Qualitas Health Privacy Policy

Current as of 11 April 2025

Introduction

Qualitas Health consists of a group of medical companies with a passion for providing the highest quality healthcare to the Australian community including primary, radiology and dental care. We are dedicated to ensuring that our patients are comfortable in entrusting their health information with our Practices and our staff. This policy provides information to patients as to how their personal information (which includes their health information and sensitive information) is collected and used within our Practices, our administrative office and in which circumstances we may disclose it to third parties.

We will handle your personal information in a responsible manner in accordance with:

- The Privacy Act 1988;
- The 13 Australian Privacy Principles (APP) from Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* which amended the *Privacy Act 1988 and* replaced the National Privacy Principles and Information Privacy Principles;
- Legal and ethical confidentiality obligations;
- Other relevant State and/or territory laws (which may or may not be health specific).

To ensure our patients' privacy is maintained at all times, we are dedicated to implementing this policy, training our staff to apply it and continual review of our processes and systems to handle personal information. Only staff who need to see your personal information will have access to it. No member of staff should access a patient's Health Information and Sensitive Information unless required to provide medical care to that patient. All actions and access to patient's medical records are recorded. If we need to use your information for anything else, we will seek additional consent from you to do this. We will update this policy to reflect any changes.

The APP

The APP provide a privacy protection framework that supports the rights and obligations of collecting, holding, using, accessing, and correcting personal information. The APP consist of 13 principle-based laws and apply equally to paper-based and digital environments. The APP complement the long-

standing general practice obligation to manage personal information in a regulated, open and transparent manner.

Types of personal information

Personal information means information or an opinion, including information or an opinion forming part of a database, "whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion".

Health information includes personal information collected to provide, or in providing, a health service (which is also sensitive information).

Sensitive information means information or an opinion about a person's racial or ethnic origin, political opinions, membership of a political, professional or trade association or trade union, religious beliefs or affiliations, philosophical beliefs, sexual preferences or practices, or criminal record, as well as health information about the person.

Patient health record means information, held about a patient, in paper form or electronic form, which may include:

- contact and demographic information
- medical history
- notes on treatment
- observations
- correspondence
- investigations
- test results photographers
- prescription records
- medication charts
- insurance information
- legal information and reports
- work health and safety reports

Practice procedure

We will:

- provide a copy of this policy upon request;

- ensure staff comply with the APP and deal appropriately with inquiries or concerns;
- take such steps as are reasonable in the circumstances to implement practices, procedures and systems to ensure compliance with the APP and deal with inquiries or complaints;
- collect personal information for the primary purpose of managing a patients' healthcare and for financial claims and payments.

Staff responsibility

The Practices' and key administrative staff who are entrusted with confidential information, all having signed confidentiality agreements, will take reasonable steps to ensure patients understand:

- what information has been and is being collected;
- why the information is being collected, and whether this is due to a legal requirement;
- how the information will be used or disclosed;
- why and when their consent is necessary;
- the Practices' procedures for access and correction of information, and responding to complaints of information breaches, including by providing this policy.

Patient consent

We will only interpret and apply a patient's consent for the primary purpose for which it was provided. We must seek additional consent from the patient if the personal information collected may be used for any other purpose.

Collection of information, storage, and security

We need to collect personal information as a provision of clinical services to patients at the Practices. Collected personal information will include patients':

- names, addresses, date of birth, gender, and contact details;
- Medicare number (where available) (for identification and claiming purposes);
- healthcare identifiers;
- medical information including medical history, medications, allergies, adverse events, immunisations, social history, family history and risk factors;
- payment information such as credit card and direct debit details;
- information from patient enquiries;
- communication between the Practice and the patient.

A patient's personal information may be held securely at the relevant Practice and/or in the Admin Office in various forms:

- as paper records, in hard copy format in secured environment;
- as electronic records in protected password-secured information systems;
- as visual – x-rays, CT scans, videos and photos;
- as audio recordings.

Our procedure for collecting personal information is set out below:

1. Practices' staff collect patients' personal and demographic information via registration when patients present to the Practices for the first time. Patients are encouraged to pay attention to the Privacy Consent form and collection statement attached to/within the form and information about the management of collected information and patient privacy;
2. During the course of providing medical services, the Practices' healthcare practitioners will consequently collect further personal information;
3. Information can also be collected through electronic transfer of prescriptions (eTP), My Health Record, e.g. via Shared Health Summary, Event Summary;
4. Personal information may also be collected from the patients' guardian or responsible person (where practicable and necessary), or from any other involved healthcare specialists, your health fund, Medicare or the Department of Veterans' Affairs (as necessary);
5. We may also collect your personal information when you visit our website, send us an email or SMS, telephone us, make an online appointment or communicate with us using social media. Information collected through our website may also include website analytics, cookies etc;
6. Some practices may collect CCTV footage for security and safety purposes. Those practices will have signs indicating the presence of CCTV;
7. Photos and medical images can be taken using personal devices for medical purposes where necessary following the guidelines outlined by Royal Australian College of General Practitioners. Those photos and images will be removed completely from the personal device once the photos and images are added to the patient's medical record.

Information may be collected in various ways, such as over the phone, in writing, in person in our Practices, in our Admin Office or at home visits, over the internet if you communicate with us online as well as information which are entered into our Practices' website.

We hold all personal information securely, whether in electronic format, in protected information systems or in hard copy format in a secured environment.

Trans-border Data Flows

To help deliver timely and high-quality care, our radiology practice may securely transmit limited or de-identified health information overseas for specific processing tasks, such as AI-based referral interpretation or medical transcription. For example, some referrals may be processed using AI tools hosted in the United States, or by trained medical transcriptionists in the Philippines. Importantly, all health data is stored in Australia. Only the necessary information is temporarily processed offshore and then securely returned.

We ensure that all overseas providers comply with Australian Privacy Principles and maintain strict confidentiality, privacy, and data protection standards.

Document Automation Technologies

Document automation is where systems use existing data to generate electronic documents relating to medical conditions and healthcare. Some practices use document automation technologies to create documents such as referrals, which are sent to other healthcare providers. These documents contain only your relevant medical information. These document automation technologies are used through secure medical software such as Best Practice, Medisecure, Medical Objects and other industry standard secured software. All users of the medical software have their own unique user credentials and password and can only access information that is relevant to their role in the practice team.

Artificial Intelligence (AI) Scribes

Some doctors at our general practice (exclude radiology practice) may use an AI scribe tool to support the doctor to take notes during their consultations with you. The AI scribe uses an audio recording of your consultation to generate a clinical note for your health record.

The AI scribe tool:

- does not share information outside of Australia
- destroys the audio file once the transcription is complete
- retains sensitive, personal identifying information as part of the transcription

The practice will only use data from our digital scribe service to provide healthcare to you.

Referrers and their Staff

For our radiology practices, Information we collect about our referring physicians, their staff and the practices include:

- Name, address, telephone numbers, fax / email address and other contact details
- Details of IT systems
- Medicare provider numbers and billing information
- Area of specialisation
- Employment history
- Service delivery preferences, referral patterns and fees paid by referred patients
- Information gathered by marketing liaisons during site visits
- Expressed wishes about the future provision of health services
- Details of feedback, complaints, incidents and suggestions

Qualitas Health Staff

Information we collect about our staff may include:

- Name, address, email address and other contact details
- Letters of application / expression of interest and associated correspondence
- Curriculum Vitae / resume
- Referee comments
- Performance records
- Superannuation membership details
- Bank details, tax file number and other employment records
- Language skills for assistance with patient communication

Employment Applicants

Information we may collect and store about employment applicants may include:

- Name, address, email address and other contact details
- Letters of application / expression of interest and associated correspondence
- Curriculum Vitae / resume
- Referee comments

This information is stored for unsuccessful applicants as a future reference to other available positions that may arise.

Use and disclosure of information

Personal information will only be used for the purpose of providing medical services and for claims and payments, unless otherwise consented to. In relation to referral to specialists, we ensure only sensitive patient personal health information that is relevant to the referral are included and disclosed in the referral. Our practice software allows us to use document automation technologies, particularly so that only the relevant medical information is included in referral letters. Some disclosure may occur to third parties engaged by us for business purposes, such as accreditation, for the provision of information technology, medical research and medical studies. These third parties are required to comply with the APP and our policy. We will inform the patient where there is a statutory requirement to disclose certain personal information (for example, some diseases require mandatory notification).

We will not disclose personal information to any third party other than in the course of providing medical services, without full disclosure to the patient or the recipient, the reason for the information transfer and full consent from the patient. We will not transfer your personal information to an overseas recipient (unless under exceptional circumstances permitted by law) unless we have your consent. Limited or de-identified health information transmitted overseas temporarily described under the Data Trans-border Data Flows section are for processing purposes only and is not transferred to and will not be stored by the overseas service provider.

Exceptions to disclosure without patient consent are where the information is:

- required by law;
- necessary to lessen or prevent a serious threat to a patient's life, health or safety or public health or safety, or it is impractical to obtain the patient's consent;
- to assist in locating a missing person;
- to establish, exercise or defend an equitable claim;
- for the purpose of a confidential dispute resolution process;
- during the course of providing medical services, through eTP, My Health Record (e.g. via Shared Health Summary, Event Summary).

We will not use any personal information in relation to direct marketing to a patient without that patient's express consent. Patients may opt-out of direct marketing at any time by notifying the relevant Practice or our Admin Office in a letter or email.

We evaluate all unsolicited information we receive to decide if it should be kept, acted on or destroyed.

Website(s)

Our Website(s) uses Google Analytics and Google Tag Manager to help us to improve our Website(s) and services as well as enhance user experience. Google Analytics collects data with respect to your interaction with our website and produce reports on how visitors use our website. The type of data that we may collect using this tool include, but are not limited to, time of visit, pages visited, referring site details, geographic locations, search terms, number of visitors, number of bookings made through the website(s).

Google Analytics is a US-based service. The information generated about your use of our Website(s) (including your IP address) will be transmitted to and stored by Google Analytics on servers located outside Australia. Google will not associate your IP address with other data they hold. Please see Google's Privacy Policy.

By using our Website(s), you consent to the processing of data about you by Google Analytics in the manner described in Google's Privacy Policy and for the purposes set out above. You may opt out of the collection of information via Google Analytics by downloading the Google Analytics Opt-out browser add on.

Google Analytics collects information using cookies. A cookie is a small piece of text sent to your browser by a website you visit. It helps the website to remember information about your visit. It enhances the website's functionality and improve your user experience. Most browsers allow you to choose whether to accept cookies. You can find further information on how to manage or disable cookies in common browsers such as Google Chrome and Internet Explorer. However, if you disable all cookies in your browser, certain sections of our website may not work.

Our Website(s) may contain links to third-party websites. We have no control over these websites or any of their content and are not responsible for any loss or damage you may suffer from using them. Third-party websites are governed by their own terms of use (including privacy policies). We recommend you satisfy yourself with respect to their terms of use and policies on handing of your personal information.

Storage and Security of Information

Qualitas Health has procedures in place that ensure your personal information is stored securely and protected from misuse, loss and unauthorised access. Some of the steps taken to ensure this include:

• A secure electronic database of both your personal information, images and of any procedures performed by our practices.

• Dedicated back up / archive system of the database.

• Database only accessible by persons requiring access to the database for the purpose of their employment e.g. Medical Receptionist.

• Hard copy storage in secure onsite and offsite storage facilities.

• Hard Copy destruction using dedicated third party secure destruction company.

• Staff training regarding use of patient personal information and Privacy policy.

• Regular review of policies and procedures.

Qualitas Health does not record real-time audio/visual recording, duplication, or storage of consultations, including those via Telehealth or those conducted remotely. If necessary, informed consent will be obtained and recorded in the patient's file.

Online Access to your Images and Reports

Qualitas Health radiology Practices may provide your report to your referring physician via a secure electronic system. The system is encrypted and requires certificates at the referrers end to allow them to de-encrypt the report and download it into their patient management system.

We also provide online access to your images, via a secure website that requires secure login by users. Your referring physician may request access to your images via this method.

A third party specialist may also request access to these images for purposes relating to your medical treatment so we will acknowledge your consent through the Collection and Privacy Statement signed at the time of your examination.

You can also choose to have your images sent to you via electronic method, which would mean no hard copy images will be printed. These images are yours and may be used as you wish for your own personal use. You may also choose who gains access, by providing them with an email, link, web portal view and an access key to the images online. Images are accessed via a secure online cloud.

Your permission to use, send and disclose your records via these secure online / electronic methods will be sought by the Collection and Privacy Statement. Information will only be sent to your referring

physician or third party treating specialist in relation to your healthcare. At any time, should you wish to withdraw this permission, or request us to seek permission each time, you may contact the practice or Administration Office to revoke the permission.

Access, corrections, and privacy concerns

We acknowledge patients may request access to their medical records. Patients are encouraged to make this request in writing, and the Practices and/or the Admin Office will respond within a reasonable time, usually 30 days. There will be a fee for the administrative costs of retrieving and providing you with copies of your medical records.

We take reasonable steps to correct personal information where it is satisfied they are not accurate or up to date. From time to time, the Practices and/or staff from the Admin Office will ask patients to verify the personal information held by us is correct and up to date. Patients may also request us to correct or update their information, and patients should make such requests in writing.

Complaints

We take complaints and concerns about the privacy of patients' personal information seriously. Patients should express any privacy concerns in writing. We will then attempt to resolve it in accordance with its complaint resolution procedure. We will investigate the complaint and endeavour to respond as quickly as possible. If you feel your complaint has not been dealt with correctly or you are unsatisfied with the response, you may lodge a complaint to the Office of the Australian Information Commissioner (OAIC).

You have the right to deal with us anonymously or under a pseudonym unless it is impracticable for us to do so or unless we are required or authorised by law to only deal with identified individuals.

Breach of this Policy

A breach of this policy by Qualitas Health employee may result in disciplinary action, up to and including summary dismissal.

Access to this Policy

This policy is available on the Qualitas Health website to the public and on the Qualitas Health human resources online system "Employment Hero". Hard copies can be located at the Practices. This policy is incorporated in the employee induction information packs and training for new employees.

Policy Review

This privacy policy will be reviewed regularly to ensure that it is in accordance with any changes that may occur. When amendment/s occur, we will notify you by posting an updated version of the policy at the Practices and on our websites.

Qualitas Health Privacy Officer

Anna Pittard (nee Huang)

Suite 32.02, 1 Denison Street, North Sydney NSW 2060

Phone – 02 9466 5950

Email – anna@qualitashealth.com.au

Radiology Privacy Officer

Peter Bonovas

Director of Operations

Suite 32.02, 1 Denison Street, North Sydney NSW 2060

P – 02 8889 6320

Email – pbonovas@synrad.com.au

Office of the Australian Information Commissioner (OAIC)

GPO Box 2999, Canberra ACT 2601

Phone: 1300363992

Email: enquiries@oaic.gov.au

Web: http://ww.oaic.gov.au/

OAIC Online Privacy Complaint form

https://forms.business.gov.au/aba/oaic/privacy-complaint-/