Fact Sheet November 2026

Privacy considerations when developing mobile applications

Who is this information for?

NSW public sector agencies who develop mobile applications (apps) to deliver services to the community.

Why is this information important?

Mobile apps can be a useful and efficient way to interact with the public and deliver services to the community but can also introduce privacy risks Apps which fail to protect an individual's privacy may result in low user confidence.

This fact sheet provides information about the app environment and its potential impact on the privacy of users.

What is an app?

A mobile application or 'app' is a software program designed to run on a smartphone, tablet computer or other mobile device.

Although apps can improve access to government services, they also create privacy risks anytime they collect, store, use or disclose personal and health information.

For more information about what constitutes personal information, see the IPC's guidance on NSW Privacy Law.

Do privacy laws apply to apps?

Yes. NSW public sector agencies must comply with the *Privacy and Personal Information Protection Act 1998* (PPIP Act) whenever they collect, store, use or disclose personal information, including through an app. The Information Protection Principles (IPPs) apply.

The *Health Records and Information Privacy Act 2002* (HRIP Act) and Health Privacy Principles (HPPs) also apply where agencies, health service providers and other covered organisations handle health information.

Considerations when developing apps

As with any other project involving personal and/or health information, privacy should be built into an app's planning, design, development, testing, deployment, maintenance and retirement. Privacy-related risks should be reviewed whenever the app, its handling of personal or health information, or supporting services materially change.

A privacy by design approach embeds good privacy practices in decisions about the app, its supporting systems and business processes. It anticipates and prevents privacy issues from the outset rather than responding after they occur.

Some privacy considerations include:

1. Complete a Privacy Impact Assessment (PIA) as part of project planning

A Privacy Impact Assessment (PIA) maps the flow of personal and health information and how it is collected, used, disclosed, accessed, stored and deleted. PIAs help to identify privacy vulnerabilities in a systematic way and potential ways to manage, minimise or avoid those vulnerabilities.

A PIA should be undertaken early enough to influence the app's design. It should be treated as an ongoing process that assesses positive and adverse privacy impacts, legal compliance and measures to avoid or minimise risks. An effective PIA should consider how personal and health information is handled by the app and by integrated or supporting services, including analytics tools, cloud services, software development kits (SDKs), AI services and other third parties.

As the app is developed, implemented or updated, it is important to consult any relevant stakeholders as well as the implementation of the recommendations made in the PIA.

Publishing the PIA is an effective way of building user confidence in an app by showing a commitment to privacy and demonstrating that privacy impacts have been considered and addressed.

For more information refer to the IPC's Guide to Privacy Impact Assessments.

2. Consider what personal information is necessary for the app

Consider whether it is necessary for the app to collect any personal information. If so, legislation requires you to collect only information that is reasonably necessary for the service provided by the mobile app.

If you cannot be satisfied the reason you are collecting a specific piece of personal information or device

permissions for the App is really required, the information or device permission should not be collected. For example, even if you think the personal information might be useful in the future, this is not a valid reason for collecting personal information

Avoid collecting information identifying people or their activities, unless it relates directly to the purposes of the app.

Any information collected must be accurate and up to date.

3. Tell individuals how the app will handle personal information

When an app collects personal information, it must tell users why that information is collected, how it will be used and disclosed, whether providing it is voluntary or required by law, the consequences of not providing it, and how they can access and correct it. Being transparent also builds trust with consumers.

A privacy policy or collection notice providing this information should be easily accessible and reader friendly. It should also be accessible to people using assistive technologies and provide alternatives where information is conveyed only through colour, graphics or sound.

For example, if the app takes photos or video and tags the image with location data, a notice may be provided to the user the first time this function is activated.

It can be difficult to communicate this information effectively in the small screen environment. Consideration should be given to strategies for giving an effective notice, such as using short form notices where possible, putting important information up front with links to more detailed explanations.

Individuals should have as much control over the personal information collected by the app as practicable. Where possible, allow users to opt out of the collection of their personal information.

If the personal information could be considered by an individual as highly personal or intrusive, such as a user's location data, sound or activation of the device camera, consider having the user' provide specific consent for the manner in which the app will handle that information. Any component of the app that relies on consent should also include the capacity to allow the user to withdraw their consent at a later time.

Where possible, a tool should be provided that displays the user's privacy settings with easy means of changing them.

For more information refer to the IPC Fact Sheet - Consent

4. Consider how personal information will be stored and secured

The PPIP Act and HRIP Act require agencies and other covered organisations to protect personal and health information against loss, unauthorised access, modification, or other misuse.

Ensure the storage and collection of information on the device, in transit and in back-end systems is protected using appropriate encryption, authentication, access controls, logging, testing and timely security updates. Do not store passwords or other authentication credentials in plain text. Use appropriate, industry-standard controls to protect stored credentials.

Any contracts with third-party providers related to the app should cover privacy, security, breach response, retention, disposal, audit and data location.

Include the ability for users to refuse to update a mobile app and that they can easily deactivate or delete the app.

5. Have clear and accessible privacy information

Privacy statements and collection notices must be clear, up to date and easy to access, including a link to the agency's Privacy Management Plan for more detail. Users should be able to access this information to evaluate what you propose to do with their personal information and before deciding whether to download the app.

Privacy information should be easy to find at all stages of the user's interaction with the app, including before download, at first use and within the app.

Make sure this privacy information tells individuals:

- what personal and health information the app collects, including through device permissions
- why it is needed, how it will be used and where it will be stored
- who it may be disclosed to, including third-party, cloud, analytics or AI providers
- whether it may be disclosed to a Commonwealth agency or outside the NSW jurisdiction
- how they can delete the App or their subscription to the App, and what will happen to personal information already collected and stored
- how individuals can change permissions or request access, correction or deletion
- how to make a privacy complaint; and
- how data breaches will be managed and the process for notifying individuals.

You should regularly review the app's operation and data flows to confirm that personal information is handled consistently with the information provided to users. This includes explaining any material changes and available choices clearly and obtaining fresh consent where required.

When making changes to the privacy policy, inform users in advance of the changes taking effect and provide details of what has changed so that users do not have to compare old and new policies to understand what has changed.

6. Access and amendment

Information collected through apps forms part of the agency's personal information holdings. The PPIP Act and HRIP Act provide individuals with rights regarding access and correction of their personal information held by agencies.

Some types of information that can potentially be captured by Apps such as geo-location, the user's usage patterns or the address book on their device will not only be unique to the mobile device environment but also could potentially be of interest to both the user and third parties

Information collected through apps should be incorporated into records and information management processes, including the agency's:

- business classification terms
- functional retention and disposal schedule
- list of personal information holdings; and
- information asset register.

Agencies should tell users how to exercise their access and amendment rights. Collection notices or tools within the app could include a link to this information on the agency's website.

7. Use and disclose personal information only as permitted

Agencies may need to use and disclose personal information for an App to function. For example, geo-location data may be required to deliver certain functions in a navigation or public transport App. Agencies may need to share personal information with another entity to provide the services offered by the App. Apps should generally only use personal information for the purpose it was collected, and only disclose to the individual it is about, except in limited circumstances.

Do not collect personal information about third parties from a user's device, such as a user's address book or contact list, unless you can obtain the consent of those parties.

Avoid associating personal information between the App and a user's social media account unless it is obvious to the user and necessary to do so.

Agencies should monitor Apps to ensure personal information is only used and disclosed in ways that are permitted by the PPIP and HRIP Act and in accordance with their privacy policy.

8. Will personal information be transferred out of Australia?

The PPIP Act sets out additional requirements when personal information is transferred outside of Australia. If the development or delivery of the app will involve the transfer of personal information outside of Australia, such as for storage in a cloud, you will need to consider the associated privacy risks and impacts.

For more information refer to the IPC's Guide - Transition to Cloud – managing your agency privacy risk.

9. Consider the use of contracted service providers

For contracted app services, an agency will need to clarify how the PPIP Act and HRIP Act apply and the responsibilities of the agency, provider and any subcontractors. Section 12(d) of the PPIP Act requires agencies to do everything reasonably within their power to prevent unauthorised use or disclosure of personal information given to a service provider.

The agency should assess providers before engagement, include appropriate privacy and security protections in contracts with them and monitor their compliance. Contractual requirements should also apply to any subcontractors involved in the development and delivery oi the app.

10. Plan for retention and disposal

Agencies should keep personal and health information collected through apps no longer than necessary and dispose of it securely, subject to state records and other legal obligations. Ensure that a plan exists for when the App is deleted or de-identification when an account closes or the app is retired, including of any information held in backups or by service providers.

11. Plan for breaches and complaints

Agencies should develop specific procedures for dealing with privacy breaches and complaints., Under the Mandatory Notification of Data Breach (MNDB) Scheme agencies must keep an internal data breach incident register and a publicly accessible data breach policy. Eligible breaches require notification to the Privacy Commissioner and affected users.

For more information

Contact the Information and Privacy Commission NSW (IPC):

Freecall: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Website: www.ipc.nsw.gov.au

NOTE: The information in this fact sheet is to be used as a guide only. Legal advice should be sought in relation to individual circumstances.