

Updated and effective as of 31 March 2025

1. About our Privacy Statement

Interweave Integration Pty Ltd (ACN 685 229 967) values and respects the confidentiality of information provided by our customers. We are committed to protecting the privacy of patients, staff, and others for whom we hold data, adhering to the Privacy Act 1988 (Cth) (the Privacy Act), and complying with the Australian Privacy Principles set by the Federal Australian Government for the handling of Personal Information under the Privacy Act.

Our objective is to ensure that all data accessed by Interweave or uploaded into our Servers is kept secure in accordance with the principles outlined in this Privacy Statement.

This Privacy Statement also details our response to unauthorised access, data breach, or suspected data breaches.

This Privacy Statement contains common questions arising from individuals and customers engaging with us and using our Interwoven Solutions or other services we offer.

2. What is Personal Information?

Under the Privacy Act, "Personal Information" means any information or opinion, whether true or not, and whether recorded in a material form or not, about an identified individual or an individual who is reasonably identifiable. In general terms, this includes information or an opinion that personally identifies you (or another person) either directly (e.g your name) or indirectly.

3. What Personal Information do we collect?

3.1 Contact Information

We collect contact information of our customers, users and other people we need to contact in order to run our business and services.

3.2 Patient Administration System Data

In order to provide our services we require access to our customers' Patient Administration Systems and other systems within our customers' network, however we do not collect or retain any Personal Information from these systems.

3.3 Patient Information for Custom Solutions

Where we provide custom solutions that uses identifiable patient data, the system runs on computer system provided by our customers and that run on

their network. We comply with our customers' remote access and network security policies and the responsibility of protecting this Personal Information remains with our customers.

4. How do we collect Personal Information?

We may collect Personal Information when you email us, interact with us over the telephone, or interact with us in person, whether at our address of business or at any other location.

We may collect Personal Information when information is sent to our systems via APIs, either through integration components we install on our customers' networks, or via integration components developed but our customers in accordance with our API documentation.

5. Non-consented Collection of Information

As there are many circumstances in which we may collect information electronically, we endeavour to ensure that a person from Interweave is always aware when Personal Information is being collected. Where we obtain Personal Information without a person's knowledge (such as by accidental acquisition from a client or other third party) we will either delete/destroy the information or inform the individual that we hold the information in accordance with the Australian Privacy Principles.

6. How do we use an individual's Personal Information?

We use Personal Information for several purposes in connection with our services, including but not limited to:

1. providing our services,
2. improving the quality of the services we offer,
3. internal administrative purposes; or
4. any other purposes that we may need from time to time.

7. Disclosure of Personal Information to Third Parties

We may disclose a person's Personal Information to third parties in accordance with this Privacy Statement in circumstances where you would reasonably expect us to disclose a person's information. For example, we may disclose a person's Personal Information to:

1. our professional services advisors (such as our Accountants, Consultants, Lawyers etc.);
2. any other entity that provides a service that we may utilise from time to time;
3. our employees, contractors and/or related entities;
4. IT service providers, data storage, web-hosting and server providers; or
5. third party contractors, technology service providers and suppliers that assist us with providing our business processes, products and services. This may include artificial intelligence models.

8. Overseas disclosure

While we store Personal Information in Australia, where we disclose personal information to overseas third parties these third parties may store, transfer or access personal information outside of Australia. We will only disclose your Personal Information overseas in accordance with the Australian Privacy Principles contained in the Privacy Act.

9. How do we protect Personal and Sensitive Information?

9.1 Internal and External Electronic Protection Measures

Our Privacy Officer oversees the management of this Privacy Statement and ensures compliance with the Australian Privacy Principles and the Privacy Act. We commit to taking all reasonable steps to keep the Personal and Sensitive Information we hold confidential and secure. To achieve this, we:

1. Maintain physical security at our business locations.
2. Store data on virtual machines within your network or in secure data centres based in Australia.
3. Ensure data transmission to us is via secure channels such as HTTPS or WSS.
4. Use secure protocols like RDP or SSH for accessing remote services.
5. Implement multifactor authentication for access to our systems and servers.
6. Deploy security software, including anti-virus and firewalls, on our computers.
7. Restrict data access to key personnel who require it to provide services as part of their role with us.
8. Refrain from disclosing any Personal or Sensitive Information to overseas entities in jurisdictions without a regime comparable to the Australian Privacy Principles or without a similar enforceable privacy statement.
9. If there's a need to provide Personal or Sensitive Information to an overseas entity, we ensure that the entity agrees in writing to safeguard the information to standards comparable to ours before any disclosure.
10. Maintaining security on our servers or on third party servers we use is in line with current practices having regard to the size and nature of our business.

10. Online Activity Tracking

10.1 Direct Marketing

1. Upon request, we can send you direct marketing communications and information about our services that we consider may be of interest to you if you have requested or consented to receive such communications. These communications may be sent in various forms, including mail, SMS, fax and email, in accordance with applicable marketing laws, such as the *Australian Spam Act 2003* (Cth).

2. You consent to us sending you those direct marketing communications by any of those methods. If you indicate a preference for a method of communication, we will endeavour to use that method whenever practical to do so.
3. You may opt-out of receiving marketing communications from us at any time by following the instructions to “unsubscribe” set out in the relevant electronic or print communication as well as contacting us with the details set out in the “How to contact us” section (see below).

11. Data Breach Response Plan and Investigation Measures

1. If we are subject to a data breach or suspected data breach, we will adopt our Data Breach Response Plan ("Response Plan") to ensure that we will use our best endeavours to mitigate any loss or damage to both us and any individuals whose information may be leaked.
2. Our Response Plan is similar to the one that the Office of Australian Information Commissioner (“OAIC”) has adopted. Our Response Plan also contains all the recommendations that the OAIC suggests for entities that follow the Australian Privacy Principles.
3. Outlined below is an overview of our data breach Response Plan:
 1. **Identification**
 - Record the date and time the breach (or suspected breach) was discovered;
 - The type of information (personal, sensitive or other) at risk;
 - The cause and extent of the breach; and
 - the context of the affected information and the breach.
 2. **Containment**
 - Identify the information that has been exposed and lock the databases;
 - Inform our off site IT support of the breach and to take action to trace the breach and review current protections;
 - Ensure all other information held is protected and unaffected.
 3. **Assessment**
 - The Privacy Officer will decide whether the breach is a notifiable data breach (If no, then no further action will be taken)
 - If yes, provide all information about the breach that has been gathered to the affected individuals and update them of the ongoing investigation, the cause of the breach and the extent of the harm as well as other harms;
 - contact IT support to implement further systems or recovery operations;
 4. **Report**
 - The Privacy Officer will file an online submission to the OAIC outlining the aforementioned actions undertaken at <https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach>
 - This is in accordance with the Notifiable Data Breach Scheme (NDBS).
 5. **Review & Reflect**

- Once we have submitted our breach to the OAIC, we will review our actions in consultation with our IT Support to identify any weaknesses in our plan and how it can be improved, in addition to further training that may be required;
- All records and documents created during a breach (or suspected breach) will be stored for seven (7) years.

12. Security

We are dedicated to the security of the Personal Information we gather, implementing appropriate physical, electronic, and managerial measures having regard to the size and nature of our business to prevent unauthorized access, disclosure, and safeguard against misuse, interference, loss, and unauthorized access, modification, and disclosure. Despite our commitment to security, we cannot assure the security of:

1. information transmitted to or by us over the Internet or
2. maintained on your servers to which we have access.

The transfer and storage of data on your end, as well as the exchange of information between us, is carried out at your own risk. Further, although we access your system through a secure channel, please note that we do not continuously monitor this channel.

13. Retention of Personal and Sensitive Information

We will not keep a person's Personal or Sensitive information for any longer than we need to. In most cases, this means that we will only retain a person's Personal or Sensitive Information for the duration of your relationship with us unless we are required to retain any Personal or Sensitive Information to comply with applicable laws, for example record-keeping obligations.

14. How to access and correction of an individual's Personal and Sensitive Information

1. At all times, Interweave will use its best endeavours to keep a person's Personal and Sensitive Information accurate, complete and up to date.
2. If you wish to make a request to access and/or correct the Personal Information we hold about a person you represent, you should make a request by contacting us directly and we will usually respond within 1-2 business days. For more urgent requests or suspected breaches, we will investigate and respond immediately in accordance with our Response Plan.

15. Updates to this Privacy Statement

1. If we decide to change this Privacy Statement, we will post the changes and updates on our webpage at <https://Interweave.au/>;
2. Please refer back to this Privacy Statement to review any amendments. We may do things in addition to what is stated in this Privacy Statement to comply

with the Australian Privacy Principles, and nothing in this Privacy Statement shall deem us to have not complied with the Australian Privacy Principles.

As an Australian Privacy reporting entity under the Privacy Act, we are obligated to adhere to the Privacy Act and the Australian Privacy Principles.

You can review the Australian Privacy Principles at: <https://www.oaic.gov.au/privacy/australian-privacy-principles/read-the-australian-privacy-principles>

16. Privacy Act, the Australian Privacy Principles and Inconsistency

1. For clarity, anything that is not covered under our Privacy Statement is governed by the provisions in the Privacy Act and the Australian Privacy Principles.
2. In the event of any inconsistency between our Privacy Statement and the Privacy Act or the Australian Privacy Principles, the Privacy Act and the Australian Privacy Principles will prevail to the extent of the inconsistency.

17. Inquiries and Complaints

1. For complaints about how Interweave handles, processes or manages Personal and Sensitive Information, please contact our Privacy Officer. Please note that we may require proof of your identity and full details of your request before we can process your complaint.
2. Please allow up to 5 business days for Interweave to respond to your complaint. It will not always be possible to resolve a complaint to every individual's complete satisfaction. If you are not satisfied with our response to a complaint, you have the right to contact the Office of Australian Information Commissioner at www.oaic.gov.au/ to lodge a complaint.

How to Contact Us

If you have a question or concern in relation to our handling of the Personal or Sensitive Information that we may hold about you or the person you are representing for or this Statement, you can contact us for assistance as follows:

Privacy Officer
privacy.officer@interweave.au