

Privacy Notice

Document Management

Organisation: Dental Reporting AI

Issue Date: Aug 21, 2026

Document Owner: No assignees

Document Version Control

Version	Date	Summary of changes	Author
1.0	Aug 21, 2026, 13:31	complete	Simon Harvey

Privacy Notice

This Privacy Notice describes the organisation's policies and procedures on the collection, use and disclosure of personal data and informs users about privacy rights and how the law protects individual rights and freedoms.

Contents

[Who we are and how to contact us](#)

[The types of personal data we collect about all the users of our app](#)

[1.0 How is your personal data collected?](#)

[2.0 How we use your personal data](#)

[2.1 Legal basis](#)

[2.2 Purposes for which we will use your personal data](#)

[2.3 Direct marketing](#)

[2.4 Third-party marketing](#)

[2.5 Opting out of marketing](#)

[2.6 Cookies](#)

[3.0 Disclosures of your personal data](#)

[3.1 Business Transactions](#)

[3.2 Law enforcement](#)

3.3 Other legal requirements

4.0 International transfers

5.0 Data security

6.0 Data retention

6.1 How long will you use my personal data for?

7.0 Protecting your sensitive data

7.1 People

7.2 Cyber resiliency, business continuity, and disaster recovery

7.3 Technology

8.0 Your legal rights

8.1 No fee usually required

8.2 What we may need from you

8.3 Time limit to respond

9.0 Contact details

10.0 Complaints

11.0 Changes to the Privacy Notice and your duty to inform us of changes

12.0 Third-party links

13.0 Payments

Privacy Notice

This Privacy Notice gives you information about how Dental Reporting AI” collects and uses your personal data through your use of our app and when you communicate with us in any way, including any data you may provide when you sign up and use our services.

Who we are and how to contact us

Dental Reporting AI is the controller and responsible for your personal data (collectively referred to as, "we", "us" or "our" in this Privacy Notice). Dental Reporting Alis a company registered in England and Wales with company number 11919496 with its registered office at Preston Park House, South Road, Brighton, East Sussex, United Kingdom, BN1 6SB.

If you would like to contact us about anything in this Privacy Notice, or if you have any questions about how we use your information or if you would like to exercise any of your data subject rights, please contact us here: dentalreportingai@icloud.com

The types of personal data we collect about all the users of our app

Personal data means any information about an individual from which that person can be identified.

We may collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

- **Identity Data** includes: first name, last name, job title, and professional role at the client organisation (for example: consultant radiologist, practice manager, IT lead, procurement contact).
- **Contact Data** includes: work email address, hospital or dental practice name, hospital or practice postal address, and work telephone number (where provided).
- **Transaction Data** includes details of the contract between us and your organisation, purchase orders, invoices issued, payments received, and records of the products and services provided to your organisation under that contract.
- **Technical Data** includes limited technical information necessary to operate and secure our website and software, which may include internet protocol (IP) address, browser type and version, operating system, and device information. Because end users of our software access it via generic, non-attributable logins issued by the hospital, we do not link technical data to identifiable individual users of the software itself.
- **Profile Data** includes account administration information relating to the named client contacts at your organisation, such as job role, communication preferences, and any feedback or correspondence you have shared with us. We do not hold personal usernames or passwords for end users of the software, as logins are generic and issued by the hospital rather than created by us for named individuals.
- **Usage Data** includes aggregated and anonymised information about how our software is used (for example, feature usage patterns and volumes), which we use to maintain and improve the service. Because logins are generic and not linked to identifiable individuals, usage data is not personal data in our hands.
- **Marketing and Communications Data** includes preferences in receiving service updates and other communications from Report Wizard, and a record of your communication preferences. We do not share data with third parties for marketing purposes.
- **Health Data** — Not applicable. We do not collect, process, store, or transmit any health data, patient data, or special category data as defined under UK GDPR Article 9. Our software assists clinicians in producing reports but does not require us to receive or hold any patient information, and we do not ask for or accept health data from our clients or their contacts.

We also collect, use and share **anonymised aggregated data** such as statistical or demographic data which is not personal data as it does not directly (or indirectly) reveal your identity. For example, we may use this anonymised data for the purposes of helping us build evidence to justify formal clinical trials and feasibility studies in a clinical setting, or for internal research and product development, including product development involving machine learning and big data analysis, or for future publications.

1.0 How is your personal data collected?

We use different methods to collect data from and about you including through:

- **Direct interactions with us.** You may give us your personal data by corresponding with us by post, phone, email, video call, or in person, or by completing forms during the sales, contracting, or onboarding process. This includes personal data you provide when you or your organisation:
- enquire about Report Wizard or request a demonstration;
- enter into a contract or commercial arrangement with us for the supply of our software;
- are nominated by your organisation as a named point of contact for account, procurement, IT, clinical, or billing purposes;
- request technical support or otherwise correspond with our support or account management teams;
- provide feedback, respond to a survey, or take part in a product discussion;
- opt in to receive service updates or other communications from us.

Note. We do not collect personal data from patients. Report Wizard is supplied on a business-to-business basis to hospitals and dental practices, and the personal data we hold relates only to the professional contacts at those client organisations. End users of the software (clinicians and other staff) access it via generic, non-attributable logins issued by their employer, so they are not personally identifiable to us.

- **Automated technologies or interactions.** As you interact with our app, we will automatically collect Technical Data about your equipment, browsing actions and patterns. We do not collect any cookies from users in our mobile app – delete if not applicable.
- **Third parties.** We do not receive personal data about you from any third parties. All personal data we hold is collected directly from you or from your organisation during the sales, contracting, onboarding, or ongoing service relationship.

2.0 How we use your personal data

2.1 Legal basis

The law requires us to have a legal basis for collecting and using your personal data. We rely on one or more of the following legal bases:

- **Performance of a contract with you:** Where we need to perform the contract we are about to enter into or have entered into with you.
- **Legitimate interests:** We may use your personal data where it is necessary to conduct our business and pursue our legitimate interests, for example to prevent fraud and enable us to give you the best and most secure customer experience. We make sure we consider and balance any potential impact on you and your rights (both positive and negative) before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law).
- **Legal obligation:** We may use your personal data where it is necessary for compliance with a legal obligation that we are subject to. We will identify the relevant legal obligation when we rely on this legal basis.
- **Consent:** We rely on consent only where we have obtained your active agreement to use your personal data for a specified purpose.

2.2 Purposes for which we will use your personal data

We have set out below, in a table format, a description of all the ways we plan to use the various categories of your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

	Type of data	Legal basis
To establish and administer a commercial relationship with your organisation, including registering you as a named client contact and setting up your organisation's account	(a) Identity (b) Contact	Performance of a contract with your organisation, and our legitimate interests in operating our business
To process payments, issue invoices, manage refunds, and maintain records of the products and services supplied to your organisation	(a) Identity (b) Contact (c) Transaction	(a) Performance of a contract with your organisation (b) Necessary to comply with a legal obligation (tax and accounting record-keeping)
To deliver Report Wizard to your organisation, including account provisioning, service delivery, and issuing generic logins to the hospital or practice(a) Identity (b) Contact	(a) Identity (b) Contact	Performance of a contract with your organisation
To provide technical support, respond to queries, and manage our ongoing relationship with your organisation, including notifying you about changes to our terms or Privacy Notice, and dealing with your requests, complaints, and queries	(a) Identity (b) Contact (c) Profile	(a) Performance of a contract with your organisation (b) Necessary to comply with a legal obligation (c) Necessary for our legitimate interests (to keep our records updated and manage the client relationship)
To send you service-related communications (for example, updates about the software, maintenance notices, security notifications, and changes affecting the service)	(a) Identity (b) Contact	Necessary for our legitimate interests (to keep clients informed about the service they use)
To send you optional service updates or product news	(a) Identity (b) Contact (c) Marketing and	Consent, having obtained your prior consent to

where you have opted in to receive them	Communications	receive such communications, which you may withdraw at any time
To carry out market research or gather feedback through your voluntary participation in surveys or discussions	(a) Identity (b) Contact (c) Profile	Necessary for our legitimate interests (to understand how clients use our products and to improve and develop them)
To administer and protect our business and IT systems, including troubleshooting, system maintenance, network security, and hosting of data	(a) Identity (b) Contact (c) Technical	(a) Necessary for our legitimate interests (running our business, IT administration, network security, fraud prevention, and business continuity) (b) Necessary to comply with a legal obligation
To use aggregated and anonymised usage information to improve Report Wizard and understand how the software is used	Aggregated Usage Data (not personal data in our hands, as end users are not identifiable to us)	Not applicable (data is not personal data once aggregated and de-identified)

2.3 Direct marketing

We may use Your Personal Data to contact You with newsletters, marketing or promotional materials and other information that may be of interest to You. You may opt-out of receiving any, or all, of these communications from Us by following the unsubscribe link or instructions provided in any email We send or by contacting Us at dentalreportingai@icloud.com

2.4 Third-party marketing

We will get your express consent before we share your personal data with any third party for their own direct marketing purposes.

2.5 Opting out of marketing

You can ask to stop sending you marketing communications at any time by following the opt-out links within any marketing communication sent to you or by contacting us at dentalreportingai@icloud.com

If you opt out of receiving marketing communications, you will still receive service-related communications that are essential for administrative or customer service purposes.

2.6 Cookies

We use Cookies and similar tracking technologies to track the activity on Our Service and store certain information. Tracking technologies used are beacons, tags, and scripts to collect

and track information and to improve and analyse Our Service. The technologies We use may include:

- **Cookies or Browser Cookies:** A cookie is a small file placed on Your Device. You can instruct Your browser to refuse all Cookies or to indicate when a Cookie is being sent. However, if You do not accept Cookies, You may not be able to use some parts of our Service. Unless you have adjusted Your browser setting so that it will refuse Cookies, our Service may use Cookies.
- **Web Beacons:** Certain sections of our Service and our emails may contain small electronic files known as web beacons (also referred to as clear gifs, pixel tags, and single-pixel gifs) that permit the Company, for example, to count users who have visited those pages or opened an email and for other related website statistics (for example, recording the popularity of a certain section and verifying system and server integrity).

Cookies can be "Persistent" or "Session" Cookies. Persistent Cookies remain on Your personal computer or mobile device when You go offline, while Session Cookies are deleted as soon as You close Your web browser. We use both Session and Persistent Cookies for the purposes set out below:

- **Necessary / Essential Cookies**

Type: Session Cookies

Administered by: Us

Purpose: These Cookies are essential to provide You with services available through the Website and to enable You to use some of its features. They help to authenticate users and prevent fraudulent use of user accounts. Without these Cookies, the services that You have asked for cannot be provided, and We only use these Cookies to provide You with those services.

- **Cookies Policy / Notice Acceptance Cookies**

Type: Persistent Cookies

Administered by: Us

Purpose: These Cookies identify if users have accepted the use of cookies on the Website.

- **Functionality Cookies**

Type: Persistent Cookies

Administered by: Us

Purpose: These Cookies allow us to remember choices You make when You use the Website, such as remembering your login details or language preference. The purpose of these Cookies is to provide You with a more personal experience and to avoid You having to re-enter your preferences every time You use the Website.

- **Tracking and Performance Cookies**

Type: Persistent Cookies

Administered by: Third-Parties

Purpose: These Cookies are used to track information about traffic to the Website and how users use the Website. The information gathered via these Cookies may directly or indirectly identify you as an individual visitor. This is because the information collected is typically linked to a pseudonymous identifier associated with the device you use to access

the Website. We may also use these Cookies to test new pages, features or new functionality of the Website to see how our users react to them.

3.0 Disclosures of your personal data

We may share your personal data where necessary with external third parties who provide services to us, e.g: cloud service providers and technology services, or clinical research organisations. We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We have Data Processing Agreements in place with these third party providers and we do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions. We do not sell your data to anyone and only share it with our contracted processors.

We also may share your personal data where necessary with the parties set out below for the purposes set out in the table above.

3.1 Business Transactions

If the Company is involved in a merger, acquisition or asset sale, Your Personal Data may be transferred. Alternatively, we may seek to acquire other businesses or merge with them. We will provide notice before Your Personal Data is transferred and becomes subject to a different Privacy Policy.

3.2 Law enforcement

Under certain circumstances, the Company may be required to disclose Your Personal Data if required to do so by law or in response to valid requests by public authorities (e.g. a court or a government agency).

3.3 Other legal requirements

The Company may disclose Your Personal Data in the good faith belief that such action is necessary to:

- Comply with a legal obligation
- Protect and defend the rights or property of the Company
- Prevent or investigate possible wrongdoing in connection with the Service
- Protect the personal safety of Users of the Service or the public
- Protect against legal liability

4.0 International transfers

We may transfer your personal data to service providers that carry out certain functions on our behalf. This may involve transferring personal data outside the UK or EEA to countries which have laws that do not provide the same level of data protection as the UK or EU law.

Whenever we transfer your personal data out of the UK or EEA to service providers, we ensure a similar degree of protection is afforded to it by ensuring that the following safeguards are in place:

- We will only transfer your personal data to countries that have been deemed by the UK or the EU to provide an adequate level of protection for personal data; or
- We may use specific standard contractual terms approved for use in the UK and/or EEA which give the transferred personal data the same protection as it has in the UK or EEA, or another transfer mechanism which has been approved by the relevant regulator in the UK and/or the EEA. To obtain a copy of these contractual safeguards, please contact us at dentalreportingai@icloud.com

5.0 Data security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

6.0 Data retention

6.1 How long will you use my personal data for?

Your information is securely stored. Dental Reporting AI will retain Your Personal Data only for as long as is necessary for the purposes set out in this Privacy Notice.

We will retain and use Your Personal Data to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies. The Company will also retain Usage Data for internal analysis purposes. Usage Data is generally retained for a shorter period of time, except when this data is used to strengthen the security or to improve the functionality of Our Service, or We are legally obligated to retain this data for longer time periods.

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

In some circumstances we will anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

7.0 Protecting your sensitive data

Dental Reporting AI follows the information security values of

- confidentiality - making sure your information is always kept secret and private;
- integrity - we ensure the completeness, consistency, and accuracy of the data over its lifecycle; and
- availability - we ensure the right information is available to the right person at the right time.

We use the following techniques and best practices to protect your sensitive data:

7.1 People

- Training - All staff receive regular appropriate training on data protection and security and their related duties to ensuring your personal data is secure;
- Minimised access: your personal data, including Health Data, can only be accessed on a strictly needs to know basis by our admin staff, or customer support as and when necessary, specifically as relates to your particular request for support;

7.2 Cyber resiliency, business continuity, and disaster recovery

- We utilise the most secure and resilient infrastructure from Render which ensures servers are always patched and up to date.
- Web servers store no sensitive information. Automated tests are performed internally across the codebase on every commit.
- In addition, we commit to undertaking annual third-party security audits with certified security auditors including web, desktop and mobile application penetration tests to ensure comprehensive coverage.

7.3 Technology

We adopt principles of Secure by Design, including:

- Architecture in line with industry standards.
- This includes role based access controls.
- Our REST APIs utilise authentication and authorization to ensure data minimization and prevent unauthorised access to data.
- Our password quality validation for users ensures only strong passwords are allowed and are stored hashed using SHA-256.

We use encryption in all of the following scenarios:

- In transit using modern protocols (TLS only) and secure ciphers (both internally within the VPC and externally with users & applications)
- At rest using AES-256 encryption

Data centres:

- We host data in multiple availability zones/regions in order to maximise availability. All production environments are located within the UK and EEA.
- Where possible, deploy a High Availability (HA) architecture to ensure resilience with automated failover to provide uninterrupted service.

Development, security & operations:

- We operate a mature secure software development life cycle (SDLC), which includes but is not limited to:
 - Separation of keys for each environment and robust key management processes
 - Regular dependency and package management audits and remediation
 - Logical separation of production and development environments including isolated databases
 - Static code testing to ensure code is free from known vulnerabilities
 - Dynamic code testing to ensure applications do not expose vulnerabilities
 - Manual security testing (annual penetration test)

8.0 Your legal rights

You have a number of rights under data protection laws in relation to your personal data.

You have the right to:

- Request **access** to your personal data (commonly known as a "subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- Request **correction** of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.
- Request **erasure** of your personal data in certain circumstances. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.
- **Object to processing** of your personal data where we are relying on a legitimate interest (or those of a third party) as the legal basis for that particular use of your data (including carrying out profiling based on our legitimate interests). In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your right to object.
- You also have the absolute right to object any time to the processing of your personal data for direct marketing purposes.

- Request the **transfer** of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.
- Withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.
- Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in one of the following scenarios:
 - If you want us to establish the data's accuracy;
 - Where our use of the data is unlawful but you do not want us to erase it;
 - Where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or
 - You have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.
 - If you wish to exercise any of the rights set out above, please contact us at dentalreportingai@icloud.com

8.1 No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we could refuse to comply with your request in these circumstances.

8.2 What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

8.3 Time limit to respond

We try to respond to all legitimate requests within one month. Occasionally it could take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

9.0 Contact details

If you have any questions about this Privacy Notice or about the use of your personal data or you want to exercise your privacy rights, please contact us in the following ways:

- Email address: dentalreportingai@icloud.com

10.0 Complaints

You have the right to make a complaint to us if you believe that our processing of your personal data infringes any part of the UK GDPR. You also have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK regulator for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

11.0 Changes to the Privacy Notice and your duty to inform us of changes

We keep our Privacy Notice under regular review. This version was last updated in Aug 21, 2026.

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us, for example a new address or email address.

12.0 Third-party links

This website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the Privacy Notice of every website you visit.

We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

13.0 Payments

We may provide paid products and/or services within the Service. In that case, we may use third-party services for payment processing (e.g. payment processors). We will not store or collect Your payment card details. That information is provided directly to Our third-party payment processors whose use of Your personal information is governed by their Privacy Notice.