**NOTE:**

This template is provided by the Office of the Information Commissioner (OIC) as an example of the content that is typically included in a PIA Report. It is a guide only. You may need to adapt the template to meet your agency’s needs or build on the template to include additional information due to the size and complexity of the project.

If you are unsure whether to complete a Privacy Impact Assessment (PIA), you can complete the screening questions in OIC’s [Threshold Privacy Assessment](https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/overview-privacy-impact-assessment-process/undertaking-a-privacy-impact-assessment). If you answer yes to any of the questions, the project will benefit from a PIA.

This template is based on the National Privacy Principles (NPPs) and as such, is suitable for use by health agencies, i.e. a Hospital and Health Service (HHS) or the Department of Health (Queensland Health). If your agency is not a health agency, please use the template which is based on the Information Privacy Principles.

Instructions and tips for completing the report are provided in blue italicised text. Please delete this text as you complete each section.

Alternatively, the Department of Health has a tailored Threshold Privacy Assessment tool focussing on personal information and confidential information. To access this resource, please contact the Privacy and Right to Information Unit, Department of Health at RTI-Privacy@health.qld.gov.au or (07) 3082 0546.

Feedback on suggested improvements to this template or your experience using the template is most welcome. Please send feedback to enquiries@oic.qld.gov.au or contact OIC’s Enquiries Service on (07) 3234 7373.

<Project name>

**Privacy Impact Assessment Report**

<Day> <Month> <Year>

## **Document information**

|  |  |
| --- | --- |
| Date PIA completed: |  |
| Status: | [ ]  New PIA  | [ ]  Update. Date of previous version:  |
| Prepared by: |  |
| Position: |  |
| Email:  |  | Telephone: |  |

## **Endorsement and approval**

Project manager:

I **recommend** the project proceeds as proposed in this document.

|  |  |
| --- | --- |
| 1. Name:
 |  |
| 1. Position:
 |  |
| 1. Signature
 |  | 1. Date:
 |  |

The following officer/s have **endorsed** this document:

|  |  |
| --- | --- |
| 1. Name:
 |  |
| 1. Position:
 |  |
| 1. Signature
 |  | 1. Date:
 |  |

*Add further names as required*

Project Executive/Steering Committee/senior management:

I **agree** to the project proceeding as proposed in this document.

|  |  |
| --- | --- |
| Name: |  |
| Position: |  |
| Signature |  | 1. Date:
 |  |
| 1. Comments:
 |

**Table of Contents**

[**Document information** 2](#_Toc159401808)

[**Endorsement and approval** 2](#_Toc159401809)

[**1** **Introduction** 4](#_Toc159401810)

[**1.1** **Purpose** 4](#_Toc159401811)

[**1.2** **Applicable legislation** 4](#_Toc159401812)

[**1.3** **Project description** 4](#_Toc159401813)

[**1.4** **Scope of the PIA** 4](#_Toc159401814)

[**1.5** **Review** 4](#_Toc159401815)

[**2** **Information flows** 5](#_Toc159401816)

[**3** **Risk analysis** 7](#_Toc159401817)

[**3.1** **Personal information – *Information Privacy Act 2009* (Qld)** 7](#_Toc159401818)

[**3.2** **The *Hospital and Health Boards Act 2011* (Qld) (HHB Act) and *Human Rights Act 2019* (Qld)** 13](#_Toc159401819)

[**3.3** **Risk ratings** 15](#_Toc159401820)

[**4** **Actions to address the identified risks** 16](#_Toc159401821)

[**5** **Stakeholder consultation** 17](#_Toc159401822)

[**6** **PIA outcomes** 18](#_Toc159401823)

[**6.1** **Agreed recommended actions** 18](#_Toc159401824)

[**6.2** **Action plan** 18](#_Toc159401825)

[**6.3** **Contact point for future enquiries** 18](#_Toc159401826)

## **Introduction**

## **Purpose**

This Privacy Impact Assessment (PIA) Report:

* identifies possible impacts on:
	+ the privacy of individuals' personal information;
	+ confidentiality of patient information;
	+ legislative compliance requirements; and
* recommends options for mitigating or minimising any negative impacts.

## **Applicable legislation**

This PIA analyses the impacts of collecting, storing, using and disclosing personal information for the purposes of <the project> against the privacy principles set out in the *Information Privacy Act 2009* (Qld) (IP Act) and the confidentiality obligations in part 7 of the *Hospital and Health Boards Act 2011* (Qld) (HHB Act) relating to the disclosure of confidential information (i.e. patient information).

*If there is other legislation that explicitly requires, permits or limits the collection, use or disclosure of personal information and/or confidential information that relates to this project, you should also cite the legislation and relevant sections within that act.*

## **Project description**

*Explain the project and what it intends to achieve by addressing the following key points:*

* *what the project will deliver*
* *why the project is needed*
* *the benefits to the agency or the community; and*
* *whether the project is part of a program of related projects.*

*The term ‘project’ is used broadly in this context. It is intended to cover the full range of activities and initiatives that may have privacy or confidentiality implications, such as new systems, processes or practices for handling personal information, confidential information, new legislation or policies, or information sharing initiatives.*

## **Scope of the PIA**

*If applicable, explain what part or stage of the project the PIA covers and, if necessary, what it does not cover.*

## **Review**

*In the case of a large or complex project, the PIA may need to be reviewed a number of times throughout the project’s lifecycle to ensure that its findings continue to be relevant. If applicable, outline any dates or milestones that will be used as a checkpoint to review whether anything significant has changed since this PIA was last completed, reviewed and/or updated.*

## **Information flows**

This section explains how personal information and/or confidential information will flow through the agency’s systems and processes as a result of the output or deliverable to be produced by the project. It describes:

1. what personal information will be collected, used and disclosed
2. what confidential information will be disclosed
3. who will have access to this information; and
4. how it will be stored and protected.

*Describe what personal information and/or confidential information is involved and document the flow of this information through the proposed systems and processes. This includes how the information will be handled after the project’s output or deliverable has been implemented and responsibility has been handed over to the relevant business unit. For example:*

* *What is the nature of the information being collected and who is it collected from? For example, is the information collected directly from the individual, or will it be sourced from an internal system or from outside the HHS/agency (such as another HHS?)?*
* *How will the information be collected?*
* *How will it be stored and what safeguards will be put in place to protect it?*
* *Who will have access to the information?*
* *What will the personal information be used for and by whom?*
* *Will the personal information be routinely disclosed and if so, to whom will it be given and for what purpose?*
* *How can individuals seek access or amendment to their personal information?*
* *How long will the information need to be retained?*

*Keep in mind that* ***personal information*** *includes any information or opinion about a living individual who is or can reasonably be identified[[1]](#footnote-2). However,* ***confidential information*** *most often relates to patients of Queensland Health, and includes deceased persons.[[2]](#footnote-3)*

*There is no ‘one size fits all’ approach to documenting the flow of information. The following table is one example of how you could describe the information flows. You may prefer to use a diagram or business process map. The approach will depend on the complexity of the project’s information flows.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Business process/activity***(For example, an individual applies for permit or licence)* | **Components of personal information***(For example, name, date of birth, address)** *List any components of confidential information if needed.*
 | **Collection*** *From?*
* *By who?*
* *How?*
* *Lawful authority (if any)?*
 | **Storage*** *How?*
* *Where?*
* *By who?*
* *For how long?*
 | **Use*** *By who?*
* *Why?*
* *How?*
* *When?*
* *Lawful authority (if any)?*
 | **Disclosure*** *By who?*
* *To?*
* *Why?*
* *How?*
* *When?*
* *Lawful authority (if any) - for example, disclosure of confidential information.*
 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## **Risk analysis**

## **Personal information – *Information Privacy Act 2009* (Qld)**

*The following table summarises the key requirements of each privacy principle and outlines key questions to help you to identify potential privacy risks. This list is not exhaustive, but gives an indication of the types of questions you could consider.*

|  |  |  |
| --- | --- | --- |
| **Privacy principles** | **Proposed information handling practices** | **Identified risks** |
| **Collection of personal information (NPPs 1 and 8)*** Collect only that personal information which is necessary for one or more functions or activities of the health agency.
* Where lawful and practicable, give individuals the option of not identifying themselves when they transact with you.
* Collect personal information from the individual concerned unless it is not reasonable or practicable to do so.
* Inform the individual of what will happen with their information, of any applicable laws and of any third parties the information will be given to.
* Obtain personal information lawfully and fairly and in a way that is not unreasonably intrusive.
* Take steps to ensure the information is accurate, complete and up-to date.
 | *For example:* * *What business process or function is enabled by collecting this information?*
* *How is the collection of each piece of personal information necessary for this purpose?*
* *Are there any laws that require or authorise the agency to collect this information? If so, include details of the legislation and the relevant section and a description of the information to be collected. Include only those laws that create an explicit authority or obligation for your agency to collect personal information, rather than legislation that broadly details the nature and extent of the agency’s responsibilities and powers.*
* *What reasonable steps will be taken to ensure individuals are aware of the following information (often referred to as a ‘collection notice’ or ‘privacy notice’:*
* *identity of the health agency and how to contact it*
* *the fact that the individual is able to gain access to the information*
* *the purposes for which the information is collected*
* *any law that requires the particular information to be collected*
* *the entities to whom their personal information will be routinely disclosed; and*
* *the main consequences, if any, of not providing this information?*
* *Will this collection/privacy notice be given at this time of collection? If not, why it is not practicable to do so? Is the collection/privacy notice easy to understand and can it be easily accessed by the individual?*
* *Will personal information be collected directly from the individual it is about? If not:*
* *why it is not reasonable and practical to do so?*
* *what reasonable steps will be taken to provide the individual whom the information is about with a collection notice or do you intend to rely on one of the exemptions in NPP 1(5)?*
* *Will the information be sourced from an internal system? If yes:*
* *Will the personal information be used for the same purpose for which it was originally collected? If not, what exemption in NPP2 will be relied upon to effect this secondary use?*
* *Is the personal information being collected for more than one purpose (e.g. demographic information that is collected that will be used to improve customer engagement)? If so, how will an individual know what information will be used for which purpose?*
* *Is the individual likely to be upset by the way in which their personal information will be collected? If so, is the collection unreasonably intrusive?*
* *Can individuals choose to not identify themselves when interacting with the health agency for a purpose other receiving a health service[[3]](#footnote-4)? If not:*
* *Why is it impracticable or unlawful to allow the individual to remain anonymous or to use a pseudonym?*
* *Will individuals be required to verify their identity? If so, do their identification documents need to be recorded or just sighted?*
 | *Common risks may include:** *Personal information is collected without a clear purpose, which could increase the risk of scope creep or unauthorised use.*
* *Information collected is either unnecessary or excessive.*
* *Individuals are not aware of how their personal information will be used, or to whom it will be routinely disclosed, which can lead to a lack of trust.*
* *Collection notices are not consistently provided, for example, across all communication channels.*
* *Information is collected unfairly because the individual provides information that they would not have, had they known they had a choice not to provide it.*
* *Collection methods may be unjustifiably intrusive.*
* *Personal information collected from a third party may be of poor quality, as the affected person does not have the opportunity to check the data for accuracy.*
 |
| **Collection of sensitive information (NPP 9)*** ‘Sensitive information’ (i.e. health information or information about an individual’s racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, trade union membership, sexual preferences or practices or criminal record) can only be collected under limited conditions.
 | *For example:* * *Will sensitive information be collected? If yes:*
* *is it health information necessary to provide a health service to the individual and*
	+ *would the individual reasonably expect the health agency to collect the information for that purpose; or*
	+ *is the collection of information authorised or required by law?*
* *Is it other sensitive information? If so, what circumstances in NPP 9(1) permit this collection? For example:*
* *NPP 9(1)(a): the individual has consented*
* *NPP 9(1)(b): the collection is required by law*
* *NPP 9(1)(c): the collection is necessary to prevent or lessen a serious threat to the life, health, safety or welfare of an individual, and the individual is physically or legally incapable of giving consent; or physically can not communicate*
* *NPP 9(1)(e): the information is a family medical history, social medical history or other relevant information that is collected for the purpose of providing a health service and is collected from:*
	+ *the person who is to receive or is receiving the service*
	+ *a parent of the relevant individual*
	+ *a child or sibling of the relevant individual if the child or sibling has capacity*
	+ *a spouse or de facto partner of the relevant individual*
	+ *a relative of the relevant individual if a member of the relevant individual's household*
	+ *a guardian of the relevant individual*
	+ *a person exercising a power under an enduring power of attorney made by the relevant individual that is exercisable in relation to decisions about the relevant individual's health*
	+ *a person who has sufficient personal interest in the health and welfare of the relevant individual; or*
	+ *a person nominated by the relevant individual to be contacted in case of emergency.*
 |  |
| **Note:***If you are disclosing ‘confidential information’ (i.e. patient information) as defined in the HHB Act, you will also need to complete section 3.2 of this PIA, as the available exceptions that may authorise the disclosure of confidential information are confined to the HHB Act.  Where the disclosure of confidential information is authorised under the HHB Act, the health agency will satisfy its obligations under the IP Act by relying on the exemption in NPP 2(f) that permits the disclosure of personal information where it is authorised or required by law.**When completing the following section, keep in mind that ‘personal information’ as defined in the IP Act can be any information or opinion about an identifiable living individual; including staff, patients and the community more broadly.  This includes, but not limited to:-* * *Personal information about an individual that was provided by someone else (i.e. a patient provides a family medical history, next of kin details)*
* *Staff information such as a work email address, a work phone number, a work classification, a professional opinion given wholly in a professional capacity, etc.*
 |
| **Limits on use and disclosure (NPP 2)** * Personal information can only be used and disclosed for the **primary** purpose for which it was collected.
* Use and disclosure for a **secondary** purpose is not permitted except where the use or disclosure falls within the exceptions listed in NPP 2.
 | *For example:* * *Will the personal information be routinely disclosed outside the service/agency (for example, to another HHS or from a HHS to the Department of Health, and vice versa?) If yes, how and why is this information being disclosed? What reasonable steps will be taken when collecting the personal information to make the individual who the information is about aware of this disclosure (as required under NPP 1)?*
* *What process will be followed when a request is made to use or disclose personal information for a secondary purpose? How will you ensure that one of the permitted exemptions in NPP 2 is satisfied? For example:*
* *use or disclosure by or for a law enforcement agency*
* *where authorised or required under a law*
* *where the individual has expressly or impliedly agreed; or*
* *use or disclosure for research or statistical purposes.*
* *Will consent be relied upon to use or disclose the information? If yes, will you be relying on implied or express consent?*
* *If you are relying on implied consent, what are the facts and circumstances of the particular situation that support an assumption of the individual’s consent?*
* *If you will be seeking express consent from the individual concerned, how will you ensure their consent is valid, i.e. that it is voluntary, informed, specific and current? What mechanisms will be in place to accommodate an objection to the proposed use or disclosure? Will individuals be permitted to opt out if they change their mind and if so, how?*
 | *Common risks may include:** *Function creep – information collected for one purpose is then used for another purpose.*
* *Information is disclosed in circumstances not permitted under the IP Act. If found to be in breach of the IP Act, there is capacity for an individual to be awarded up to a maximum of $100,000 in compensatory damages.*
* *Individuals are surprised or upset by a secondary use, which can lead to a privacy complaint, a lack of trust or negative publicity.*
* *An individual’s refusal of consent, or conditional consent, is not respected.*
 |
| **Data quality (NPP 3)*** Take reasonable steps when collecting, using or disclosing personal information to make sure the information is accurate, complete and up to date.
 | *For example:* * *What reasonable steps will be taken to ensure the information is accurate, complete and up to date at the time it is collected?*
* *Has the information been supplied by the individual directly? If not, can it be checked with the individual who it is about?*
* *What reasonable steps will be taken to ensure the information is accurate, complete and up to date before it is used or disclosed? (Tip: It may not be reasonable to assume that the personal information was accurate at the time it was collected.)*
* *How will you know when the personal information was last updated?*
* *Is it information that is likely to change over time (such as an address) or information that is static (such as a date of birth)?*
* *How damaging will it be to the individual if information that is inaccurate, incomplete or out of date is acted upon? (The more damaging it will be, the more rigorous the steps should be to check its accuracy.)*
* *Is there any opportunity for individuals to routinely correct or update their personal information or to verify its accuracy?*
 | *Common risks may include:** *Incomplete, inaccurate or out-dated information lead to incorrectly informed decisions, which in turn may have a negative impact on the individual concerned.*
* *Inadvertent disclosure of personal information if the agency sends correspondence using incorrect or out of date contact information.*
 |
| **Data security (NPP 4)*** Take reasonable steps to protect personal information from misuse, loss and unauthorised access, modification or disclosure.
* If the personal information is no longer needed, take reasonable steps to de-identify the information. Depending on the nature of the personal information, how it is stored, the format/medium, and the agency’s obligations under the *Public Records Act 2002* (Qld), this may include destruction or de-identification.
 | *For example:* * *What steps will be taken to protect the personal information from misuse, loss and unauthorised access, modification or disclosure – while in transit and at rest? Has the project considered operational (e.g. policies or training), technical (e.g. access controls or encryption) and physical controls (e.g. doors or locks)? Are these safeguards adequate to provide the level of protection that can reasonably be expected to be provided? Can you reference any standards or documents that support the chosen controls?*
* *Will you be emailing clinical or sensitive information? The Queensland Health information security control for the electronic transmission of ‘CLINICAL-IN-CONFIDENCE’ information (that is, patient information) is that it should be encrypted.*
* *How will access be controlled? Who will authorise access? What process will be used to grant access? How will access be changed or revoked when the user leaves or their role changes? Will access be audited regularly?*
* *What measures will be in place to prevent and detect misuse or unauthorised access? For example – will audit logs enable actions to be linked to individuals and will these logs be reviewed on an ongoing basis?*
* *What training and awareness is necessary to ensure that staff are aware of their privacy and confidentiality obligations, as well as the agency’s security policies and practices?*
* *Can the personal information be accessed remotely? Can users access or save the personal information to their personal device? If yes, what controls will be in place?*
* *Is there a testing or training environment? If yes, is real or dummy data used?*
* *What steps will be taken to ensure that the individual the subject of the information can no longer and cannot not in the future, be identified from personal information that is no longer needed for any purpose?*
 | *Common risks may include:** *Access is not limited to the ‘need-to-know’ requirement.*
* *System users with administrative privileges is not limited to staff requiring those privileges.*
* *Access is not revoked promptly when no longer required.*
* *Unencrypted clinical and/or sensitive information is electronically transferred (e.g. sent by email), making it vulnerable to interception by unauthorised parties.*
* *The system does not log who has accessed a file, making it difficult to detect or investigate unauthorised access or misuse.*
* *Staff are unaware of their privacy, confidentiality and security obligations.*
* *Information is saved onto privately-owned storage devices, increasing the risk of loss, unauthorised access or disclosure.*
* *Personal and confidential information is kept for longer than required under approved retention and disposal schedule/s.*
 |
| **Openness, access and amendment of documents containing personal information (NPPs 5, 6 and 7)*** On request by a person, you must take reasonable steps to let the person know, generally, what sort of personal information you hold, for what purposes and how it is collected, held, used and disclosed.
* Inform the public about what sort of personal information you hold and how it is used and how to request access to or amendment of documents containing their personal information.
 | *For example:* * *Will requests from individuals for access to, or amendment of, documents containing their personal information be handled as a formal application under the IP Act or can the request be handled administratively?*
* *Will the project allow information to be amended if it is inaccurate, irrelevant, incomplete, out of date or misleading? If information cannot be altered, what mechanism will be in place for a notation to be attached?*
* *If information is held by a contracted service provider, how can your agency get it back when you need it?*
* *Will your agency’s list of personal information holdings need to be updated in light of this project? If yes, you should*
* *If yes,* [*contact the relevant Privacy and Confidentiality Contact Officer in your HHS*](https://www.health.qld.gov.au/system-governance/contact-us/access-info/privacy-contacts/default.asp) *or for the Department of Health, the Privacy and Right to Information Unit via email at* RTI-Privacy@health.qld.gov.au *to discuss the relevant changes.*
 | *Common risks may include:** *Individuals are not able to easily access or amend their personal information.*
* *An individual’s access to their personal information may be hampered if the data is held by a contracted service provider.*
* *An individual’s lack of access to their personal information increases the risk of inaccurate or out-dated information.*
* *The Privacy Plan does not accurately reflect the types of personal information held by the agency or its information handling practices. This reduces its effectiveness in terms of helping an individual to find out what information is held about them or how their personal information is managed and protected.*
 |
| **Transfer of personal information outside Australia (section 33)**Do not transfer personal information outside Australia unless: * the individual agrees to the transfer
* there is legal authority for the transfer
* it is necessary to prevent or lessen a serious threat to life, health, safety or welfare; or
* at least two of the criteria in [section 33(d) of the IP Act](https://www.oic.qld.gov.au/annotated-legislation/ip/chapter-2/part-3/33-transfer-of-personal-information-outside-australia) are satisfied.
 | *For example:* * *Will personal information be transferred outside Australia? For example – collected using an online survey tool or stored (including back-ups) with a cloud-based service or that uses servers physically located overseas? Or, could information potentially be accessed from outside Australia, for example, where information is posted on a website or social media site? If so, what provision in section 33 of the IP Act will be relied upon to permit this transfer?*
* *If the exemption in section 33(a) will be relied on, how will you ensure their agreement is valid, i.e. that it is voluntary, informed, specific and current? What mechanisms will be in place to accommodate an objection to the secondary use or disclosure? Will individuals be permitted to opt out if they change their mind and if so, how?*
* *If the exemption in section 33(d) will be relied on, what evidence can be provided to show that the requirements of this exemption have been satisfied?*
 | *Common risks may include:** *Personal information transferred outside Australia is not afforded the same of privacy protections as are in Queensland’s IP Act.*
* *Individual does not wish for their information to be transferred outside Australia.*
* *An individual’s refusal of consent, or conditional consent, is not respected.*
* *Relying on a ‘collection notice’ to obtain an individual’s agreement to transfer their personal information outside Australia where the individual has no choice in whether to participate.*
 |
| **Use of contracted service providers (chapter 2, part 4)*** Take all reasonable steps to bind a contracted service provider to compliance with the privacy principles.
 | *For example:* * *Will the project involve contracting an external service provider to provide a service for the purpose of performing a function of the agency? And is this service provided directly to the agency, or to a third party of behalf of the agency? If so, will the provision of services under the contract or arrangement involve the exchange or handling of personal information in any way? If yes:*
* *What steps will your agency take to ensure that the service provider is bound to comply with the privacy principles? Note – even if the service provider is subject to the Commonwealth Privacy Act 1988 you must still take all reasonable steps to bind them to Queensland’s IP Act as the obligations in the Commonwealth legislation do not apply to a contracted service provider for any acts or practices it undertakes in relation to a State Government contract.*
* *Have you considered additional contractual provisions, such as limiting secondary use, placing conditions on the use of sub-contractors or mandatory reporting of any breaches?*

*It is recommended that you contact your procurement unit and/or legal services unit to ensure the contract includes clauses/provisions to bind the service provider appropriately. You can also refer to the standardised procurement templates available on QHEPS.* | *Common risks may include:** *Reliance is placed on a whole of government contract or agreement that only binds the service provider to the Information Privacy Principles and not the NPPs.*
* *Existing government Information Technology Contracting (GITC) framework contracts may not adequately address the privacy risks of this particular project.*
* *The standardised contracts in the Queensland Information Technology Contracting (QITC) framework may not adequately address the privacy risks of this particular project.*
* *If the contractor has not been appropriately bound to comply with the IP Act and HHB Act, the contracting health agency will be liable for any breaches arising from the actions of the service provider.*
 |

## **The *Hospital and Health Boards Act 2011* (Qld) (HHB Act) and *Human Rights Act 2019* (Qld)**

*The IP Act governs the collection and handling of personal information by agencies, but it is not the only limitation on how agencies deal with information. The Human Rights Act 2019 (Qld) (HR Act) contains a right to privacy and a right to access government information. Additionally, the HHB Act governs 'confidential information’, defined in the HHB Act to include information from which a person who is receiving or has received a public sector health service could be identified, including deceased persons.*

*Confidential information most often relates to patients of Queensland Health. For further information on the duty of confidentiality and the circumstances when confidential information by disclosed, please refer to the Department of Health’s* [*Confidentiality General Principles*](http://qheps.health.qld.gov.au/governance/privacy-rti/docs/confidentiality_guidelines.pdf)*. If you require assistance in completing this section of the report, please consult with the Privacy and Confidentiality Contact Officer and/or the Human Rights officer.*

|  |  |  |
| --- | --- | --- |
| **Act** | **Proposed information handling practices** | **Identified risks** |
| **The HHB Act - prohibited disclosure of confidential information** Confidential information must not be disclosed by a designated person[[4]](#footnote-5) unless one of the permitted exceptions applies.* Confidential information must not be disclosed by a prescribed health practitioner unless one of the permitted exceptions applies.
* Designated persons or prescribed health practitioners must not disclose, either directly or indirectly, confidential information to another person (including to other ‘designated persons’ or ‘prescribed health practitioners’) unless the disclosure is required or permitted under the HHB Act.
 | * *Will the project require disclosing (whether directly or indirectly) confidential information that would identify a person who has received a health service (past, present, or deceased)? If yes, what permitted exception will be relied upon to disclose the confidential information? For example, common exceptions include:*
* *s143: the disclosure is required or permitted by an Act or law*
* *s144: consent will be obtained from the patient to disclose their confidential information in the manner proposed*
* *s145: the purpose of disclosure is for the care or treatment of the person to whom the information relates*
* *s149: the disclosure and receipt of the confidential information to another designated person is to give effect to or manage a funding arrangement for a public sector health service or for analysing, monitoring or evaluation public health and the other designated person is authorised in writing by the Director-General (or a delegate) to receive the confidential information*
* *s150(a): the disclosure is to another designated person for evaluating, managing, monitoring or planning health services*
* *s150(b): the disclosure is to a prescribed external entity for evaluating, managing, monitoring or planning health services*
* *s151: the disclosure is to the Commonwealth or another State, or an entity of the Commonwealth or another State, and the disclosure is required or allowed under an agreement or in writing by the Director-General (or a delegate) that it is considered to be in the public interest; or*
* *s161A and s161B: access is necessary to enable an external service provider to provide a health service under an agreement between the Director-General (or a delegate) and the service provider.*

*Part 7 of the HHB provides further exceptions that authorise the disclosure of confidential information. Some of the less common exceptions, include: s146, s147, s148, s150A s152, s153, s154, s155, s156, s157, s158, s159, s160, s161 and s161C of the HHB Act.**Where relevant, please ensure you detail and indicate whether the proposed disclosure will be undertaken by the Department of Health/HHS or a prescribed health practitioner.* | *Common risks may include:** *It is an offence to disclose confidential information about a person unless one of the exceptions in Part 7 of the HHB Act applies.*
* *If a staff member discloses identifiable patient confidential information in contravention of part 7 of the HHB Act; this will be a breach of confidentiality and could result in staff receiving a monetary penalty (maximum penalty – 100 penalty units).*
* *A breach of confidentiality may also be a breach of the IP Act, which can result in a privacy complaint.*
* *A breach of the duty of confidentiality of the HHB Act or provisions in the IP Act may be dealt with as staff disciplinary matters under the Code of Conduct.*
 |
| **The HR Act** Agencies must act compatibility with human rights in the *Human Rights Act 2019* (Qld) (**HR Act**), including: * the human right to privacy (section 25)
* the human right to access government information (section 21)
 | Is the project generally compatible with these (and any other relevant) rights? Can people access their information and information about the project? Will the agency proactively publish information about the project or provide it administratively on request? Will the project impact individual's privacy generally, eg bodily privacy or territorial privacy? Are individuals informed about how the project will impact on their privacy? If the project limits these rights, is the limitation reasonable and justifiable? How is it reasonable and justifiable? If it's not reasonable and justifiable, is the limitation required by, or a result of compliance with, another law? Does the project strike an appropriate balance between any competing rights?  | * *Decisions or actions incompatible with Human Rights may be a breach of the HR Act.*
* *Could result in a complaint to the Queensland Human Rights Commission.*
* *Breaching human rights impacts public trust and confidence and can harm the affected individuals.*
 |

## **Risk ratings**

*Rating each risk can help you to prioritise your responses according to how likely it is that the risk will materialise and the severity of its consequences. You should refer to your agency’s risk management framework for guidance on the descriptors for risk likelihood and consequences and definitions of the overall ratings. You should also record all privacy and confidentiality risks in the project’s risk register/log.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Identified privacy risk**  | **Consequences for the individual or agency** | **Likelihood** | **Risk rating** |
| 1 | *Copy your list of identified risks from section 3.1 and 3.2* | *E.g. Minor, Moderate, Significant* | *E.g. Unlikely, Possible, Likely* | *E.g. Low, Medium, High* |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |

## **Actions to address the identified risks**

*Describe the strategies or actions that will mitigate or minimise the identified risks. Note: While a PIA does not set out to eliminate every possible privacy or confidentiality risk; risk management does not provide an alternative to compliance with the privacy principles or the HHB Act. Privacy and confidentiality needs to be incorporated with other project goals such as functionality; not balanced against them.*

*Adapt this table to suit the nature of the project and the needs of your agency, particularly as large or complex project may require a more complex risk analysis. For example, an assessment of any residual risk, or a more detailed analysis of the costs, strengths and weaknesses of all potential actions that could address the risks.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Identified privacy risk**  | **Existing controls that contribute to managing the identified risk** | **Recommended actions** | **Comments** |
| 1 | *Copy your list of identified risks from sections 3.1 and 3.2* | *What current safeguards help mitigate or minimise the identified risks?* | *What additional measures can be implemented to mitigate or minimise the risk?* | *If there are other strategies that could address the risk, provide comments about why the recommended action is the preferred option.*  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
|  |  |  |  |  |

## **Stakeholder consultation**

*Consultation with key stakeholders is essential to the PIA process. It helps to ensure that key privacy issues are identified, addressed and communicated. Provide details of who you consulted with, how you engaged with them, what you asked them and what information was gathered.*

* *For projects, information and statewide initiatives relating to the* ***Department of Health****, please consult with the Privacy and RTI Unit, Department of Health via* RTI-Privacy@health.qld.gov.au
* *For projects or information relating to the* ***HHSs****, please contact the relevant HHS’ Privacy and Confidentiality Contact Officer (PCCO). A contact list for the PCCO at each HHS is available on the* [*Queensland Health website*](https://www.health.qld.gov.au/system-governance/contact-us/access-info/privacy-contacts/default.asp)*.*

The following stakeholders were consulted in undertaking this PIA:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Stakeholder** | **Internal/External** | **Scope of consultation** | **Method** | **Results** |
| *Name of stakeholders or group of stakeholders* | *Are the stakeholders internal to the agency or external?* | *What did you ask the stakeholder?* | *How did you engage with the stakeholders? For example, meeting, email, etc.* | *What input did the stakeholder provide?* |
|  |  |  |  |  |
|  |  |  |  |  |

## **PIA outcomes**

*Complete this section after the Project Executive/Steering Committee/Senior Management has reviewed the proposed actions and strategies set out in section 5.*

*Agreed recommendations should also be integrated into a revised project plan to ensure that the activities necessary to implement the recommendations are managed.*

## **Agreed recommended actions**

|  |  |  |
| --- | --- | --- |
| **#** | **Recommendation** | **Agreed Y/N** |
| 1 | *Copy the list of recommended actions from the table in section 4.* | *Document whether the recommendation was approved by the Project Executive/Steering Committee or senior management. If the recommended actions will not be implemented, record the rationale for this decision.* |

## **Action plan**

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Actions to be taken** | **Responsibility for action** | **Date for completion** |
| 1 | *List the agreed additional actions.* | *Record who will be responsible for implementing the agreed actions.*  | *Record the planned date for completion.* |

## **Contact point for future enquiries**

|  |  |
| --- | --- |
| Name: |  |
| Position: |  |
| Business unit: |  |
| Email:  |  | Telephone: |  |
| File name/reference:  |  |

1. Whether information is about a ‘reasonably’ identifiable individual requires case-by-case consideration of factors such as the nature and amount of information, who will have access to the information and other information that is available and the practicability of using that information to cross-match or link the information held by the agency to an individual. [↑](#footnote-ref-2)
2. Confidential information is defined in the HHB Act and is information that could identify someone who has received, or is receiving a public sector health service, including deceased persons; it most often relates patients of Queensland Health. [↑](#footnote-ref-3)
3. See ‘Using another name’ section at <https://www.health.qld.gov.au/system-governance/records-privacy/health-personal> [↑](#footnote-ref-4)
4. The term ‘designated person’ is broadly defined in the HHB Act and includes Queensland Health staff, the chief health officer and HHS board members. See section 139 of the HHB Act for the full definition. [↑](#footnote-ref-5)