Information Privacy Procedure - State Wide Procedure

Document ID:	MPPL-04251	Version number:	3
Release date:	22 Jul 2021	Approval authority:	Chief Digital Officer

Table of contents

Affirmation

This governance document is consistent with Mater's Mission, Vision and Values.

1. Introduction

1.1 Purpose

This procedure sets out Mater's procedure in relation to the management of personal information.

1.2 Scope and context

This Procedure applies to all persons who have access to personal information collected by the Mater and all persons about whom personal information is collected.

1.3 Governing policy

Document ID	Document title
PY-IID-100016	Information Privacy Policy

2. Procedure requirements

The following procedures are to be followed.

2.1 Notification Statements

2.1.1 Notification of Collection of Personal Information Statements shall be displayed and copies made available in all public areas where collection of personal information occurs in addition to being available on the Mater internet and all consumer facing applications that collect personal information. Notification Statements may vary depending upon which Mater service is being provided. The general types of Notification Statements refer to Mater Health, Mater Education, Mater Research and Mater Foundation.

2.2 Collection of Personal Information

2.2.1. As a general rule, information should only be collected from the individual to whom the information relates.

2.2.2. Where information is collected from another source, reasonable steps must be taken to inform the individual that we have collected that information.

2.2.3. Only information necessary for providing services related to Mater functions should be collected.

2.2.4. Collection must be lawful, fair and not obtrusive. For example, it is not lawful to publish or disclose a recording of a private conversation made without the other party's consent. For fairness, the means of collection should be open/disclosed and not obtained by coercion.

2.2.5. Wherever possible, information must be collected in a private manner in a place where the parties cannot be overheard. If information is being collected in a public area staff must ensure that they lower their voices to suit the environment and remain conscious of the person's right to privacy.

2.2.6. Copies of identity documents (such as drivers' licence, passport etc) must not be stored at Mater. If a copy of identification is received, it should be reviewed to ensure it is a valid/certified copy. Once this has been completed, the person responsible for checking the identification should document in their local system:

- What document was received
- What date it was received
- Who checked the validity/certification of the document

The copy of the identification document should then be deleted if received electronically or discarded into a confidentiality bin if received as a paper copy. In rare circumstances, a department may need to store an identification document before it is confirmed. If this occurs, it must be saved in a file location which is access protected with limited access. The files must be destroyed once they have been reviewed and identity has been confirmed.

2.3 Use and Disclosure

2.3.1. Information collected by Mater shall only be used for the purposes for which it was collected or as otherwise required or authorised by law. Use for any purpose other than the purpose for which it was collected, including any other use by Mater staff, must be referred to the Manager Information Privacy. Mater is not entitled to use information collected from staff where those staff members were patients without the consent of the staff member or otherwise required or authorised by law. Mater is also not permitted to use information collected from one part of the business, e.g. health, in another part of the business e.g. Foundation, unless the person to whom the information relates has consented to that use. All requests for use or disclosure of information for a purpose other than the purpose of collection must be referred to the Privacy Office.

2.3.2. Mater may use de-identified information for quality improvement, service management, research and educational purposes.

2.3.3. Staff should take care when discussing health information not to do so within earshot of persons not permitted to share the information.

2.3.4. When discussing a patient's condition with a patient, staff should be careful to ensure that the patient is happy for any visitors or family members who are present to remain. Staff must not assume that patients are willing to share their health information with family members including partners.

2.3.5. Although staff may have the ability to access health or other information because of their access to computer systems or other records, staff are only authorised to access and use information where it is necessary for the purpose of providing a relevant Mater service.

2.3.6. Staff should not assume that they are entitled to use health information for research, study or academic performance. Staff wishing to use health information for research purposes will need approval from either the Privacy Office or the Research Governance Office depending on the circumstances. Initial inquiries may be made to either Office. Use of information for study or academic purposes shall be referred to the Privacy Office.

2.4 Privacy Status

2.4.1. In addition to privacy measures that are followed in the collection, use and disclosure of personal and sensitive information for all people, a person may request an additional level of privacy when they interact with the Mater. Appropriate processes are documented in the Patient Alert Procedure, Patient Alert Work Instruction and the Inpatient Privacy Work Instruction or advice can be sought from the Privacy Office.

2.5 Access to Personal Information

2.5.1. All requests for access to or use of information (except use for the purposes of providing the service for which the information was collected) shall be referred to the Privacy Office. The Privacy Office may authorise written work instructions providing for the disclosure of information by other Mater staff or business units.

2.5.2. In clinical situations, clinicians may discuss health information with patients but all requests for copies of information, including from inpatients, must be referred to the Privacy Office.

2.5.3. No Mater person may access their own health record or health information or record of any friend or family member. If a staff member needs to access such a record for work purposes, they should first inform the Manager Information Privacy. Staff who breach this requirement will be subject to disciplinary action which may include termination of employment.

2.5.4. Mater enables access to patient information held by third parties solely for the purpose of providing health care at Mater. This includes access to the Queensland Health Viewer, through Verdi, and access to the national My Health Record, through Verdi. All requirements of this procedure apply to accessing patient information held by third parties. There are separate rules relating to access to My Health Record found in the My Health Record Procedure.

2.5.5. All legal process documents including Subpoenas, Summonses to Produce Documents, Search Warrants, Notices of Claim, Notices of Non-Party Disclosure, Office of the Health Ombudsman requests, Police Requests/Summonses, Requests for Medical Reports, Coroner Requests for Information (other than as provided in the Deceased Patient – Processes and Management Procedure) must be forwarded to the Privacy Office for attention.

2.5.6. If a death at Mater is referred to the Coroner, a copy of the health record is to be made and forwarded to the Privacy Office. The original is to be sent to the Coroner together with print outs of any pathology and other information on computer systems that is not available in the health record.

2.5.7. Any person wishing to rely on a court order, power of attorney, notice of appointment of guardian or any other legal document for any purpose must produce the document for inspection and registration by the Privacy Office.

2.5.8. Except in emergency situations or formalised share care arrangements, health information is not to be provided verbally over the phone or in person, unless authorised by the Manager Information Privacy or other authorising staff member. All persons are required to establish the identity of the recipient prior to providing information over the phone and, where practicable, should make arrangements to call back the recipient to ensure the source of the call.

2.6 Consent

2.6.1. In general, information shall only be collected, used and disclosed with the consent of the person unless otherwise required or authorised by law.

2.6.2. Each of Mater Health, Education, Research and Foundation should develop the necessary mechanisms for collecting consent and withdrawal of consent for their areas of activity. Consent templates are to be reviewed by the Privacy Office.

2.6.3. All patients who receive a health service from the Mater, excluding members of the public who access Mater community pharmacies or pathology collection centres, must complete a Patient Information Consent Form.

2.6.4. The consent status of the Patient Information Consent Form must be entered into iPM or WebPAS and the Form must be added to the patient health record.

2.6.5. The consents on the Patient Information Consent Form are valid until the person chooses to revoke or change them. An additional or replacement Patient Information Consent Form only needs to be completed by the patient where:

- The patient chooses to change their consent status, or
- The patient reaches the ages of 18 years of age, or
- A new version of the Patient Information Consent Form is released

2.6.6. The wishes expressed by the patient on the Patient Information Consent Form in relation to the use of their information must be adhered to. The consent status from the patient must be known and applied before their personal information can be used for the secondary purposes outlined on the form.

2.6.7. If a current Patient Information Consent Form is not completed by a patient, then their previous consent status continues to apply, or where no consent status has been previously collected, information cannot be used for the secondary uses outlined in the Form.

2.7 Correction

2.7.1. Mater has an obligation to take reasonable steps to ensure that personal information is accurate, complete and up to date. Where staff are requested to update personal demographic information by the person or their care giver, they may do so by entering the information into the appropriate system. All requests to correct other personal information, including health information, must be referred to the Privacy Office and should be in writing.

2.7.2. The Privacy Office will liaise with the appropriate service to investigate the authenticity of the information and facilitate any correction required.

2.7.3. No person may destroy or erase health information. Where it is necessary to correct a paper record, the incorrect part should be ruled through and a note added in the margin indicating when the record was amended, by whom it was amended and, where relevant, the reason for amendment. In electronic systems, a note must be made specifying that information is incorrect.

2.8 Information Classification, Protection and Privacy Breaches

2.8.1. All information collected and obtained by Mater must be assigned an applicable information classification so that it is managed and secured in a manner appropriate with its sensitivity and importance, in accordance with the Information Classification Procedure.

2.8.2. Mater has an obligation to protect the information it holds from misuse and loss, as well as from unauthorised access, modification or disclosure. If personal information is not securely stored and managed there is an increased risk of privacy breaches. Steps must be taken to protect information against both accidental loss and intentional breach.

2.8.3. All staff shall immediately notify the Privacy Office if they become aware of any privacy breaches or if they suspect that there has been a privacy breach, in addition to logging an incident on the incident reporting system. Mater has a procedure for Managing a Mandatory Data Breach Incident.

2.8.4. Physical records and information shall be transported and stored in a manner which does not disclose the personal details of the person. Other than for the purpose of providing

healthcare, health information must not be transferred outside of the Mater unless authorised by the Privacy Office. Transmission must be by approved secure means.

2.8.5. All regular or ongoing reporting of personal information to an external agency must be authorised by the Privacy Office to ensure all privacy and security requirements are met and recorded on the External Reporting Register.

2.8.6. Personal Information is not to be transmitted by email unless the information is secured in a manner satisfactory to the Chief Digital Officer. Mater has secure email connection to Queensland Health and to various other organisations.

2.8.7. In order to ensure the protection and confidentiality of personally identifiable information, it may not be appropriate for personally identifiable information to be stored in certain media or in certain systems as advised by the Privacy Office.

2.8.8. Personal Information which is no longer needed must be securely destroyed in a manner approved by the Manager Information Privacy. Personal information is not to be deposited in general wastepaper bins and must be placed in secure bins.

2.9 Privacy Impact Assessments

2.9.1. For all projects, initiatives or organisational changes involving the handling of information a Privacy Impact Assessment must be completed as per the Privacy Impact Assessment Procedure.

3. Definitions

Term	Definition
Demographic details	Patient demographic details uniquely identify the patient and describe the administrative type data that is collected for the purposes of providing health services to the patient. Patient demographic details include: name, date of birth, gender, address, alternate patient identifiers, GP information, Next of kin and emergency contact, Medicare information, insurance details, compensable information, country of birth, marital status, language spoken, indigenous status, religion, consent information and patient alerts. Patient demographic details, along with the patient UR number, form the Patient Master Index (PMI).
Health Information	means: a) information or an opinion about: i. the health, including an illness, disability or injury, (at any time) of an individual; or ii. an individual's expressed wishes about the future provision of health services to the individual; or iii. a health service provided, or to be provided, to an individual; iv. that is also personal information; b) other personal information collected to provide, or in providing, a health service to an individual; c) other personal information collected in connection with the donation, or intended donation, by an individual of his or her body parts, organs or body substances; d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.
Mater	Mater means all services operated by Mater Misericordiae Limited as well as Mater Education Limited , Mater Research and Mater Foundation
Mater People	The term Mater People may refer to one or more individuals. The term 'Mater person' is the singular of 'Mater People'. Mater people incudes all employees, visiting medical officers, students enrolled through Mater Education or who are on a placement at a Mater Facility, contracted service providers or such other persons who provides services on behalf of the Mater.
Personal Information	Means information or an opinion about an identified individual, or an individual who is reasonably identifiable: a) whether the information or opinion is true or not; and b) whether the information or opinion is recorded in a material form or not
Sensitive Information	a) information or an opinion about an individual's: i. racial or ethnic origin; or ii. political opinions; or iii. membership of a political association; or iv. religious beliefs or affiliations; or v. philosophical beliefs; or vi. membership of a professional or trade association; or vii. membership of a trade union; or viii. sexual orientation or practices; or ix. criminal record; that is also personal information; or b) health information about an individual; or c) genetic information about an individual that is not otherwise health information; or

Term	Definition
	d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or e) biometric templates

4. Documents related to this procedure

Mater documents

Type	Document ID	Document Title
Policy	PY-IID-100016	Information Privacy Policy
Procedure	PR-IID-000016-01	Managing a Notifiable Data Breach Incident
	PR-IID-100047	Privacy Impact Assessment Procedure
	PR-IID-100061	Information Classification Procedure
	PR-DTI-100000	My Health Record Procedure
	PR-IID-100035	Patient Alerts Procedure
	PR-IID-100042	Patient Registration, URN and Demographic Details Procedure
Guideline	GD-DTI-100032-02	Guidelines for the appropriate use of Corporate Collaboration Platforms
Work Instruction	WI-IID-100016 WI-DTI-100059	Privacy Office Work Instruction Inpatient Privacy Work Instruction
Clinical Form		Patient Information Consent Form
Corporate Artefact	CA-IID-100010	External Reporting Register Personal Information Collection Notification Statements
Non-Clinical Form	NF-IID-100015	Patient Health Information Request Form

External documents

1.	The Privacy Act 1988 (Cth)
2.	Privacy Amendment (Enhancing Privacy Protection) Act 2012
3.	Guidelines from the Australian Information Commissioner on the application of the Australian Privacy Principles
4.	Australian Commission on Safety and Quality in Health Care. National Safety and Quality Health Service Standards. 2nd ed. Sydney: ACSQHC; 2017.(1.16)

5. Document controls

5.1 Document revision history

Version	Release date	Description	Risk-rated Review date
1.	07 Mar 2014	Release of version 1 within MDC	
1.1	16 Oct 2017	Release of version 1.1 with administrative changes and updates	
2	16 Oct 2018	Release of this version; capturing changes as follows: • Requirement for the Notification of Collection of Personal Information Statement to be available on all public facing applications that collect personal information. • Addition of access to patient information held by third parties. • Updating of the consent section to reference the Patient Declaration and Consent Form. • Addition of the Patient Information External Reporting Register.	
2.1	19 Jul 2019	Formating issues rectified	
3	22 Jul 2021	Released as version applicable to all Mater ministries and locations. Changed references from Patient Declaration and Consent Form to Patient Information Consent Form.	

5.2 Document review and approval

Name Person/committee	**Position** If applicable	**Function** Owner/author/review/approve
Alastair Sharman	Chief Digital Officer Owner	Document owner / approve
Sallyanne Wissmann	Director Information Management	Document author
Anne-Maree Schneider	Manager Information Privacy	Review
Justin Sharp	Consultant, Rogencamp & Co Lawyers	Review
	Mater Leadership Team	Endorse

5.3 Keyword indexing

Keywords:	privacy, Privacy Act, personal information, patient declaration, external reporting, APP