession or control of a health record must ensure that—
   (a) the record is protected, by reasonable security safeguards, against each of the following:
      (i) loss;
      (ii) unauthorised access, use, modification or disclosure;
      (iii) other misuse; and
   (b) if the record is given to another entity—everything reasonably within the power of the record keeper is done to prevent unauthorised use or disclosure of any information contained in the record.
2. A record keeper must keep, and must not destroy, a health record about a consumer, even if it is later found or claimed to be inaccurate.
3. However, clause 2 does not apply to the destruction of a health record about a consumer if—
   (a) the destruction is required or allowed under a law of the Territory; or
      Note Law of the Territory—see dict.
   (b) the destruction is not prohibited under any other law and happens after—
      (i) if the consumer is under 18 years old when the information is collected—the day the consumer turns 25 years old; or
      (ii) if the consumer is an adult when the information is collected—7 years after the day a service was last provided to the consumer by the record keeper; or
   (c) an electronic copy of the record has been generated—
      (i) by a method described in the Electronic Transactions Act 2001, section 11 (2) (b); and
      (ii) when the record is destroyed it is reasonable to expect that the information contained in the electronic copy will be readily accessible so as to be useable for subsequent reference.

Analysis of compliance with HPP 4.1

4.1 HPP 4.1 provides that a record keeper, such as ACT Health, must keep health records secure and that a record keeper must not destroy a health record unless:

4.1.1 required or allowed by law; or

4.1.2 an electronic copy remains available after destruction of the record.

4.2 For an adult consumer, destruction of a health record may occur seven years after the service was last provided. For a consumer aged under 18 years at the time the service was last provided, destruction of a health record may occur when the consumer turns 25 years of age.

4.3 Significantly, HPP 4.1 deals with the security of a health record and requires ACT Health to have reasonable security safeguards in place to protect from relevantly "unauthorised access" and "misuse".

4.4 The term "reasonable" is not defined in the Health Records Act, but the APP Guidelines provides some guidance which in our opinion is useful in this context. OAIC provides that the term "reasonable" bears its ordinary meaning, as being based upon or according to reason and capable of sound explanation.[30] What is reasonable can be influenced by current

[30] APP Guidelines, Chapter B, paragraph B.105.

standards and practices.[31] The APP Guidelines provide 'that it is the responsibility of an entity to be able to justify that reasonable steps were taken.'[32]

4.5 In considering what reasonable steps ACT Health can take to mitigate this risk, we believe it important to take into account and balance the following:

4.5.1 a Patient's expectation that ACT Health will take reasonable steps to ensure their personal health information will not be misused;

4.5.2 the seriousness of any consequence that may flow if there is misuse of Patient Information (noting that this will depend on the circumstances); and

4.5.3 the practical consequences for the efficient and effective delivery of health services.

4.6 The contract with Epic for the DHR Solution includes a number of important security requirements in relation to the design of the DHR Solution. We also note that there are security features that will be in place which will log a User's access to a Patient's DHR, and policies will be in place about when a person should access a record. We see these as reasonable security safeguards to protect the personal health information in a Patient's DHR.

4.7 However, we note the current design of the DHR Solution is such that all Clinicians in the Health Services will be able to access all personal health information in a DHR Solution (and other persons depending on their role) even where they are not a treating team member. We also note that this issue was of particular concern to consumers. We appreciate that this may be necessary from an operational perspective (members of the treating team may change rapidly, or the Patient may present at different Health Service sites). We note that the workflow system will have an "In Basket" which will only include the Patients who have been allocated to that Clinician. If the Clinician needs to they can search for a Patient outside of this "In Basket". However, the DHR Solution, including the "In Basket" feature, will not prevent a Clinician accessing information about a Patient who is not in their "In Basket".

4.8 Therefore, there remains a potential privacy risk associated with allowing wide-spread access that a Patient's DHR may be inappropriately accessed by persons who, although authorised to access the DHR Solution, do not have an appropriate need or reason for accessing a particular Patient's DHR. This risk of unauthorised access increases the risk for potential misuse of a Patient's DHR (for example, a User accessing the DHR Solution to obtain contact details or other information about a former partner).

4.9 While we acknowledge that Users who are employees of, or contracted to, Health Services will be bound by relevant policies, directions, procedures, and potentially professional obligations, that prohibit such misuse, we **recommend** that ACT Health give further consideration to whether it is feasible to implement additional technical measures for the DHR Solution, in addition to the current strategies of requiring compliance with policies and procedures, to mitigate the risk of Users accessing a Patient's DHR where they have no business need to do so. For example, measures that could be considered might include:

4.9.1 the DHR Solution's capabilities being used to identify any unusual or unexpected access to a Patient's DHR (for example, if a User accessed a Patient's DHR where that person had not recently interacted with a Health Service);

4.9.2 the DHR Solution including a mechanism for a Clinician who is a User to be advised that they need to be a member of the relevant Patient's treating team before being able to access a Patient's DHR (or perhaps the Clinician could be required to confirm this) – noting that the benefits of this privacy protection would need to be balanced against any operational inconvenience for Clinicians; and/or

[31] *Bankstown Foundry Pty Ltd v Braistina* [1986] HCA 20 (Mason, Wilson and Dawson JJ at paragraph 12).
[32] APP Guidelines, Chapter B, paragraph B.106.

4.9.3 DHR Solution screens that allow Users to search for a Patient's DHR, could include a prominently displayed statement that '*Persons are only authorised to access a record where they have a business need to do so. Your access will be logged and is auditable*'.

4.10 We acknowledge that it is difficult to quantify the magnitude of the risk of access for improper purposes, and that technical features to address the potential risk may not be necessary if proper training is provided to Users and routine auditing of access to the DHR Solution is undertaken. Therefore, if the above recommendations for technical measures is not practical, we **recommend**, as an alternative privacy enhancing feature, ACT Health ensure that the training provided to Users before access is granted to the DHR Solution includes training on their privacy obligations, including when they may or may not use or disclose Patient Information (**Recommendation 3**).

5. HPP 4.2 – Storage, security and destruction of personal health information—register of destroyed or transferred records

Text of HPP 4.2

Principle 4.2 — Storage, security and destruction of personal health information—register of destroyed or transferred records

1. A record keeper must keep a register of records that have been destroyed or transferred to another entity.

2. The register must identify the following for records that have been destroyed or transferred:

   (a) the consumer to whom the record relates;
   (b) the period of time the record covers;
   (c) for a destroyed record—the date the record was destroyed;
   (d) for a transferred record—the entity to which the record has been transferred.

3. A record keeper need not keep a record on the register under clause 1 for longer than 7 years after the day the record is made.

Analysis of compliance with HPP 4.2

5.1 HPP 4.2 provides that the record keeper, such as ACT Health, must keep a register of records that have been destroyed or transferred to another entity for seven years after the day the record is made.

5.2 We **recommend** that ACT Health confirm that the design specifications for the DHR Solution contain functionality that meets HPP 4.2, that is, includes the maintenance of a register of records that have been destroyed or transferred (**Recommendation 6**).

6. HPP 4.3 – Storage, security and destruction of personal health information—destruction of health information

Text of HPP 4.3

Principle 4.3 — Storage, security and destruction of personal health information—destruction of health information

1. Health information may be kept by a health service provider if it is needed for the purpose for which it was collected, or another purpose allowed under a law of the Territory, even if its destruction is allowed under principle 4.1.

2. An entity other than a health service provider must take reasonable steps to destroy, or permanently deidentify, health information if it is no longer needed for the purpose for which it was collected or for any other purpose allowed under a law of the Territory.

Analysis of compliance with HPP 4.3

6.1 HPP 4.3 provides that a health service provider may keep personal health information for longer than specified in HPP 4.1, if needed for the purpose for which it was collected or for another lawful purpose. A record keeper other than a health service provider must destroy health information if it is no longer needed for the purpose for which it was collected.

6.2 The DHR Solution does not impact on current practices of Health Services relating to the destruction of records, but we **recommend** that ACT Health confirm that the design specifications for the DHR Solution contain functionality that meets HPP 4.3, that is, will allow Health Services to destroy or de-identify a Patient's DHR if it is no longer needed (**Recommendation 6**).

7. HPP 5 – Information relating to records kept by record keeper

Text of HPP 5

Principle 5 - Information relating to records kept by record keeper

1. A record keeper who has possession or control of health records must, subject to clause 2 of this principle, take such steps as are reasonable in the circumstances to enable any consumer to ascertain—
    (a) whether the record keeper has possession or control of any health records, or personal health information, relating to the consumer; and
    (b) if so—
        (i) the nature of the records or information; and
        (ii) the main purposes for which the records are, or the information is, used; and
        (iii) the steps that the person should take if the person wishes to obtain access to the records or the information.
2. A record keeper is not required to give a person information if, under a law of the Territory (including this Act) or a law of the Commonwealth, the record keeper is required or authorised to refuse to give that information to the person.

Analysis of compliance with HPP 5

7.1 HPP 5 provides that a record keeper must take reasonable steps to enable a consumer (in this case, a Patient) to know whether the record keeper holds health records or personal health information in relation to the consumer and how the consumer can access the records or the information.

7.2 We note that ACT Health makes available on its website information about how persons can access their records. These processes will continue with the implementation of the DHR Solution. In addition, the implementation of the Patient Portal can be characterised as a privacy enhancing feature as another means for persons to access their own records and further enhance compliance with HPP 5. We note that implementation of **Recommendation 2** would further enhance compliance with HPP 5.

8. HPP 6 – Access to health records by people other than the consumer

Text of HPP 6

Principle 6— Access to health records by people other than the consumer

1. A health service provider who is a member of a treating team for a consumer may have access to the personal health information about the consumer so far as necessary for the provision by the provider of a health service to the consumer.
2. If a person reasonably requires access to personal health information about a consumer for the purpose of the management, funding or quality of a health service received, or being received, by the consumer, the person may have access to the extent necessary for that purpose without the consumer's consent.
3. A treating health service provider for a consumer may disclose personal health information about the consumer to an immediate family member if—
   (a) the disclosure is made for compassionate reasons; and
   (b) the provider believes, on reasonable grounds, that the disclosure would be expected by the consumer; and
   (c) the disclosure is not contrary to any wishes previously expressed by the consumer that the provider is, or ought reasonably to be, aware of. Note Section 17 deals with information subject to confidentiality.
4. An entity must not require a consumer, directly or indirectly, to obtain or grant access to a health record about the consumer unless the entity is required or allowed to make the requirement under—
   (a) a law of the Territory; or
   (b) a law of the Commonwealth; or
   (c) an order of a court.

Analysis of compliance with HPP 6

8.1 HPP 6 provides that a Clinician who is a member of a treating team for the Patient may have access to Patient Information.

8.2 Additionally, a Clinician may disclose the Patient's Information to immediate family members if:

8.2.1 the disclosure is made for compassionate reasons;

8.2.2 the disclosure would be expected by the Patient; and

8.2.3 the disclosure is not contrary to any wishes previously expressed by the Patient that the Clinicians is, or should reasonably be, aware of.

8.3 In our view, the DRH Solution does not impact on current policies and processes that are used by Health Services to address HPP 6, as the DHR Solution provides access to a Patient's DHR to Clinicians in a treating team, and the matters in HPP 6.2 to HPP 6.4 are business as usual processes that will be implemented using the DHR Solution.

8.4 However, as discussed in relation to HPP 4.1, we have highlighted a potential risk of unauthorised access by Clinicians who are not treating team members. We note that consumers were also particularly concerned with this and sought to understand the sanctions that would apply to Clinicians that inappropriately accessed a Patient's DHR.

8.5 The inappropriate access to medical records by a Clinician is a risk that currently exists (though we acknowledged that the DHR Solution may make it easier for a Clinician to do so), accordingly the sanctions that can apply currently will continue to apply with the implementation of the DHR Solution. We understand this could cover disciplinary action by a

Health Service for the Clinician's failure to abide by policies, and could potentially impact on a Clinician's registration if they are referred to the relevant health practitioner national board and the Clinician's conduct is found to be inappropriate. We note that the Health Services Commissioner in the Territory works with the national boards to consider complaints about registered health practitioners. In addition, the Health Services Commissioner can investigate the role of a Health Service and ACT Health where there has been inappropriate access to a Patient's DHR (that is, potential breach of the Health Records Act).

8.6 In our view, implementing **Recommendation 3** will further strengthen compliance with this HPP and assist in addressing consumer concerns.

9. Principle 7 – Alteration of Health Records

Text of HPP 7

Principle 7—Alteration of Health Records

1. A person must not delete information from a health record, even where it is later found or claimed to be inaccurate, unless the deletion is part of a program of archival destruction.

2. A record keeper who has possession or control of a health record must take such steps, by way of making appropriate corrections and additions as are reasonable in the circumstances, to ensure that the record is—

   (a) up to date and accurate; and

   (b) relevant to the purpose for which the information was collected or is to be used and to any other purpose that is directly related to that purpose

3. Where—

   (a) the record keeper of a health record is not willing to amend that record, by making a correction or an addition, in accordance with a request by the consumer concerned; and

   (b) no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request is pending, or has been made, under a law of the Territory (including this Act) or a law of the Commonwealth;

   the record keeper must, if the consumer gives to the record keeper a written statement concerning the requested correction or addition, take such steps as are reasonable in the circumstances to include the statement in the record.

4. Where the record keeper accepts the need to amend the health record but—

   (a) the record keeper considers it likely that leaving incorrect information on a health record, even if corrected, could cause harm to the consumer or result in incorrect health care treatment or assistance being provided; or

   (b) the form in which the record is held makes correction impossible; or

   (c) the corrections required are sufficiently complex or numerous for a real possibility of confusion or error to arise in relation to interpreting or reading the record if it were to be so amended;

   the record keeper must place the incorrect information on a record which is not generally available to the consumer's treating practitioner or treating team, and to which access is restricted, and take such steps as are reasonable in the circumstances to ensure that only the corrected copy is generally available to the practitioner or treating team.

Analysis of compliance with HPP 7

9.1 HPP 7 provides that information must not be deleted from a health record, even where it is later found or claimed to be inaccurate. A record keeper should make appropriate corrections and amendments to a record to keep it up to date and relevant. A consumer can request that a record be amended.

9.2 If the record keeper is not willing to amend the record in accordance with a request, the consumer can give the record keeper a written statement to be included in the record. If the record keeper is willing to amend the record in accordance with a request but holds a concern that the incorrect information could cause adverse consequences, the record keeper can place the incorrect information on a separate record that is not generally accessible.

9.3 We note that in designing the DHR Solution, the system will need to be able to deal with alterations to the DHR as set out under this HPP. We **recommend** that ACT Health confirm that the design specifications for the DHR Solution contain functionality to deal with alterations in the manner as set out in HPP 7 (**Recommendation 6**).

10. Principle 8 – Record keeper to check accuracy etc of personal health information before use etc

Text of HPP 8

Principle 8— Record keeper to check accuracy etc of personal health information before use etc

1. A record keeper who has possession or control of a health record must not use personal health information in that record without taking such steps (if any) as are reasonable in the circumstances to ensure that, having regard to the purpose for which the information is proposed to be used, the information is up to date and accurate.
2. Where a person gives information in confidence to a health service provider about a consumer, the provider must—
    (a) encourage the person to waive the requirement of confidentiality; and
    (b) if the information remains confidential—
        (i) record the information only if it is likely to assist in the treatment or care of the consumer; and
        (ii) take such steps (if any) as are reasonable in the circumstances to ensure that the information is accurate and not misleading.

Analysis of compliance with HPP 8

10.1 Record keepers must not use Patient Information without taking reasonable steps to ensure that the information in the record is up to date and accurate. If a person gives information in confidence to a Clinician about a Patient, the Clinician should encourage the person to waive the requirement of confidentiality. If the information remains confidential, the Clinician should only record the information if it is likely to assist in the treatment of the Patient, and take reasonable steps to ensure that the confidential information is accurate and not misleading.

10.2 We note that the usual practices of Clinicians to meet HPP 8 will able to be followed after implementation of DHR Solution. In particular, we understand that the DHR Solution has the functionality for Clinicians to mark certain information as confidential, which means that it can only be accessed if the 'Break the Glass' functionality in the DHR Solution is used by a User (we understand this to mean that the DHR Solution will display a notice to the Clinician, which must be actioned by the Clinician by confirming that they are properly authorised and need to access that information, with this action being logged and auditable). We see this as a measure that further strengthens compliance with HPP 8. We also note that the 'Break the Glass' feature would assist in addressing the concerns raised by consumers that sensitive records, such as mental health history, are not readily accessible when information in those records is not relevant to the Clinician providing a particular health service.

11. HPP 9 – Limits on use of personal health information

Text of HPP 9

Principle 9 — Limits on use of personal health information

1. Except where personal health information is being shared between members of a treating team to the extent necessary to improve or maintain the consumer's health or to manage a disability of the consumer, a record keeper who has possession or control of a health record that was obtained for a particular purpose must not use the information for any other purpose unless—
   - (a) the consumer has consented to use of the information for that other purpose; or
   - (b) the record keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a significant risk to the life or physical, mental or emotional health of the consumer or another person; or
   - (c) use of the information for that other purpose is required or authorised by—
     - (i) a law of the Territory; or
     - (ii) a law of the Commonwealth; or
     - (iii) an order of a court of competent jurisdiction;
   - (d) the purpose for which the information is used is directly related to the purpose for which the information was obtained; or
   - (e) the use of the information is related to the management, funding or quality of the health service received by the consumer.
2. In relation to the sharing of information among a treating team, unless it is obvious from the circumstances or context of the health service, the person in charge of the treating team must inform the consumer of the identity of all members of the treating team who will have access to the consumer's personal health information.
3. The treating team leader is not required to notify the consumer of the identity of individuals, or of classes of individuals, who are required for the management, funding or quality of the health service received by the consumer to handle health records or personal health information.

Analysis of compliance with HPP 9

11.1 HPP 9 provides that except where information in a health record is shared among members of a treating team for treatment purposes, a record keeper must not use the information for any other purpose unless:

11.1.1 the Patient has consented to its use for another purpose; or

11.1.2 the use is necessary to prevent or lessen a significant risk to life or health of a person; or

11.1.3 the use is required or authorised by law; or

11.1.4 the information is for the purpose of managing, funding or assessing the quality of the health service provided.

11.2 A "treating team" includes the current and referring health service providers for a particular episode of care. For example, if a consumer when admitted to hospital nominates a particular GP, the GP is to be considered as a member of the treating team. If it is not obvious from the circumstances, the consumer must be informed about who is included in the treating team.

11.3 We note that the usual practices of Clinicians and other Users designed to meet HPP 9 will not be impacted by the implementation of DHR Solution. We do not consider that any of the disclosures discussed in section 10 in **Part C** are likely to represent non-compliance with HPP 9 if the usual ACT Health policies and procedures are followed.

11.4 We understand that a Clinician may use the information in the DHR Solution to run reports to assist with clinical management of a Patient. For example, a report on all persons with a particular condition to assist the Clinician to consider what may be done for a particular Patient would, in our view, meet HPP 9.1(e) above, as is reasonable to conclude that it is treated to the 'quality of the health service' a Patient receives, as there will be a link between the use of the information about other Patients and the provision of the services to the first Patient.

11.5 We also note that Clinicians may use the DHR Solution to identify potential research participants (though any actual research will be subject to relevant research and ethics approvals). In our view there is an argument that this 'use' could also similarly fall within HPP 9.1(e). However, from a best practice privacy perspective, persons should be given the option not to be included in any such list of potential candidates. We therefore **recommend** that Patients are given the option, at the very least, to 'opt-out' of their Patient DHR being used for the purposes of identifying potential candidates for participation in approved research projects. Where a Patient opts-out, the DHR Solution should not include them in any lists identifying them as potential candidates for research (**Recommendation 8**).

11.6 We note for completeness, that consumers thought it important that Patients be able to consider whether to participate in research on a case-by-case basis. We note that this issue is broader than the implementation of the DHR Solution, and goes to the processes used to assess research proposals and how such research is conducted. We note that if a Patient decides not to opt-out of their Patient DHR being used to identify potential candidates for research (and therefore may be included in a list of potential candidates), the conduct of any research and what informed consent is required for that research project will continue to be subject to relevant research and ethics approvals.

11.7 We understand that as part of implementing the DHR Solution, training will be provided to Users, including Clinicians. In our view, if the training included reminders to Clinicians of their privacy obligations under the Health Records Act, this would also strengthen compliance with HPP 9 (see the alternative recommendation in **Recommendation 3**).

12. HPP 10 – Limits on disclosure of personal health information

Text of HPP 10

Principle 10— Limits on disclosure of personal health information

1. A record keeper who has possession or control of a health record must not disclose personal health information about a consumer from the record to an entity other than the consumer.

2. Clause 1 does not apply to the disclosure of personal health information about a consumer to an entity if—

   (a) the information is being shared between members of a treating team for the consumer only to the extent necessary to improve or maintain the consumer's health or manage a disability of the consumer; or

   (b) the consumer is reasonably likely to have been aware, or to have been made aware under principle 2, that information of the kind disclosed is usually disclosed to the entity; or

   (c) the consumer has consented to the disclosure; or

   (d) the record keeper believes, on reasonable grounds, that the disclosure is necessary to prevent or lessen a serious and imminent risk to the life or physical, mental or emotional health of the consumer or someone else; or

   (e) the disclosure is required or allowed under—

      (i) a law of the Territory (including this Act); or Note Disclosure is allowed under cl 8, cl 9 and cl 10.
      (ii) a law of the Commonwealth; or
      (iii) an order of a court; or

   (f) the disclosure of the information is necessary for the management, funding or quality of the health service received, or being received, by the consumer.

3. Clause 1 also does not apply to the disclosure of personal health information about a consumer to an entity if—

   (a) the disclosure is necessary for the purpose of research or the compilation or analysis of statistics, in the public interest; and

   (b) it is impracticable to seek the consumer's consent before disclosure; and

   (c) the purpose mentioned in paragraph (a) cannot be achieved by the disclosure of information that does not identify the consumer and from which the consumer's identity cannot reasonably be worked out; and

   (d) the entity is required for any disclosed information (identifiable information) that identifies the consumer, or from which the consumer's identity can be reasonably worked out—

      (i) to provide protection that is at least equal to that of this Act and that prevents any further disclosure of it; and

      (ii) to take reasonable steps to deidentify the information and destroy identifiable information at the earliest possible opportunity; and

      (iii) to ensure that identifiable information is not made publicly available.

   (e) the disclosure is in accordance with guidelines prescribed by regulation for this clause; and

   (f) the record keeper believes, on reasonable grounds, that the recipient of the health information will not disclose the personal health information.

4. Clause 1 also does not apply to the disclosure of personal health information about a consumer to the consumer's carer if—

   (a) the consumer cannot give or withhold consent to the disclosure, whether or not because the consumer is a—

      (i) child or a young person who does not have sufficient maturity and developmental capacity to understand the nature of the young person's request to access a health record and the nature of the record; or

(ii) legally incompetent person; and

(iii) in the record keeper's opinion, the disclosure is necessary to enable the carer to safely and effectively provide appropriate services to, or care for, the consumer.

5. In relation to the sharing of information among the treating team under clause 2 (a), unless it is obvious from the circumstances and context of the health service, the person in charge of the treating team must tell the consumer about the identity of each member of the treating team who will have access to the personal health information about the consumer.

6. However, the treating team leader need not tell the consumer about the identity of individuals who are required to handle health records, or personal health information about the consumer, for the management, funding or quality of the health service received, or being received, by the consumer.

7. A consent given by a consumer for clause 2 (c) must—

(a) be in writing and signed—

(i) if the consumer is a child or a young person who does not have sufficient maturity and developmental capacity to understand the nature of the young person's request to access a health record and the nature of the record—by a person with parental responsibility for the consumer; or

(ii) if the consumer is a legally incompetent person—by a guardian of the consumer; or

(iii) in any other case—by the consumer; and

(b) name the health service provider who made the record.

8. An entity to which information is disclosed under clause 2, clause 3 or clause 4 must not use or disclose the information for a purpose other than the purpose for which the information was given to the entity.

9. If there is an emergency and a consumer cannot give or withhold consent to the disclosure of personal health information about the consumer, the treating health service provider may discuss relevant personal health information with an immediate family member of the consumer to the extent reasonable and necessary for the proper treatment of the consumer.

10. A treating health service provider for a consumer may disclose personal health information about the consumer to the consumer's carer if—

(a) the consumer cannot give or withhold consent to the disclosure, whether or not because the consumer is a child, young person who does not have sufficient maturity and developmental capacity to understand the nature of the young person's request to access the health record and the nature of the record or legally incompetent person; and

(b) in the provider's opinion, the disclosure is necessary to enable the carer to safely and effectively provide appropriate services to, or care for, the consumer.

11. A treating health service provider for a consumer may disclose personal health information about the consumer to an immediate family member if—

(a) the consumer cannot give or withhold consent to the disclosure, whether or not because the consumer is—

(i) a child or a young person who does not have sufficient maturity and developmental capacity to understand the nature of the young person's request to access the health record and the nature of the record; or

(ii) a legally incompetent person; and

(b) disclosure is made for compassionate reasons; and

(c) the provider believes, on reasonable grounds, that the disclosure would be, or would have been, expected by the consumer; and

(d) the disclosure is not contrary to any wishes previously expressed by the consumer of which the provider is aware or ought reasonably to be aware.

12. In this principle:
carer, of a consumer, means a person who gives care, support or assistance to the consumer but does not include—

(a) a person who gives short-term care, support or assistance to the consumer; or

(b) a person who gives care, support or assistance to the consumer—

(i) under a commercial arrangement, or an arrangement that is substantially commercial; or
(ii) in the course of doing voluntary work for a charitable, welfare or community organisation; or
(iii) as part of a course of education or training; or

(c) a person just because the person—
(i) is the domestic partner, parent, child or other relative, or guardian of the consumer; or
(ii) lives with the consumer

Analysis of compliance with HPP 10

12.1 Generally, information in a health record can only be disclosed to a person other than the Patient with the written consent of the Patient. However, there are exceptions such as where:

12.1.1 the information is being shared between members of a Patient's treating team and is necessary for the treatment of the Patient;

12.1.2 the Patient is aware that this type of information is usually disclosed to a particular person or organisation;

12.1.3 the disclosure is necessary to prevent or lessen a serious and imminent risk to the life or health of a person;

12.1.4 the disclosure is required or authorised by law;

12.1.5 the disclosure is necessary for the purpose of managing, funding or assessing the quality of the health services provided;

12.1.6 the information is necessary for research purposes in the public interest;

12.1.7 the disclosure is to a Carer and the information is necessary to enable the Carer to safely and effectively provide appropriate care for the Patient;

12.1.8 it is an emergency and an immediate family member needs to be consulted in order to provide a service; or

12.1.9 the disclosure is to an immediate family member, where that disclosure is made for compassionate reasons, is a disclosure that would be expected by the Patient, and is not contrary to previously expressed wishes of the Patient.

12.2 In our view disclosures from the DHR Solution:

12.2.1 to a Patient – is supported under HPP 10.1;

12.2.2 to a Carer through the Patient Portal – is supported under HPP 10.4;

12.2.3 to external health care providers (including those engaged to support the relevant Health Service) – is supported under HPP 10.2(a); and

12.2.4 to My Health Record – is supported by HPP 10.2(e) as disclosures are authorised under the *My Health Records Act 2012* (Cth).

12.3 We note for other 'business as usual' operations that the DHR Solution will now be utilised for, to the extent any disclosures were supported by HPP 10 they will also be supported by HPP 10 for the DHR Solution (for example, responding to medico-legal requests will be supported by HPP 10.2(e)).

12.4 In this context, we note that the particular 'business as usual' operation relating to mental health consumer decisions under the *Mental Health Act 2015* (ACT) will need to be facilitated by the DHR Solution. That Act provides for processes in relation to 'nominated persons', 'advance agreements' and 'advance consent directions'[33], which can enable persons (other than the Patient) to receive information about a Patient (who is a mental health consumer). Access to a Patient's DHR by these other persons would be supported by HPP 10.2(e) (disclosure allowed by a Territory law) and the processes that apply to Carers obtaining access to the Patient Portal will equally apply to such persons. We note that this would address concerns raised by consumers about ensuring there is 'proxy' access to a Patient's DHR in appropriate circumstances.

12.5 We note for completeness that in the context of mental health, there may be circumstances, as is the case now, that a Patient should not have access to their own medical records (as opposed to a Carer or other authorised person) as it may be detrimental to the Patient's health and safety. The DHR Solution will need to be able to remove access to a Patient's DHR through the Patient Portal or otherwise limit what can be seen. We note that this situation will likely arise in very limited circumstances. However, it will be a simple matter of 'switching off' access to the Patient Portal, following appropriate consideration of the issues by ACT Health.

[33] Detailed information about a mental health consumers rights are explained in *My Rights, My Decisions Form Kit* (https://www.health.act.gov.au/sites/default/files/2019-03/2019-02-15%20Form%20Kit%20My%20Rights%20My%20Decisions.pdf)

13. HPP 11 – Relocation and closure of health service practice

Text of HPP 11

Principle 11— Relocation and closure of health service practice

1. This principle applies if a health service practice is or is proposed to be—
   (a) relocated; or
   (b) permanently closed.
2. Not later than 30 days before the proposed relocation or closure, the provider must—
   (a) give public notice of the relocation or closure (a transfer notice); and
   (b) take other practicable steps to inform each consumer who has attended the health service practice of the matters mentioned in the transfer notice.
3. The transfer notice must state—
   (a) that the consumer may request (a transfer request) that a copy or written summary of the consumer's health record be given to the consumer or a health service provider nominated by the consumer; and
   (b) that the transfer request must be made not later than 14 days after the day the transfer notice (the transfer request period) is published; and
   (c) if a fee has been determined under section 34 for this principle—that there is a fee that the consumer must pay before the provider will give a copy or written summary of the record to the consumer or health service provider nominated by the consumer; and
   (d) that if the consumer does not make a transfer request within the transfer request period, a copy of the consumer's health record will be given to a stated health service provider or record keeper; and
   (e) the stated health service provider's or record keeper's address and contact details.
4. As soon as practicable after publishing the transfer notice, the provider must give a copy of the transfer notice, or written notice of the information in the transfer notice, to the director-general.
5. If a consumer has made a transfer request, the provider must give the consumer or the consumer's nominated health service provider the requested copy or written summary of the consumer's health record as soon as practicable but not later than the later of—
   (a) if a fee is payable for this principle—7 days after the day the fee is paid; and
   (b) 30 days after the day the provider receives the transfer request.
6. If, however, the consumer is receiving or needs urgent health services, the provider must give the consumer or the consumer's nominated health service provider the requested copy or written summary of the consumer's health record as soon as practicable but not later than 7 days after the day the provider receives the transfer request.
7. If a consumer does not make a transfer request within the transfer request period, the provider must, within 30 days after the end of the transfer request period, give a copy of the consumer's health records to the health service provider or record keeper stated in the transfer notice.
8. If a record keeper holds health records following the relocation or closure of a health service practice, the record keeper must promptly notify the director-general of any change to—
   (a) the record keeper's contact details; or
   (b) the location of the stored health records.
9. The director-general must promptly give a copy of a notice under clause 4 or clause 8 to the health services commissioner.
10. If this principle applies because a sole provider in a health service practice dies or becomes legally incompetent, a legal representative or guardian of the provider must comply with the requirements of this principle as soon as practicable.
11. It is sufficient to establish that a consumer is receiving or needs urgent health services for prioritising the giving of records by a provider (the record holder) if another health service provider advises the record holder that the consumer is receiving or needs urgent health services.
12. However—

(a) an advice under clause 11 need not be in writing; and

(b) the record keeper may be satisfied that a consumer is receiving or needs urgent health services without an advice mentioned in clause 11.

13. The requirement under clause 5, clause 6 or clause 7 to give a copy of the consumer's health record is taken to be satisfied if the original of the record is given.

14. To remove doubt, clause 13 does not require a provider to give the original of the consumer's health record.

15. In this principle:

health record means a health record held by, or on behalf of, the provider.

health service practice means the business or premises where a health service provider provides health services.

provider means—

(a) the provider of a health service practice; or

(b) if the provider is legally incompetent—the guardian of the provider; or

(c) if the provider is dead—the legal representative of the provider.

relocate, a practice, includes—

(a) relocate to another premises or location; or

(b) stop, temporarily or otherwise, the provision of health services at a particular location.

transfer notice—see clause 2 (a).

transfer request—see clause 3 (a).

transfer request period—see clause 3 (b).

Analysis of compliance with HPP 11

HPP 11 sets out the requirements in relation to the relocation and closures of health service practices. This HPP is not relevant to the implementation of the DHR Solution.

14. HPP 12.1 – Consumer moves to another health service provider

Text of HPP 12.1

Principle 12.1— Consumer moves to another health service provider

1. If a consumer moves from 1 health service provider (the first provider) to another health service provider (the second provider), the consumer may ask the first provider to give the second provider a copy or written summary of the consumer's health record.

2. If the first provider receives a request under clause 1 (a transfer request), the first provider must

   (a) if a fee has been determined under section 34 for this principle—not later than 7 days after the day the first provider receives the transfer request, give the consumer notice that the consumer must pay a stated fee before the first provider will give the second provider the requested copy or written summary of the consumer's health record; or

   (b) not later than 30 days after the day the first provider receives the transfer request, give the second provider the requested copy or written summary of the consumer's health record.

3. If the consumer pays the fee stated in a notice under clause 2 (a), the first provider must give the second provider the requested copy or written summary of the consumer's health record not later than the later of—

   (a) 7 days after the day the fee is paid; and
   (b) 30 days after the day the first provider receives the transfer request.

4. If the consumer is receiving or needs urgent health services, the first provider must give the second provider the requested copy or written summary of the consumer's health record as soon as practicable but not later than 7 days after the day the first provider receives the transfer request.

5. It is sufficient to establish that a consumer is receiving or needs urgent health services for prioritising the giving of records by the first provider (the record holder) if another health service provider advises the record holder that the consumer is receiving or needs urgent health services.

6. However—
   (a) an advice under clause 5 need not be in writing; and

   (b) the record keeper may be satisfied that a consumer is receiving or needs urgent health services without an advice mentioned in clause 5.

7. The requirement under clause 2 (b), clause 3 or clause 4 to give a copy of the consumer's health record to the second provider is taken to be satisfied if the original of the record is given.

8. To remove doubt, clause 7 does not require the first provider to give the original of the consumer's health record to the second provider.

9. In this principle:

   first provider—
   (a) see clause 1; and
   (b) includes—
      (i) if the first provider becomes legally incompetent—a guardian of the provider; or
      (ii) if the first provider dies—a legal representative of the provider.

   health record means a health record held by, or on behalf of, the first provider.

   second provider—see clause 1.

   transfer request—see clause 2.

Analysis of compliance with HPP 12.1

14.1 The usual practices of transfer of records will not be impacted by the implementation of the DHR Solution. We understand that manual processes will continue to be utilised to transfer records to another health service provider in another state or territory.

15. HPP 12.2 – Health service provider moves to another health service practice

Text of HPP 12.2

Principle 12.2— Health service provider moves to another health service practice

1. If a health service provider (the provider) moves from 1 health service practice (the first practice) to another health service practice and a consumer continues to see the provider, the consumer may ask the first practice to give the provider a copy or written summary of the consumer's health record.
2. If the first practice receives a request under clause 1 (a transfer request), the first practice must—
   (a) if a fee has been determined under section 34 for this principle—not later than 7 days after the day the first practice receives the transfer request, give the consumer notice that the consumer must pay a stated fee before the first practice will give the provider the requested copy or written summary of the consumer's health record; or
   (b) not later than 30 days after the day the first practice receives the transfer request, give the provider the requested copy or written summary of the consumer's health record.
3. If the consumer pays the fee stated in a notice under clause 2 (a), the first practice must give the provider the requested copy or written summary of the record not later than the later of—
   (a) days after the day the fee is paid; and
   (b) 30 days after the day the first practice receives the transfer request.
4. If the consumer is receiving or needs urgent health services, the first practice must give the provider the requested copy or written summary of the consumer's health record as soon as practicable but not later than 7 days after the day the first practice receives the transfer request.
5. It is sufficient to establish that a consumer is receiving or needs urgent health services for prioritising the giving of records by the first practice (the record holder) if another health service provider advises the first practice that the consumer is receiving or needs urgent health services
6. However—
   (a) an advice under clause 5 need not be in writing; and
   (b) the record keeper may be satisfied that a consumer is receiving or needs urgent health services without an advice mentioned in clause 5.
7. The requirement under clause 2 (b), clause 3 or clause 4 to give a copy of the consumer's health record to the provider is taken to be satisfied if the original of the record is given.
8. To remove doubt, clause 7 does not require the first practice to give the original of the consumer's health record to the provider.
9. In this principle:

   first practice—see clause 1.

   health record means a health record held by, or on behalf of, the first provider.

   health service practice means the business or premises where a health service provider provides

   health services. provider—see clause 1.

   transfer request—see clause 2.

Analysis of compliance with HPP 12.2

15.1 This HPP is not relevant to the DHR Solution as it deals with movement of records where a health service provider moves between health services.

Part F TPP COMPLIANCE

As set out above, we have considered compliance against the TPPs in relation to the potential handling of personal information in the DHR Solution of persons other than Patients, and from a best privacy practice perspective.

16. TPP 1 – Open and transparent management of personal information

Text of TPP 1

1 Territory Privacy Principle 1—open and transparent management of personal information

1.1 The object of this TPP is to ensure that public sector agencies manage personal information in an open and transparent way.

Compliance with the TPPs etc

1.2 A public sector agency must take reasonable steps to implement practices, procedures and systems relating to the agency's functions or activities that—

(a) will ensure that the agency complies with the TPPs and any TPP code that binds the agency; and

(b) will enable the agency to deal with inquiries or complaints from individuals about the agency's compliance with the TPPs or a code.

TPP privacy policy

1.3 A public sector agency must have a clearly expressed and up-to-date policy (the ***TPP privacy policy***) about the management of personal information by the agency.

1.4 Without limiting TPP 1.3, the TPP privacy policy of the public sector agency must contain the following information:

(a) the kinds of personal information that the agency collects and holds;

(b) how the agency collects and holds personal information;

(c) the purposes for which the agency collects, holds, uses and discloses personal information;

(d) how an individual may access personal information about the individual that is held by the agency and seek the correction of the information;

(e) how an individual may complain about a breach of the TPPs, or any TPP code that binds the agency, and how the agency will deal with the complaint;

(f) whether the agency is likely to disclose personal information to overseas recipients;

(g) if the agency is likely to disclose personal information to overseas recipients—the countries in which the recipients are likely to be located if it is practicable to state those countries in the policy.

Availability of TPP privacy policy etc

1.5 A public sector agency must take reasonable steps to make its TPP privacy policy available—

(a) free of charge; and

(b) in an appropriate form.

Example

on the agency's website

1.6 If a person requests a copy of the TPP privacy policy of a public sector agency in a particular form, the agency must take reasonable steps to give the person a copy in that form.

Note ***Person*** includes a reference to a corporation as well as an individual (see Legislation Act, s 160).

Analysis of compliance with TPP 1

16.1 TPP 1 is intended to ensure that agencies manage personal information in an open and transparent way.

16.2 We note that ACT Health has established a website about the DHR Solution to inform persons of the work that is currently underway. We see this as an important transparency measure.

16.3 TPP 1.2 requires ACT Health to implement practices, procedures and systems to comply with the TPPs. Undertaking PIAs such as this one also represents a reasonable step for agencies which are subject to the TPPs to take. To ensure that personal information is managed in an open and transparent way, we **recommend** that ACT Health consider:

16.3.1 publishing this PIA, or a summary form of its findings and recommendations, on its website;

16.3.2 ensuring that information on the DHR is included on its, and/or Canberra Health Services, websites so persons understand how their personal information in the DHR Solution will be handled (by whom personal information will be accessed, for what purpose, and how it will be used and disclosed). This information could include a suitable privacy notice; and

when implementing the DHR Solution, include as part of the work program that any relevant admissions forms be updated to refer to the website. Information (for example, in the form of pamphlets) containing information about the DHR Solution could also be prepared and made available when a person presents at a Health Service.

(**Recommendation 2**)

16.4 We note the implementation of the DHR Solution is an iterative process, involving a number of decision points about design and configuration. We understand that future PIAs are likely to be undertaken as further functionality decisions are made and more information is available.

16.5 In our view, a good governance structure also promotes TPP 1, as well as assisting in addressing other privacy risks, such as 'function creep'. As is generally case with projects of this nature, and noting the potential for the DHR Solution to be flexible and for its design to be significantly further developed and enhanced in the future, there is a potential risk that privacy factors may not be appropriately considered at the time that the extended functionalities are approved or implemented.

16.6 The project documentation we have reviewed includes strong governance arrangements, including processes for how changes to configuration need to be reviewed and approved. We understand the final project governance structure is currently being finalised. It is not, however, clear from the documentation provided *how* privacy implications of any changes are considered as part of the governance structure, apart from in a general sense.

16.7 We therefore **recommend** that ACT Health ensure that it has suitable governance processes in place in relation to the further functionality or enhancement of the DHR Solution, which will ensure any privacy implications of the new or changed functionality which might affect the information flows identified in this PIA are considered and addressed before any extended functionalities are approved or implemented. This could include:

16.7.1 ensuring that examination of privacy implications is a standing item/issue that must be addressed in any change documentation; and

16.7.2 treating this PIA as a 'living document' which is reviewed and updated as further enhancements are considered, including undertaking further updates or supplementary PIA processes as required.

(**Recommendation 1**)

16.8 For example, we consider that such review and re-examination is likely to be required when further details are available about any integration with the longitudinal data sets in the "ACT Health Data Repository", with the DHR Solution (since it will be necessary to examine the particular data sets stored within the ACT Health Data Repository, and determine whether this further use, and the use or disclosure once integrated into the DHR Solution – which may depend on the purpose for which the data was originally collected, and what the relevant individuals were told at the time of collection).

16.9 For completeness, we note that TPP 1.3 to 1.6 deal with a requirement to have a Privacy Policy. We note that ACT Health has a relevant TPP Policy covering personal information.

17. TPP 2 – Anonymity and pseudonymity

Text of TPP 2

2 Territory Privacy Principle 2—anonymity and pseudonymity

2.1 Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with a public sector agency in relation to a particular matter.

2.2 TPP 2.1 does not apply if, in relation to the matter—

(a) the public sector agency is required or authorised by or under an Australian law, or a court or tribunal order, to deal with individuals who have identified themselves; or

(b) it is impracticable for the public sector agency to deal with individuals who have not identified themselves or who have used a pseudonym.

Analysis of compliance with TPP 2

17.1 TPP 2.1 requires public sector agencies to give individuals the options of not identifying themselves, or of using a pseudonym, when dealing with the entity in relation to a particular matter, unless an exception under TPP 2.2 applies.

17.2 Importantly, TPP 2.2(b) provides that TPP 2.1 does not apply if it is impracticable for the public sector agency to deal with individuals who have not identified themselves, or who have used a pseudonym.

17.3 We note that personal information about:

17.3.1 Users from external health providers;

17.3.2 Carers; and

17.3.3 Users from Epic (and potentially other ICT service providers)

will be collected in connection with granting access to the DHR Solution (in additional personal health information about Patients which will be subject to the HPPs rather than the TPPs).

17.4 Given the sensitivity of the information about Patients that will be stored in the Patient's DHR, the identity of persons who may be given access to the DHR Solution is a critical component.

17.5 We consider TPP 2.1 does not apply to the DHR Solution by virtue of the exception arising under TPP 2.2(b), where it would be impractical (and unsafe) to deal with persons authorised to access Patient Information if they cannot be identified.

18. TPP 3 – Collection of personal information

Text of TPP 3

3 Territory Privacy Principle 3—collection of personal information

Personal information other than sensitive information

3.1 A public sector agency must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, 1 or more of the agency's functions or activities.

Note The equivalent provision in the Commonwealth APPs includes a provision applying to certain private sector entities (see Commonwealth APP 3, s 3.2).

Sensitive information

3.3 A public sector agency must not collect sensitive information about an individual unless—

(a) the individual consents to the collection of the information and the information is reasonably necessary for, or directly related to, 1 or more of the agency's functions or activities; or

(b) TPP 3.4 applies in relation to the information.

Note The equivalent provision in the Commonwealth APPs also applies to certain private sector entities (see Commonwealth APP 3, s 3.3 (a) (ii)).

3.4 This subsection applies in relation to sensitive information about an individual if—

(a) the collection of the information is required or authorised by or under an Australian law or a court or tribunal order; or

(b) a permitted general situation exists in relation to the collection of the information by the public sector agency; or

Note The equivalent provision in the Commonwealth APPs includes a provision applying to certain private sector entities (see Commonwealth APP 3, s 3.4 (c)).

(d) the public sector agency is an enforcement body and the agency reasonably believes that the collection of the information is reasonably necessary for, or directly related to, 1 or more of the agency's functions or activities.

Note The equivalent provision in the Commonwealth APPs includes a provision applying to—

- the Commonwealth Immigration Department (see Commonwealth APP 3, s 3.4 (d) (i)); and
- non-profit organisations (see Commonwealth APP 3, s 3.4 (e)).

Means of collection

3.5 A public sector agency must collect personal information only by lawful and fair means.

3.6 A public sector agency must collect personal information about an individual only from the individual unless—

(a) either—

(i) the individual consents to the collection of the information from someone other than the individual; or

(ii) the agency is required or authorised by or under an Australian law, or a court or tribunal order, to collect the information from someone other than the individual; or

(b) it is unreasonable or impracticable to do so.

Note The equivalent provision in the Commonwealth APPs applies, in part, to certain private sector entities.

Solicited personal information

3.7 TPP 3 applies to the collection of personal information that is solicited by a public sector agency.

Analysis of compliance with TPP 3

18.1 As the HPPs deal in particular with the collection of personal health information (which forms the basis of the clinical record in the Patient's DHR), we have not considered the principles in this TPP in great detail in relation to the Patient's DHR.

18.2 However, we note that the DHR Solution will also collect personal information about external health care providers, Carers and external ICT support staff, to provide them with access to the DHR Solution. This will involve the collection of solicited personal information.

18.3 Determining whether a collection of personal information is permitted under TPP 3.1 requires a two-step process:

18.3.1 **Step 1** – identifying a public sector agency's functions or activities; and

18.3.2 **Step 2** – determining whether the relevant collection of personal information is reasonably necessary for or directly related to one of those functions or activities.

18.4 Whether a collection of personal information is "reasonably necessary" for a public sector agency's functions or activities is an objective test, which considers whether a reasonable person who is properly informed would agree that the collection is necessary. It is the responsibility of a public sector agency to be able to justify that the particular collection is reasonably necessary. Factors relevant to determining whether a collection of personal information is reasonably necessary for a function or activity include:

18.4.1 the primary purpose for collection;

18.4.2 how the personal information will be used; and

18.4.3 whether the entity could undertake the function or activity without collecting that personal information.

18.5 The term "necessary" is not defined and should be interpreted in a practical sense. However, the OAIC considers that in the context of the *Privacy Act 1988* (Cth), which is in the same terms as TPP 3, that it would not be sufficient if the collection is merely helpful, desirable or convenient.

18.6 To be "directly related to" an agency's functions or activities, a clear and direct connection must exist between the personal information being collected and an agency's functions or activities.

18.7 In our view, the collection of personal information about external health care providers would be directly related to ACT Health's function of providing healthcare to Patients, as communicating with other health care providers is an essential part of undertaking that function. Similarly, the collection of personal information about Carers, is also directly related to the provision of health services to a Patient.

18.8 Best practice also requires consideration of the "data minimisation principle", under which an APP entity should minimise the amount of personal information collected to the extent possible, and limit collection to only that information which is necessary for the purposes for which it is collected.

18.9 We note that ACT Health is currently considering the processes that will be used for registering or otherwise allowing access by health care providers, Carers and external ICT support staff. We provide the following guidance to be taken into account in the design of the processes for granting access: only the minimum personal information required to identify the person should be solicited. For example, information about their political associations would not be relevant or necessary (**Recommendation 7**).

Collection of Patient photographs

18.10 We note that, while the DHR Solution does not require that a photograph of a Patient be included in a Patient's DHR, this is possible and currently being considered to assist in confirming identification of the Patient. The process for doing this has not yet been determined but is anticipated that a photograph may be taken (i.e. collected) when a person attends at a Health Service.

18.11 We note that a photograph, to be used for manual identification processes as is the case here, is unlikely to be 'sensitive information' for the purposes of TPP 3, which means that although consent is not required to ensure compliance, as discussed above the collection must be still be reasonably necessary for an entity's functions and activities. We consider that collection of a Patient photograph and storage in the DHR Solution so that it can be used for manual identification purposes, where this will assist in the proper administration of the health service and the delivery of medical care to a Patient, meets this requirement.

18.12 However, we consider that the discussion in paragraphs 2.11 to 2.18 above in relation to clinical photographs is also relevant here. In our view, the reasoning that has been applied to the requirement for Patient consent in relation to the collection and storage of clinical photographs, should also be applied to the collection and storage of other Patient photographs.

18.13 Accordingly, we **recommend** that, in accordance with best practice, specific consent be obtained from a Patient if their photograph will be uploaded to the Patient's DHR so that it can be used by Users to assist them in identifying that person in the future. We do note that such consent could be obtained orally, if appropriate, but the proposed use of the photograph should be explained to the Patient, and the consent should be obtained from a person with the necessary legal capacity if the Patient does not have this (**Recommendation 8**).

18.14 In addition, it will be important that the collected photograph does not, over time, become used for additional purposes (such as automated biometric identification). We note that implementation of **Recommendation 1** will assist in ensuring that such "function creep" does not occur.

19. TPP 4 – Dealing with unsolicited personal information

Text of TPP 4

4 Territory Privacy Principle 4—dealing with unsolicited personal information

4.1 If—

(a) a public sector agency receives personal information; and

(b) the agency did not solicit the information;

the agency must, within a reasonable period after receiving the information, decide whether or not the agency could have collected the information under TPP 3 if the agency had solicited the information.

4.2 The public sector agency may use or disclose the personal information for the purposes of making the decision under TPP 4.1.

4.3If—

(a) the public sector agency decides that the agency could not have collected the personal information; and

(b) the information is not contained in a territory record;

the agency must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.

4.4 If TPP 4.3 does not apply in relation to the personal information, TPPs 5 to 13 apply in relation to the information as if the agency had collected the information under TPP 3.

Analysis of compliance with TPP 4

19.1 TPP 4 only applies where the DHR receives unsolicited personal information (i.e. information that it receives but has taken no active steps to solicit).

19.2 The OAIC's guidance is that an entity 'solicits' personal information where it 'requests' the information. A 'request' is an active step taken by an entity to collect personal information and may not involve direct communication between the entity and an individual.[34]

19.3 All personal information collected through the DHR Solution about external health care providers to register for access to the DHR Solution will be solicited (i.e. sought from the external health care provider, Carer or external ICT service provider). It is unlikely that a person seeking access will (or will be able to) provide additional information (i.e. unsolicited information). TPP 4 is therefore not relevant in the context of the DHR Solution.

[34] APP Guidelines, Chapter B, at 3.6

20. TPP 5 – Notification of the collection of personal information

Text of TPP 5

5 Territory Privacy Principle 5—notification of the collection of personal information

5.1 At or before the time or, if that is not practicable, as soon as practicable after, a public sector agency collects personal information about an individual, the agency must take reasonable steps—

(a) to notify the individual of the matters mentioned in TPP 5.2 that are reasonable in the circumstances; or

(b) to otherwise ensure that the individual is aware of those matters.

5.2 The matters for TPP 5.1 are as follows:

(a) the identity and contact details of the public sector agency;

(b) if—

(i) the public sector agency collects the personal information from someone other than the individual; or

(ii) the individual may not be aware that the public sector agency has collected the personal information;

the fact that the agency collects, or has collected, the information and the circumstances of that collection;

(c) if the collection of the personal information is required or authorised by or under an Australian law, or a court or tribunal order—the fact that the collection is required or authorised (including the name of the Australian law, or details of the court or tribunal order, that requires or authorises the collection);

(d) the purposes for which the public sector agency collects the personal information;

(e) the main consequences (if any) for the individual if all or some of the personal information is not collected by the public sector agency;

(f) any other public sector agency or entity, or the kinds of any other public sector agencies or entities, to which the public sector agency usually discloses personal information of the kind collected by the agency;

(g) that the TPP privacy policy of the public sector agency contains information about how the individual may access the personal information about the individual that is held by the agency and seek the correction of the information;

(h) that the TPP privacy policy of the public sector agency contains information about how the individual may complain about a breach of the TPPs, or any TPP code that binds the agency, and how the agency will deal with the complaint;

(i) whether the public sector agency is likely to disclose the personal information to overseas recipients;

(j) if the public sector agency is likely to disclose the personal information to overseas recipients—the countries in which the recipients are likely to be located if it is practicable to state those countries in the notification or to otherwise make the individual aware of them.

Analysis of compliance with TPP 5

20.1 TPP 5 requires an entity that collects personal information about an individual to take reasonable steps to notify the individual of certain matters (referred to as "TPP 5 matters"), or otherwise ensure that the individual is aware of those matters. This notification must occur at, or before the time of collection, or as soon as practicable afterwards.

20.2 ACT Health will need to ensure that a suitable TPP 5 collection notice covering the TPP 5 matters is provided to a person applying for access (i.e. from an external health care provider, a Carer, or a person from an ICT service provider) at the time they are registering or otherwise applying for access to the DHR Solution (**Recommendation 7**).

21. TPP 6 – Use or disclosure of personal information

Text of TPP 6

6 Territory Privacy Principle 6—use or disclosure of personal information

Use or disclosure

6.1 If a public sector agency holds personal information about an individual that was collected for a particular purpose (the ***primary purpose***), the agency must not use or disclose the information for another purpose (the ***secondary purpose***) unless—

(a) the individual has consented to the use or disclosure of the information; or

(b) TPP 6.2 or TPP 6.3 applies in relation to the use or disclosure of the information.

Note TPP 8 sets out requirements for the disclosure of personal information to a person who is not in Australia or an external territory.

6.2 This subsection applies in relation to the use or disclosure of personal information about an individual if—

(a) the individual would reasonably expect the public sector agency to use or disclose the information for the secondary purpose and the secondary purpose is—

(i) if the information is sensitive information—directly related to the primary purpose; or

(ii) if the information is not sensitive information—related to the primary purpose; or

(b) the use or disclosure of the information is required or authorised by or under an Australian law or a court or tribunal order; or

(c) a permitted general situation exists in relation to the use or disclosure of the information by the public sector agency; or

Note The equivalent provision in the Commonwealth APPs includes a provision applying to certain private sector entities (see Commonwealth APP 6, s 6.2 (d)).

(e) the public sector agency reasonably believes that the use or disclosure of the information is reasonably necessary for 1 or more enforcement-related activities conducted by, or on behalf of, an enforcement body.

6.3 This subsection applies in relation to the disclosure of personal information about an individual by a public sector agency if—

(a) the agency is not an enforcement body; and

(b) the information is biometric information or biometric templates; and

(c) the recipient of the information is an enforcement body; and

(d) the disclosure is conducted in accordance with the guidelines made by the information privacy commissioner for this subsection.

Note The equivalent provision in the Commonwealth APPs includes a provision applying to certain private sector entities (see Commonwealth APP 6, s 6.4).

Written note of use or disclosure

6.5 If a public sector agency uses or discloses personal information in accordance with TPP 6.2 (e), the agency must make a written note of the use or disclosure.

Related bodies corporate

6.6 If—

(a) a public sector agency is a corporation; and

(b) the agency collects personal information from a related body corporate;

this TPP applies as if the agency's primary purpose for the collection of the information were the primary purpose for which the related body corporate collected the information.

Note The equivalent provision in the Commonwealth APPs includes a provision applying to certain private sector entities (see Commonwealth APP 6, s 6.7).

Analysis of compliance with TPP 6

21.1 We see that personal information about external Users is collected for the purposes of providing access to the DHR Solution would only be used or disclosed for that purpose, or for other purposes as permitted by TPP 6.

21.2 Of particular relevance here is disclosure of personal information to ICT service providers for the DHR Solution (that is, Epic in its role of maintaining and supporting the DHR Solution[35] is likely to have access to information about other external Users). We understand that Epic will potentially have access to personal information about Patients when it provides 'hypercare' services (support and other assistance after the DHR Solution's go live date) to ACT Health.

21.3 Guidance from the OAIC indicates that, in some limited circumstances, potential disclosure to a contractor to perform services may be a considered as a 'use' by the relevant entity, rather than a 'disclosure' to that contractor and a 'collection' by that contractor. The OAIC guidance indicates that the key feature for such circumstances to apply is that the relevant entity does not release the personal information from its effective control. It also notes that there should be:

21.3.1 a binding contract between the entity and the provider, which requires the provider only to handle the personal information for these limited purposes;

21.3.2 provisions in the contract that require any subcontractors to agree to the same obligations; and

21.3.3 provisions in the contract that give the entity effective control of how the information is handled by the provider. Issues to consider include:

(a) whether the entity retains the right or power to access, change or retrieve the information;

(b) who else will be able to access the information and for what purposes;

(c) the security measures that will be used for the storage and management of the personal information; and

(d) whether the information can be retrieved or permanently deleted by the entity when it is no longer required or at the end of the contract.

21.4 In our view, the contractual arrangements with Epic do give effective control to ACT Health in relation to personal information (and personal health information in a Patient's DHR). The contractual obligations include:

21.4.1 ensuring that personnel who are required to deal with personal information for the purposes of the relevant contract are made aware of their privacy obligations;

21.4.2 specifically limits the ability of the contractor to transfer personal information to itself or to an overseas entity without appropriate approval from ACT Health and subject to conditions;

21.4.3 security obligations that are required to be implemented by the contractor, and adhered to when handling personal information and carrying out its contractual obligations; and

21.4.4 containing provisions for how a data breach is to be handled between ACT Health and contractors.

[35] We note that any use or disclosure of information to or by NTT, which will provide cloud hosting services for the DHR Solution will be considered in a separate PIA process.

21.5 Another issue is the use of personal information about staff or contractors of Health Services, which was previously collected in connection with their employment or engagement, to create profiles in the DHR Solution that will grant them access as Users of the DHR Solution.

21.6 We consider that it is certainly arguable that this use of personal information falls within the primary purpose for collection, in that the personal information was collected to facilitate the proper and effective management of their employment or engagement, and that providing access to ICT solutions which they are required to use for their employment or engagement falls within that primary purpose. But in any event, we consider that this use would fall within exception in TPP 6.2(a), in that staff would reasonably expect their personal information collected in connection with their employment or engagement to be used to grant them access to ICT solutions which are necessary for them to undertake their role, and that this purpose is related (even directly related) to the primary purpose as described above.

21.7 In our view, no further steps in connection with the DHR Solution are required in relation to TPP 6, but ACT Health should continue to implement its usual policies and procedures (such as training staff) which are designed to ensure compliance with the requirements of TPP 6.

22. TPP 7 – Direct marketing

Text of TPP 7

7 Territory Privacy Principle 7—direct marketing

Note 1 The Commonwealth Act includes a privacy principle prohibiting direct marketing by certain private sector entities (see Commonwealth APP 7).

Note 2 However, Commonwealth APP 7 applies to an act or practice of a public sector agency if the agency engages in commercial activities (see s 23).

Analysis of compliance with TPP 7

22.1 This is not relevant to the DHR Solution being implemented by ACT Health.

23. TPP 8 – Cross-border disclosure of personal information

Text of TPP 8

8 Territory Privacy Principle 8—cross-border disclosure of personal information

8.1 Before a public sector agency discloses personal information about an individual to a person (an ***overseas recipient***)—

(a) who is not in Australia or an external territory; and

(b) who is not the agency or the individual;

the agency must take reasonable steps to ensure that the overseas recipient does not breach the TPPs (other than TPP 1) in relation to the information.

Note In certain circumstances, an act done, or a practice engaged in, by an overseas recipient is taken, under s 22, to have been done, or engaged in, by the public sector agency and to be a breach of the TPPs.

8.2 TPP 8.1 does not apply to the disclosure of personal information about an individual by a public sector agency to the overseas recipient if—

(a) the agency reasonably believes that—

(i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the TPPs protect the information; and

(ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or

(b) both of the following apply:

(i) the agency expressly informs the individual that if the individual consents to the disclosure of the information, TPP 8.1 will not apply to the disclosure;

(ii) after being informed, the individual consents to the disclosure; or

(c) the disclosure of the information is required or authorised by or under an Australian law, or a court or tribunal order; or

(d) a permitted general situation (other than the situation mentioned in section 19 (1) (d) or (e)) exists in relation to the disclosure of the information by the agency; or

(e) the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia or the Territory is a party; or

(f) both of the following apply:

(i) the agency reasonably believes that the disclosure of the information is reasonably necessary for 1 or more enforcement-related activities conducted by, or on behalf of, an enforcement body;

(ii) the recipient is a body that exercises functions that are similar to those exercised by an enforcement body.

Analysis of compliance with TPP 8

23.1 TPP 8 requires entities to take particular steps if they intend on disclosing personal information to an overseas recipient.

23.2 We are not aware of ACT Health intending to disclose personal information overseas and note that the contractual arrangements with Epic include appropriate obligations, as discussed at TPP 7, about the potential disclosure of personal information overseas and in our view are sufficient to comply with TPP 8.

24. TPP 9 – Adoption, use or disclosure of government related identifiers

Text of TPP 9

9 Territory Privacy Principle 9—adoption, use or disclosure of government related identifiers

Note 1 The Commonwealth Act includes a privacy principle regulating the adoption, use or disclosure of government-related identifiers by certain private sector entities (see Commonwealth APP 9).

Note 2 However, Commonwealth APP 9 applies to an act or practice of a public sector agency if the agency engages in commercial activities (see s 23).

Analysis of compliance with TPP 9

24.1 TPP 9 is not relevant to the DHR Solution being implemented by ACT Health.

25. TPP 10 – Integrity of personal information

Text of TPP 10

10 Territory Privacy Principle 10—integrity of personal information

10.1 A public sector agency must take reasonable steps to ensure that the personal information that the agency collects is accurate, up-to-date and complete.

10.2 A public sector agency must take reasonable steps to ensure that the personal information that the agency uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

Analysis of compliance with TPP 10

25.1 TPP 10 requires ACT Health to take reasonable steps (if any) to ensure that the personal information that it:

25.1.1 collects is accurate, up-to-date, and complete; and

25.1.2 uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

25.2 Applying OAIC guidance in relation to wording in APP 10, which is informative for TPP 10, provides that in the context of TPP 10 the "reasonable steps" that an agency should take will depend upon circumstances that include:

25.2.1 the sensitivity of the personal information;

25.2.2 the nature of the agency (including its size, resources and business models);

25.2.3 the possible adverse consequences for an individual if the quality of personal information is not ensured; and

25.2.4 the practicability, including time and cost involved. However, an agency is not excused from taking particular steps by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take particular steps will depend on whether the burden is excessive in all the circumstances.[36]

25.3 It is implicit in the use of the phrase "if any" in APP 10.1 that it will be reasonable for an entity to take no steps to ensure data quality in some circumstances. For example, where an entity collects personal information from a source known to be reliable (such as the individual concerned), it may be reasonable to take no steps to ensure data quality.[37]

25.4 In our view the collection of personal information directly from persons applying for access to the DHR Solution for the purposes of registering or otherwise granting them access the DHR Solution would meet TPP 10.

[36] APP Guidelines, Chapter 10, paragraph 10.6.
[37] APP Guidelines, Chapter 10, paragraph 10.7.

26. TPP 11 – Security of personal information

Text of TPP 11

11 Territory Privacy Principle 11—security of personal information

11.1 If a public sector agency holds personal information, the agency must take reasonable steps to protect the information—

(a) from misuse, interference or loss; and

(b) from unauthorised access, modification or disclosure.

11.2 If—

(a) a public sector agency holds personal information about an individual; and

(b) the agency no longer needs the information for a purpose for which the information may be used or disclosed by the agency under the TPPs; and

(c) the information is not contained in a territory record; and

(d) the agency is not required by or under an Australian law, or a court or tribunal order, to retain the information;

the agency must take reasonable steps to destroy the information or to ensure that the information is de-identified.

Analysis of compliance with TPP 11

26.1 TPP 11.1 requires ACT Health to take such steps as are reasonable to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

26.2 We discuss similar obligations contained in HPP 4.1 above in relation to Patient Information. As set out in that discussion, we note that a number of measures will be implemented to protect the personal health information in the DHR Solution. These measures will apply equally to other personal information contained in the DHR Solution (including of external health care providers, Carers and external ICT service providers). We do not consider it necessary to provider further measures to protect the personal information in the DHR Solution.

26.3 TPP 11.2 requires ACT Health to take reasonable steps in the circumstances to destroy or de-identify personal information it holds where it no longer needs the information for any purpose for which the information may be used or disclosed, but only where the information is not held in a Territory record[38] and it is not required by law or court/tribunal order to retain the information.

26.4 We **recommend** that ACT Health confirm that the design specifications for the DHR Solution contain functionality that will allow a User to appropriately delete or de-identify the personal information when it is no longer needed, in compliance with TPP 11.2 (**Recommendation 6**).

[38] Defined for the purpose of the Information Privacy Act in s 9(3) of the *Territory Records 2002* (ACT) as 'a '*territory record* is a record made and kept, or received and kept, by a person in the course of exercising a function under a territory law'.

27. TPP 12 – Access to personal information

Text of TPP 12

12 Territory Privacy Principle 12—access to personal information

Access

12.1 If a public sector agency holds personal information about an individual, the agency must, on request by the individual, give the individual access to the information.

Exception to access—agency

12.2 If the public sector agency is required or authorised to refuse to give the individual access to the personal information by or under—

(a) the *Freedom of Information Act 2016*; or

(b) another law in force in the ACT that provides for access by people to documents;

then, despite TPP 12.1, the agency is not required to give access to the extent that the agency is required or authorised to refuse to give access.

Note The equivalent provision in the Commonwealth APPs includes a provision applying to certain private sector entities (see Commonwealth APP 12, s 12.3).

Dealing with requests for access

12.4 The public sector agency must—

(a) respond to the request for access to the personal information within 30 days after the day the request is made; and

(b) give access to the information in the way requested by the individual, if it is reasonable and practicable to do so.

Note The equivalent provision in the Commonwealth APPs includes a provision applying to certain private sector entities (see Commonwealth APP 12, s 12.4 (a) (ii)).

Other means of access

12.5 If the public sector agency refuses—

(a) to give access to the personal information because of TPP 12.2; or

(b) to give access in the way requested by the individual;

the agency must take reasonable steps to give access in a way that meets the needs of the agency and the individual.

12.6 Without limiting TPP 12.5, access may be given through the use of a mutually agreed intermediary.

Access charges

12.7 The public sector agency must not charge the individual for the making of the request or for giving access to the personal information.

Note The equivalent provision in the Commonwealth APPs includes a provision applying to certain private sector entities (see Commonwealth APP 12, s 12.8).

Refusal to give access

12.9 If the public sector agency refuses to give access to the personal information because of TPP 12.2, or to give access in the way requested by the individual, the agency must give the individual a written notice that sets out—

(a) the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by regulation.

Note The equivalent provision in the Commonwealth APPs includes a provision applying to certain private sector entities (see Commonwealth APP 12, s 12.10).

Analysis of compliance with TPP 12

27.1 Under TPP 12, ACT Health is required to give an individual access to the personal information held by it unless it is authorised by legislation specified in APP 12 to refuse access.

27.2 We understand that ACT Health has standard procedures for individuals to request access to their personal information (which can be found in its Information Privacy Policy[39]), and that the implementation of the DHR Solution will not prevent the ACT Health from implementing those procedures so as to comply with TPP 12.

[39] We note that the Information Privacy Policy is titled 'Canberra Health Services Operational Policy – Information Privacy Policy' dated 16 July 2019 and assume that it covers ACT Health. (https://www.health.act.gov.au/sites/default/files/2019-04/Information%20Privacy%20Policy.pdf)

28. TPP 13 – Correction of personal information

Text of TPP 13

13 Territory Privacy Principle 13—correction of personal information

Correction

13.1 If—

(a) a public sector agency holds personal information about an individual; and

(b) either—

(i) the agency is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out-of-date, incomplete, irrelevant or misleading; or

(ii) the individual requests the agency to correct the information;

the agency must take reasonable steps to correct the information to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading.

Notification of correction to third parties

13.2 If—

(a) the public sector agency corrects personal information about an individual that the agency previously disclosed to another public sector agency; and

(b) the individual requests the agency to notify the other public sector agency of the correction;

the agency must take reasonable steps to give the notification unless it is impracticable or unlawful to do so.

Refusal to correct information

13.3 If the public sector agency refuses to correct the personal information as requested by the individual, the agency must give the individual a written notice that sets out—

(a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by regulation.

Request to associate a statement

13.4 If—

(a) the public sector agency refuses to correct the personal information as requested by the individual; and

(b) the individual requests the agency to associate with the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading;

the agency must take reasonable steps to associate the statement in a way that will make the statement apparent to users of the information.

Dealing with requests

13.5 If a request is made under TPP 13.1 or TPP 13.4, the public sector agency—

(a) must respond to the request within 30 days after the day the request is made; and

(b) must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information.

Note The equivalent provision in the Commonwealth APPs includes a provision applying to certain private sector entities (see Commonwealth APP 13, s 13.5 (a) (ii)).

Analysis of compliance with TPP 13

28.1 TPP 13 requires ACT Health to permit correction of personal information, except in limited circumstances.

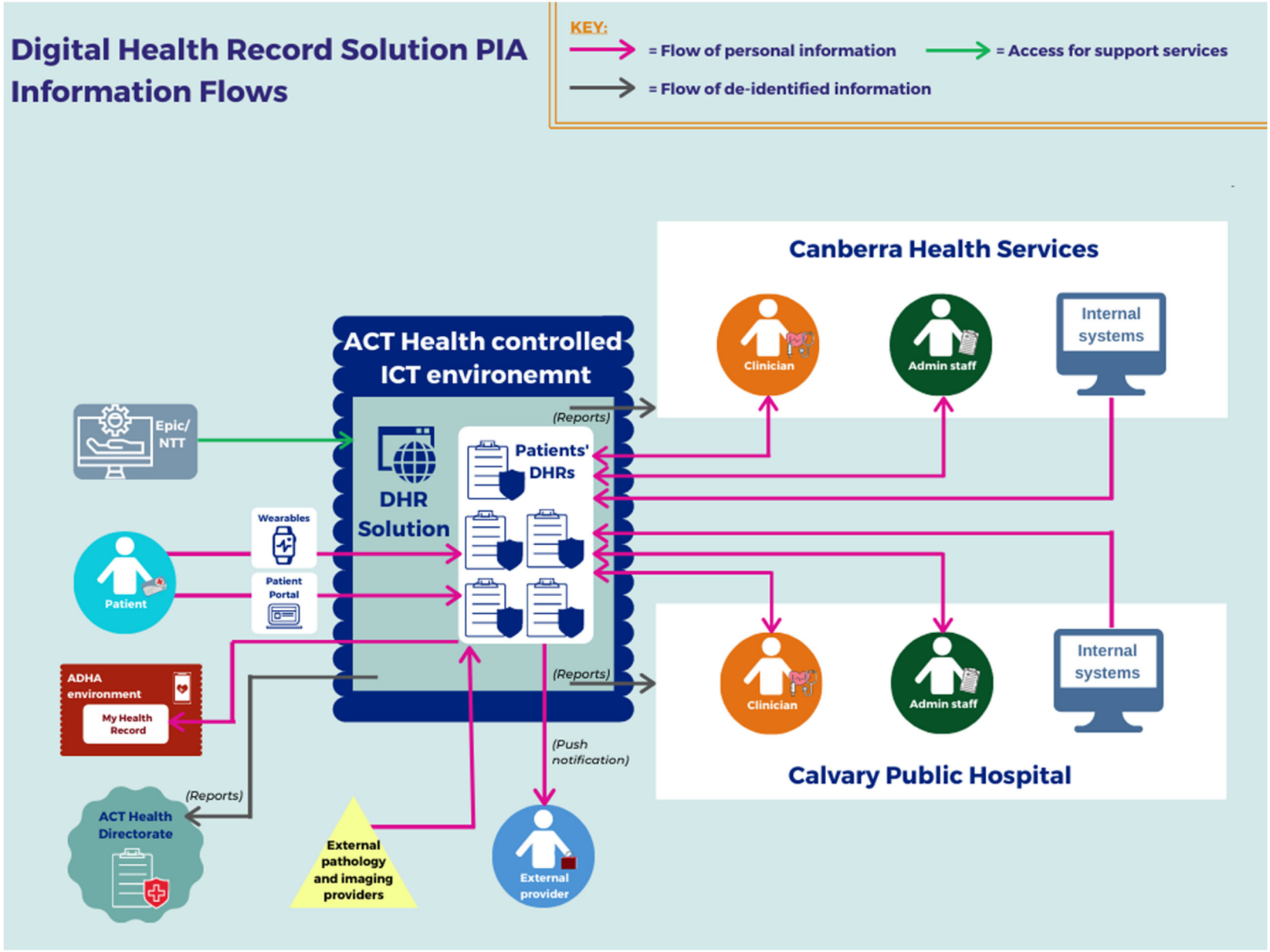
28.2 We understand that ACT Health has standard procedures for dealing with requests for correction of personal information (which can be found in its Information Privacy Policy) and that the implementation of DHR Solution will not prevent the ACT Health from implementing those procedures so as to comply with TPP 13.

Part G GLOSSARY

Definitions	
ACT Health	means the Australian Capital Territory Health Directorate.
APP Guidelines	means the *Australian Privacy Principles Guidelines* issued by the OAIC.
APPs	means the Australian Privacy Principles contained in the *Privacy Act 1998* (Cth) applicable to Commonwealth entities and certain private entities.
Calvary	means Calvary Health Care ACT Limited (ABN 74 105 304 989).
CHS	means Canberra Health Services, the administrative unit responsible for health services and facilities operated by the Territory government under the under the *Public Sector Management Act 1994*.
Carer	means an individual responsible for the care of a Patient.
Clinician	means health practitioners providing health care in a Health Service (such as doctors, specialists, nurses and allied health practitioners).
DHR	means a digital health record.
DHR Solution	means the Digital Health Record Solution being implemented by ACT Health.
Electronic Data Warehouse or EDW	means the part of the DHR Solution that will store a range of information, including all Patient Information and related system information.
Epic	means Epic Systems Melbourne Pty Ltd, ACT Health's contracted service provider responsible for developing, building, implementing and supporting the DHR Solution.
Health Records Act	means the *Health Records (Privacy and Access) Act 1997* (ACT).
Health Service	means a publicly funded facility in the Australian Capital Territory for the provision of health services to the public, including the three public hospital facilities (Canberra Hospital, Calvary Public Hospital Bruce, University of Canberra Hospital), all public mental health facilities, community health centres, walk-in centres and community based care.
Healthlink	means the existing external messaging provider.
HPPs or Health Privacy Principles	means the Privacy Principles contained in the Health Records Act.
Identity and Access Management Services	means the Access Control system, which will provide for the registration of Patients, Carers, Health Practitioners, Administrative and other staff providing Health Services to access the DHR Solution.
Information Privacy Act	mean the *Information Privacy Act 2014* (ACT).

medical device	means devices located in a Health Service such as heart rate monitors, dialysis machines, ultrasound technology, infusion pump at a Patient's bedside.
OAIC	means the Office of the Australian Information Commissioner.
Patient	means an individual receiving health services from a Health Service.
Patient Information	means a Patient's personal information (including personal health information) collected, used and disclosed in connection in connection with the Patient's access of a Health Service.
Patient Portal	means the portal that allows the Patient (and any Carer that is authorised) to access that Patient's DHR.
Patient's DHR	means the health record created for an individual in the DHR Solution.
personal health information	has the meaning given in at the dictionary in the Health Records Act.
personal information	has the meaning given in s 8 of the Information Privacy Act.
PIA	means this privacy impact assessment.
Territory	means the Australian Capital Territory.
TPP, or Territory Privacy Principle	has the same meaning as in the *Information Privacy Act 2014* (ACT).
URN	means the unique reference number assigned to a Patient by ACT Health.
User	User means an individual authorised to access the DHR Solution.
Wearables	means consumer owned wearable devices (such as, a 'fitbit') or any Health Services issued device for an outpatient service (such as, Holter Monitor or insulin pump).

Attachment 1 Diagram of information flows



Attachment 2 Material reviewed

1. ACT Health – *Digital Health Record Program Plan* [dated 27 August 2020].

2. ACT Health – *Project Initiation Document – DHR Implementation* [draft dated 22 December 2020].

3. ACT Health – *Project Initiation Document – DHR Technical Project* [draft dated 16 November 2020].

4. ACT Health – *Canberra Health Services Procedure (Clinical Record Management)* [dated 9 March 2018].

5. ACT Health – *Canberra Health Services Procedure (Confidentiality, Privacy and Access to Mental Health, Justice Health& Alcohol and Drug Services Clinical Records)* [dated 15 March 2018].

6. ACT Health – *Healthy Planet Strategy Handbook* [dated 11 November 2019].

7. ACT Health – *Care Everywhere Strategy Handbook* [dated 2 August 2019].

8. ACT Health – *Overview of Care Everywhere* [dated at November 2 2018].

9. ACT Health - *Patient Confidentiality Strategy Handbook* [dated 29 March 2017].

10. ACT Health – *Security Overview* [dated 15 April 2020].

11. ACT Health – *Manual Ambulatory Care* [dated 17 December 2020].

12. ACT Health – *Data Release Policy* [dated 30 January 2009].

13. *EPIC Guide to the General Data Protection Regulation* [dated 25 May 2018].

Attachment 3 Guidance on sharing information with external entities using Epic products

1. Purpose

1.1 As set out in 10.8 in **Part C** of this PIA Report, ACT Health is considering the potential for use of the EpicCare Link application and EpicCare Everywhere platform for sharing Patient Information with external providers who use those Epic products. In this Attachment we provide guidance from a best privacy practice perspective on issues and questions that ACT Health should consider before deciding whether to enable use of these products in conjunction with the DHR Solution.

2. EpicCare Link application

*2.1 **Overview***

2.2 Epic's "EpicCare Link" application is a web-based application that provides external health care providers with secure access to real-time Patient Information held in the DHR Solution. It enables external health care providers to access information in the DHR solution via a web platform. We understand that this application is likely to be used by providers who are members of a Patient's treating team outside of a Health Service (e.g. their general practitioner). Generally, EpicCare Link would not be used by persons outside of Australia.

*2.3 **Issues***

2.4 The table below outlines issues from a privacy perspective that we consider ACT Health should address:

Issue or Question to address	Comment
1. Informing Patients of the identity of any person or entity to which ACT Health will disclose their information through EpicCare Link	Patients should be given information so that they clearly understand who (e.g. treating general practitioner) may be able to access Patient Information in the DHR Solution, and what they can access.
2. Determine what Patient or other information it is necessary for external service providers to have access to, and ensure only access to that information is provided through EpicCare Link	HPP 6 provides that a health service provider who is a member of a treating team for a Patient may have access to the personal health information about the consumer **so far as necessary** for the provision by the provider of a health service to the consumer (our emphasis). ACT Health should be able to demonstrate to stakeholders that the deployment of EpicCare Link is based on consideration of the Patient or other information for which it is necessary for external service providers to have access. ACT Health should also consider whether, notwithstanding that in some circumstances 'consent' is not legally required before information can be disclosed to external service providers, it would be desirable to build in consent mechanisms which enable a Patient to consent to information being accessed by an external service provider (including for that consent to be withdrawn). Such consent mechanisms may be particularly helpful if there are questions about whether at any point in time an external service provider is a member of the Patient's treating team. For example,

Issue or Question to address	Comment
	a GP may check a Patient's DHR to see if there are any relevant diagnostic tests but may be doing so for another episode of treatment – obtaining Patient consent before providing access may assist in removing any doubt about whether there is a proper legal basis for the disclosure of the Patient's information.
3. Consider other technical features that can be put in place to minimise unauthorised access	We assume that external health care provider personnel will be able to search for relevant Patients by name and date of birth or combination of other information, to ensure they are reviewing the correct Patient DHR. ACT Health should consider whether there are other technical measures that may be put in place, for example, limiting search results to only Patients that are recorded in the DHR Solution as being Patients of the external health care provider, to reduce the risks of unauthorised access, including inadvertently, to a Patient's DHR. Another way for ACT Health to satisfy itself it has taken reasonable steps to draw attention to the obligations on the external services providers under the HPPs, may be to consider whether before an external service provider is able to access a Patient's DHR (or the EpicCare Link application), they should confirm or warrant they are doing because as they reasonably require information about a Patient who is also their patient.
4. Determine whether EpicCare Link will enable people to download information from a Patient's DHR (e.g. in PDF format)	Once a person downloads information from the DHR Solution, it is difficult for ACT Health to control the further use and disclosure of that information. ACT Health should consider whether it is necessary for external service providers to be able to 'download' any information (or whether information should only be able to be viewed within the DHR Solution). If downloading is deemed necessary, ACT Health should consider whether contractual or other obligations should be imposed upon recipient of the information (e.g. in relevant terms of use which must be agreed by the external user of the EpicCare Link, which could include statements about external service provider personnel accessing, downloading and using information only where they have a need to know that information in order to treat the Patient, and potentially restrictions on further disclosing the information unless the recipient is permitted under law.
5. Consider the feasibility of Patients being able to see the external service providers that have accessed their DHR, particularly in circumstances where a Patient's consent is not sought (because consent is not required).	For example, the My Health Record solution provides functionality to enable a person to see who has accessed their My Health Record. That solution has a 'My Record Access History' functionality, which shows: • the time and date that the record was accessed • which healthcare organisation or authorised person (e.g. nominated representative) accessed the record • the action that was taken in respect of the record (e.g. retrieve medicines information) • details of the Patient's own access to the record. My Health Record also allows persons to receive an email or SMS notification when a healthcare organisation has accessed their record for the first time, or in an emergency. ACT Health should consider the feasibility of implementing similar arrangements for the DHR Solution, as a privacy enhancing feature.

Issue or Question to address	Comment
6. A process to authenticate personnel from external services providers before using EpicCare Link, including mechanisms to cease access (for example, when personnel cease employment with an external service provider).	It is important that where a person no longer works for an external service provider that they no longer can access Patients' DHRs. to minimise the potential for misuse or unauthorised access to a Patient's DHR. ACT Health should consider its workflow processes with external service providers to determine ways to ensure that information about external service provider users with access to the DHR Solution through EpicCare Link is kept up to date.
7. Arrangements for the collection of personal information of external services providers	If ACT Health will be collecting the personal information of individual personnel of external service providers in order to give them access to EpicCare Link, ACT Health will need to ensure it has provided those individuals with appropriate collection notices for the collection, use and disclosure of this personal information (TPP 5).

3. EpicCare Everywhere platform

*3.1 **Overview***

3.2 Epic's "EpicCare Everywhere" platform facilitates the exchange of a Patient's DHR (that is, the whole record) with another organisation that also has an Epic digital health record system.

3.3 For example, the Royal Children's Hospital, Royal Melbourne Hospital, Royal Women's Hospital and Peter MacCallum Cancer Centre (all located in Parkville, Victoria) all use Epic digital health record systems to provide their electronic health records. EpicCare Everywhere would enable a Patient's electronic health record in one or more of these hospitals to be imported directly into a Patient's DHR; or alternatively for a Patient's DHR to be provided to one of the hospitals, for example, when a Patient is moving away from the Territory. This potential exchange of electronic health records would be subject to a Patient's specific consent.

3.4 As mentioned above, the EpicCare Everywhere platform facilitates transfer of information from, and to, an organisation (including located outside of Australia.)

*3.5 **Issues***

3.6 The issues and questions in the table in paragraph 2 above also apply in connection with the EpicCare Everywhere platform. In addition, the table below outlines further issues from a privacy perspective that we consider that ACT Health should address:

Issue or Question to address	Comment
1. Establishing the identity of the Patient	To ensure the DHR of the correct individual is exchanged, consideration will need to be given to how this will be achieved. We assume that Epic already has in place processes for this as part of the EpicCare Everywhere platform design. ACT Health will need to consider whether these processes involve the collection of new personal information about Patients (for example, if ACT Health will require the receiving entity's reference number for a Patient). If so, consideration will need to be given to whether this

Issue or Question to address	Comment
	additional information (for the purposes of facilitating exchange) is appropriate and will need to be retained.
2. Manner of obtaining Patient consent	There are four key elements that are needed in order to establish consent: • the individual is adequately informed before giving consent; • the individual gives consent voluntarily; • the consent is current and specific; and • the individual has the capacity to understand and communicate their consent. ACT Health will need to demonstrate that the four elements have been met. This will require ensuring there is adequate explanation of what the exchange of a DHR involves, for example in any information sheets or other available information for Patients. ACT Health should also consider the manner consent is collected and recorded, for example, whether consent will be provided through the signing of a paper form or through the Patient Portal.
3. Consent to disclosure of information overseas	The HPPs provide that a person can request a copy or written summary of their health record be provided to another health services provider, for example when the person has moved (HPP 12.1). However, the HPPs do not deal specifically with disclosures of personal health information to an overseas recipient. In contrast, TPP 8, in relation to personal information that is not personal health information, requires that an agency must take reasonable steps to ensure that the overseas recipient does not breach the TPPs (other than TPP 1) in relation to the information. TPP 8.2 includes an exception to this where: (i) the agency expressly informs the individual that if the individual consents to the disclosure of the information, TPP 8.1 will not apply to the disclosure; and (ii) after being informed, the individual consents to the disclosure. We suggest that stakeholders would have an expectation that the disclosure of personal health information to an overseas recipient would not be done in a manner which has lesser protections than that used for disclosure of personal information within Australia. However, we acknowledge that from a practical perspective it may be difficult for ACT Health to take steps every time a request is made for a Patient's DHR to be provided overseas, to ensure that the HPPs and TPPs will be complied with. If this is the case, any consent documentation where a Patient is seeking the disclosure of their DHR to an overseas recipient should reflect that ACT Health cannot confirm or ensure that the overseas recipient will comply with Australian privacy requirements (i.e. that the overseas recipient will not breach the HPPs or TPPs), and confirm that the Patient provides their consent on this basis.
4. Security issues	ACT Health needs to satisfy itself that the disclosure of a Patient's DHR to another entity (including one located overseas) will not introduce security vulnerabilities for the DHR Solution. ACT Health should also consider whether the platform keeps a copy of the information provided to another entity (noting that this may be data intensive, and more privacy intrusive) or alternatively the platform enables the recreation of the DHR that was provided

Issue or Question to address	Comment
	at a particular date (in case this is needed for any medico-legal purposes).
5. Quality of information	We understand certain parts of a Patient's DHR could be populated from another entity's electronic record (for example, medication lists) through this exchange via EpicCare Everywhere. ACT Health should consider whether, from a clinical perspective, it requires information that has been populated from outside of a Health Service needs to be flagged in some way in the DHR Solution so Clinicians are aware of this. We note that Clinicians are required to assess the quality of information in any health record, so it may be that after consultation ACT Health determines that this is not necessary.
6. Protocol for the exchange of a Patient's DHR	We suggest that ACT Health consider whether a specific protocol should be developed for the use of this platform and agreed with the relevant other entities before the platform is used to share DHRs with them. Such a protocol should as a minimum include: • how Patients can request their DHR to be provided to another entity; • who (if anyone) is responsible for ensuring the necessary information and consents from the Patient have been obtained (and recorded in the DHR Solution or another system) • who can authorise the exchange to occur (and where this is recorded in the DHR Solution or another system); and • where the ACT Health is the receiving entity, what checks will be done to ensure that there was no corruption in data in the transmission of information. We also understand that there is some concern about 'ownership' of health records (e.g. by the author or their employer), and any limitations about how a health record authored by one health service provider can be used by another. We assume this would be covered in the relevant Terms of Use of the platform by Epic, so any entity using the platform and exchanging a DHR provides the receiving entity with a right to use the information in the DHR that has been exchanged. We note that this is not strictly a 'privacy' issue but a copyright and other intellectual property rights issue. However, if this is not covered in the Terms of Use, then we suggest that the Protocol described above includes steps in relation to the liaison between ACT Health and another entity, including assurances about having obtained the Patient's consent for disclosure, and how the data 'owned' by an entity may be used by the other entity).