



BRIGHT HEARTS – PRIVACY POLICY

Bright Hearts Ltd (ABN 54 672 467 711) (we, us or our) understands that protecting your personal information is important. This Privacy Policy sets out our commitment to protecting the privacy of personal information provided to us, or collected by us, when interacting with you.

This Privacy Policy was last updated on 1 July 2026. This Privacy Policy is next scheduled for review on 7 July 2027.

In this Privacy Policy the word Dependent means your child, or another minor who is in your custody.

CONTENTS

1.0 The Information We Collect *(Page 3)* 1.1 Personal Information | 1.2 Clinical Technology Data | 1.3 Surveillance Data | 1.4 Sensitive Information | 1.5 Funding Agency Data

2.0 How We Collect Personal Information *(Page 5)*

3.0 Why We Collect, Hold, Use and Disclose Personal Information *(Page 6)* 3.1 Personal Information | 3.2 Sensitive Information

4.0 Our Disclosures of Personal Information to Third Parties *(Page 7)* 4.1 Personal Information | 4.2 Sensitive Information

5.0 Disclosure for Child Safety and Wellbeing *(Page 9)*

6.0 Google Analytics *(Page 9)*

7.0 Overseas Disclosure *(Page 9)*

8.0 Your Rights and Controlling Your Personal Information *(Page 10)* 8.1 Your Choice | 8.2 Information from Third Parties | 8.3 Restrict and Unsubscribe | 8.4 Access | 8.5 Correction | 8.6 Complaints

9.0 Storage and Security *(Page 11)*

10.0 Cookies *(Page 11)*

11.0 Links to Other Websites *(Page 11)*

12.0 Amendments *(Page 11)*

13.0 Governance: Clinical Technology, Surveillance, and Data *(Page 12)* 13.1 Cloud-Based Practice Management (Splose) | 13.2 Administrative Clinical AI Scribing (Heidi AI) | 13.3 General Clinic CCTV (Safety and Accountability Surveillance) | 13.4 Targeted Clinical Video Recording (Therapeutic and Evidence Management) | 13.5 Participant Rights and Consent

14.0 Contact Us *(Page 14)*

15.0 Privacy Collection Notice *(Page 15)*

1.0 THE INFORMATION WE COLLECT

1.0.1 Personal information is information or an opinion, whether true or not and whether recorded in a material form or not, about an individual who is identified or reasonably identifiable.

1.1 Personal Information

1.1.1 The types of personal information we may collect about you (or your Dependent) include:

1.1.2 Identity Data including name, age, photographic identification, and gender.

1.1.3 Contact Data including telephone number, address and email.

1.1.4 Financial Data (where you are a paying client of ours) including bank account and payment card details (through our third party payment processor, who stores such information and we do not have access to that information).

1.1.5 Background Verification Data (where you are an employee) including your government-issued identification details requested as part of our onboarding or verification or Know Your Customer process to comply with our due diligence obligations, anti-money laundering laws and related ongoing monitoring commitments.

1.1.6 Transaction Data including details about payments to you from us and from you to us and other details of products and services you have purchased from us or we have purchased from you.

1.1.7 Technical and Usage Data when you access any of our websites or platforms, details about your internet protocol (IP) address, login data, browser session and geo-location data, statistics on page views and sessions, device and network information, acquisition sources, search queries and/or browsing behaviour, access and use of our website (including through the use of Internet cookies or analytics), and communications with our website.

1.1.8 Interaction Data including information you provide to us when you participate in any interactive features, including surveys, contests, promotions, activities or events.

1.1.9 Marketing and Communications Data including your preferences in receiving marketing from us and our third parties and your communication preferences.

1.1.10 Professional Data including where you are a worker of ours or applying for a role with us, your professional history such as your previous positions and professional experience.

1.2 Clinical Technology Data

1.2.1 We may collect session audio recordings, AI-generated draft clinical progress notes, and targeted clinical video recordings captured in the course of providing therapeutic services, where explicit written consent has been obtained from the Child Representative. Full details of how this data is collected, stored, and protected are set out in section 13.0 of this policy.

1.3 Surveillance Data

1.3.1 We collect general clinic CCTV footage captured for the purposes of safety and accountability within our clinical premises. Signage is displayed at the entrance to all Bright Hearts clinic locations to notify participants, caregivers, and visitors of CCTV operation. Full details are set out in section 13.3 of this policy.

1.4 Sensitive Information

1.4.1 Sensitive information is a sub-set of personal information that is given a higher level of protection. Sensitive information means information relating to your racial or ethnic origin, political opinions, religion, trade union or other professional associations or memberships, philosophical beliefs, sexual orientation or practices, criminal records, health information or biometric information.

1.4.2 The types of sensitive information we may collect include:

1.4.3 Your (or your Dependent's) racial or ethnic origin, religious beliefs, health information, and sexual orientation.

1.4.4 Your (or your Dependent's) education records as well as any court records detailing criminal history or involvement in legal action.

1.4.5 Your (or your Dependent's) NDIS plans and any other support plan you provide us with.

1.4.6 Diagnoses of any disorders or illnesses, and medical imaging.

1.4.7 Any therapies, treatments or medications that you (or your Dependent) are currently receiving or have received, and any records of such therapies, treatments or medications.

1.5 Funding Agency Data

1.5.1 Where you are a client who has been referred to us by a third party funding agency (Funding Agency), in addition to the above we may also collect:

1.5.2 Funding Agency Data including the name of the Funding Agency, any identifying number you have, and any other details included in the referral form (which may include names of other service and health care providers).

1.5.3 In addition to the sensitive information categories listed in section 1.4, your referral number and details of funding allocated to you by the Funding Agency.

2.0 HOW WE COLLECT PERSONAL INFORMATION

2.0.1 We collect personal information in a variety of ways, including:

2.0.2 When you provide it directly to us, including face-to-face, over the phone, over email, or online.

2.0.3 When you complete a form, such as an intake form, informed consent document, service agreement, referral form, or when registering for events or newsletters, or responding to surveys.

2.0.4 When you use any website we operate (including from any analytics and cookie providers or marketing providers — see section 10.0 for more detail on the use of cookies).

2.0.5 From third parties, such as the NDIS, any Funding Agency, doctors, educators, health practitioners or any other service providers, your family members or significant others.

2.0.6 From publicly available sources.

2.0.7 Through our cloud-based practice management system (Splose) in the course of scheduling, clinical record-keeping, and NDIS billing (see section 13.1).

2.0.8 Through AI-assisted clinical scribing (Heidi AI), where you have provided explicit written consent, by way of session audio transcription used solely to generate draft clinical progress notes (see section 13.2).

2.0.9 Through our general safety CCTV infrastructure (see section 13.3).

2.0.10 Through targeted clinical video recordings that form part of your clinical health record, where explicit written consent has been obtained (see section 13.4).

3.0 WHY WE COLLECT, HOLD, USE AND DISCLOSE PERSONAL INFORMATION

3.1 Personal Information

3.1.1 We collect, hold, use and disclose your personal information for the following purposes:

3.1.2 To do business with you (or your Dependent), including to assess your application and manage your appointments.

3.1.3 To contact and communicate with you about our business, including in response to any support requests you lodge with us or other enquiries you make with us.

3.1.4 To contact and communicate with you about any enquiries you make with us via any website we operate.

3.1.5 For internal record keeping, administrative, invoicing and billing purposes.

3.1.6 For analytics, market research and business development, including to operate and improve our business, associated applications and associated social media platforms.

3.1.7 If you have applied for employment with us, to consider your employment application.

3.1.8 To comply with our legal obligations or if otherwise required or authorised by law.

3.2 Sensitive Information

3.2.1 We only collect, hold, use and disclose sensitive information for the following purposes:

3.2.2 Any purposes you consent to.

3.2.3 The primary purpose for which it is collected, which is to ensure that we can safely provide our services to you (or your Dependent) with appropriate equipment and tools to keep you (or your Dependent) and us safe.

3.2.4 Secondary purposes that are directly related to the primary purpose for which it was collected, including disclosure to the third parties listed in section 4.2 as reasonably necessary to do business with you.

3.2.5 To contact emergency services, or to speak with your family, partner or support person where we reasonably believe there is a serious risk to the life, health or safety of you or another person and it is impracticable for us to obtain your consent.

3.2.6 If otherwise required or authorised by law.

4.0 OUR DISCLOSURES OF PERSONAL INFORMATION TO THIRD PARTIES

4.1 Personal Information

4.1.1 We will only disclose personal information (excluding sensitive information) to third parties where it is necessary as part of our business or to provide you (or your Dependent) with our services, where we have your consent, or where permitted by law. This means that we may disclose personal information (excluding sensitive information) to:

4.1.2 Our employees, contractors and/or related entities.

4.1.3 IT service providers, data storage, web-hosting and server providers.

4.1.4 Marketing or advertising providers.

4.1.5 Professional advisors, bankers, auditors, our insurers and insurance brokers.

4.1.6 Payment systems operators or processors.

4.1.7 Our existing or potential agents or business partners.

4.1.8 If we merge with, or are acquired by, another company, or sell all or a portion of our assets, your personal information may be disclosed to our advisers and any prospective purchaser's advisers and may be among the assets transferred.

4.1.9 Courts, tribunals and regulatory authorities, in the event you fail to pay for goods or services we have provided to you.

4.1.10 Courts, tribunals, regulatory authorities and law enforcement officers, as required or authorised by law, in connection with any actual or prospective legal proceedings, or in order to establish, exercise or defend our legal rights.

4.1.11 Your Funding Agency and other service providers involved in your or your Dependent's care.

4.1.12 Third parties to collect and process data, such as analytics providers and cookies.

4.1.13 Any other third parties authorised by you or as required or permitted by law, such as where we receive a subpoena.

4.2 Sensitive Information

4.2.1 We will only disclose sensitive information with your consent or where permitted by law. This means that we may disclose sensitive information to:

4.2.2 Our employees, contractors and/or related entities.

4.2.3 IT service providers, data storage, web-hosting and server providers, including our cloud-based practice management provider (Splose) and, where consent has been obtained,

our AI scribing provider (Heidi AI), each operating under formal data processing agreements aligned with the Australian Privacy Principles.

4.2.4 Professional advisors.

4.2.5 If we merge with, or are acquired by, another company, or sell all or a portion of our assets, your personal information may be disclosed to our advisers and any prospective purchaser's advisers and may be among the assets transferred.

4.2.6 Courts, tribunals, regulatory authorities and law enforcement officers, as required or authorised by law, in connection with any actual or prospective legal proceedings, or in order to establish, exercise or defend our legal rights.

4.2.7 Third parties to collect and process data, such as analytics providers and cookies.

4.2.8 Your Funding Agency and other service providers involved in your or your Dependent's care.

4.2.9 Any other third parties authorised by you or as required or permitted by law, such as where we receive a subpoena.

5.0 DISCLOSURE FOR CHILD SAFETY AND WELLBEING

5.0.1 Notwithstanding other provisions in this policy, we may share information (including sensitive clinical records) with other prescribed bodies (such as NGOs, ACCOs, or government agencies) under Chapter 16A of the Children and Young Persons (Care and Protection) Act 1998 (NSW).

5.0.2 This occurs when the disclosure is believed, in good faith, to be necessary for the safety, welfare, or well-being of a child or young person. In accordance with Section 245G of the Act, such disclosures do not constitute a breach of professional ethics or a violation of privacy and are protected from civil or criminal liability. This applies specifically to ensuring continuity of care during transitions between service providers, such as from an NGO to an Aboriginal Community Controlled Organisation (ACCO).

6.0 GOOGLE ANALYTICS

6.0.1 We have enabled Google Analytics Advertising Features. Third-party vendors, including Google, may use first-party cookies (such as the Google Analytics cookie) or other first-party identifiers, and third-party cookies (such as Google advertising cookies) or other third-party identifiers together. These cookies and identifiers may collect Technical and Usage Data about you.

6.0.2 You can opt-out of Google Analytics Advertising Features by using a Google Analytics Opt-out Browser Add-on. To opt-out of personalised ad delivery on the Google content network, please visit Google's Ads Preferences Manager. To opt out of interest-based ads on mobile devices: on Android, open the Google Settings app and select Ads to control the settings; on iOS devices with iOS 6 and above, use Apple's advertising identifier via the Settings menu on your device. To find out how Google uses data when you use third party websites or applications, please refer to Google's privacy documentation.

7.0 OVERSEAS DISCLOSURE

7.0.1 If you are a Funding Agency disclosing information to us, you warrant that you are only disclosing information which you are allowed to disclose and have all reasonable consents required to disclose such information.

7.0.2 We store your personal information in Australia. Where we disclose your personal information to third parties, those 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.

8.0 YOUR RIGHTS AND CONTROLLING YOUR PERSONAL INFORMATION

8.1 Your Choice

8.1.1 Please read this Privacy Policy carefully. If you provide personal information to us, you understand we will collect, hold, use and disclose your personal information in accordance with this Privacy Policy. You do not have to provide personal information to us, however, if you do not, it may affect our ability to do business with you.

8.2 Information from Third Parties

8.2.1 If we receive personal information about you from a third party, we will protect it as set out in this Privacy Policy. If you are a third party providing personal information about somebody else, you represent and warrant that you have such person's consent to provide the personal information to us.

8.3 Restrict and Unsubscribe

8.3.1 To object to processing for direct marketing or to unsubscribe from our email database or opt-out of communications (including marketing communications), please contact us using the details below or opt-out using the opt-out facilities provided in the communication.

8.4 Access

8.4.1 You may request access to the personal information that we hold about you. An administrative fee may be payable for the provision of such information. Please note, in some situations, we may be legally permitted to withhold access to your personal information. If we cannot provide access to your information, we will advise you as soon as reasonably possible and provide you with the reasons for our refusal and any mechanism available to complain about the refusal. If we can provide access to your information in another form that still meets your needs, then we will take reasonable steps to give you such access.

8.5 Correction

8.5.1 If you believe that any information we hold about you is inaccurate, out of date, incomplete, irrelevant or misleading, please contact us using the details below. We will take reasonable steps to promptly correct any information found to be inaccurate, out of date, incomplete, irrelevant or misleading. Please note, in some situations, we may be legally permitted to not correct your personal information. If we cannot correct your information, we will advise you as soon as reasonably possible and provide you with the reasons for our refusal and any mechanism available to complain about the refusal.

8.6 Complaints

8.6.1 If you wish to make a complaint, please contact us using the details below and provide us with full details of the complaint. We will promptly investigate your complaint and respond to you, in writing, setting out the outcome of our investigation and the steps we will take in response to your complaint. If you are not satisfied with our response, you may contact the Office of the Australian Information Commissioner.

9.0 STORAGE AND SECURITY

9.0.1 We are committed to ensuring that the personal information we collect is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure personal information and protect it from misuse, interference, loss and unauthorised access, modification and disclosure.

9.0.2 While we are committed to security, we cannot guarantee the security of any information that is transmitted to or by us over the Internet. The transmission and exchange of information is carried out at your own risk.

10.0 COOKIES

10.0.1 We may use cookies on our website from time to time. Cookies are text files placed in your computer's browser to store your preferences. Cookies, by themselves, do not tell us your email address or other personally identifiable information. However, they do recognise you when you return to our online website and allow third parties to cause our advertisements to appear on your social media and online media feeds as part of our retargeting campaigns. If and when you choose to provide our online website with personal information, this information may be linked to the data stored in the cookie.

10.0.2 You can block cookies by activating the setting on your browser that allows you to refuse the setting of all or some cookies. However, if you use your browser settings to block all cookies (including essential cookies) you may not be able to access all or parts of our website.

11.0 LINKS TO OTHER WEBSITES

11.0.1 Our website may contain links to other parties' websites. We do not have any control over those websites and we are not responsible for the protection and privacy of any personal information which you provide whilst visiting those websites. Those websites are not governed by this Privacy Policy.

12.0 AMENDMENTS

12.0.1 We may, at any time and at our discretion, vary this Privacy Policy by publishing the amended Privacy Policy on our website. We recommend you check our website regularly to ensure you are aware of our current Privacy Policy.

13.0 GOVERNANCE: CLINICAL TECHNOLOGY, SURVEILLANCE, AND DATA

13.0.1 To ensure transparency and compliance with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), the Health Records and Information Privacy Act 2002 (NSW), and the NDIS Quality and Safeguards Commission standards, this section outlines how Bright Hearts Ltd manages, processes, and secures participant data across our digital platforms, clinic surveillance systems, and clinical video archives.

13.1 Cloud-Based Practice Management (Splose)

13.1.1 Bright Hearts Ltd utilises Splose as our primary secure Practice Management System to host digital health files, manage scheduling, and process NDIS billing.

13.1.2 Data Residency and Sovereignty (APP 8): All core participant records, database clusters, and clinical files are hosted on Amazon Web Services (AWS) infrastructure within the Sydney Region (ap-southeast-2). No participant data is transferred or stored outside of Australia.

13.1.3 Security and Encryption (APP 11): Data is protected using AES-256 encryption at rest and TLS 1.2+ encryption in transit. Access is restricted via platform-wide Multi-Factor Authentication (MFA) and granular, role-based access controls with audit logging.

13.1.4 AI Processing and Zero Data Retention: Where Splose's opt-in generative AI tools are utilised, processing is governed by a formal Business Associate Agreement (BAA) with the relevant AI processing provider. This legally binds the processing layer to a Zero Data Retention (ZDR) policy, ensuring clinical data is not stored beyond the immediate processing task and is never used to train public AI models.

13.2 Administrative Clinical AI Scribing (Heidi AI)

13.2.1 To maximise direct therapeutic contact time and reduce administrative burden for NDIS participants, our practitioners may utilise Heidi AI to assist in transcribing session audio and drafting clinical progress notes, where explicit written consent has been obtained from the Child Representative.

13.2.2 Human-in-the-Loop Control: Heidi AI functions strictly as an administrative transcription assistant. No clinical note is auto-submitted or finalised by the software. Your Bright Hearts practitioner personally reads, reviews, edits, and validates every draft note to ensure clinical accuracy prior to finalisation.

13.2.3 24-Hour Finalisation Rule: All clinical progress notes are finalised and securely locked within Splose within 24 hours of the session taking place.

13.2.4 Data Sovereignty and Security: Heidi AI processes and stores data on geographically ring-fenced AWS infrastructure located within Australia. The platform's security controls are independently validated through SOC 2 Type II Certification and are governed by a formal Data Processing Addendum (DPA) aligned with the APPs.

13.2.5 Zero AI Model Training: Under our data processing agreements, raw session audio is temporary and is permanently deleted once the clinical draft note is generated. Participant data is never used to train public AI models.

13.3 General Clinic CCTV (Safety and Accountability Surveillance)

13.3.1 Purpose: To ensure the physical safety and accountability of all participants, staff, and visitors within clinical playrooms and common areas.

13.3.2 Notice: Signage is displayed at the entrance to all Bright Hearts clinic premises to notify participants, caregivers, and visitors of CCTV operation prior to entry.

13.3.3 Storage and Deletion: Footage is captured automatically, stored locally on an encrypted system, and is automatically overwritten and permanently deleted after thirty (30) days, unless required for an active incident investigation or as otherwise required by law.

13.3.4 Access: Access to general CCTV footage is restricted to authorised personnel and is only reviewed in response to a documented safety incident, complaint, or lawful request.

13.4 Targeted Clinical Video Recording (Therapeutic and Evidence Management)

13.4.1 Purpose: To capture specific interactions, motor responses, or behavioural presentations directly relevant to a child's ongoing clinical assessment, therapeutic tracking, or NDIS reporting.

13.4.2 Consent: Targeted clinical video recording requires explicit, opt-in written consent from the Child Representative, obtained prior to any recording taking place. This consent is documented within the participant's clinical file.

13.4.3 Storage and Archiving: Targeted clinical video recordings are intentionally isolated from general CCTV systems and are transferred to a high-security, fully air-gapped (offline) Solid-State Drive (SSD) housed in a secure server enclosure within our clinical premises.

13.4.4 Retention Period: As these recordings form part of the primary clinical health record, they are stored as read-only files and are legally and securely archived in accordance with the Health Records and Information Privacy Act 2002 (NSW) until the participant reaches twenty-five (25) years of age, or as otherwise required by applicable law.

13.5 Participant Rights and Consent

13.5.1 Explicit Consent: The use of Heidi AI session audio transcription and targeted clinical video recording each require separate, explicit, opt-in written consent from the Child Representative prior to use. Consent forms clearly describe the purpose, storage arrangements, and retention periods applicable to each technology and are provided as part of our clinical intake documentation.

13.5.2 Absolute Right to Opt Out: Caregivers hold the absolute right to withdraw consent for AI scribing, session audio recording, or targeted clinical video recording at any time, without penalty, reduction in the quality of care provided, or impact on NDIS funding entitlements.

Where consent is withdrawn or not provided, the treating practitioner will rely solely on contemporaneous manual written documentation.

13.5.3 General CCTV Notice: Participants, caregivers, and visitors are notified of general safety CCTV operation by signage displayed at the entrance to all clinic premises operated by Bright Hearts Ltd.

14.0 CONTACT US

14.0.1 For any questions or notices, please contact us at:

Bright Hearts Ltd (ABN 54 672 467 711) Email: connect@brighthearts.org.au

© *LegalVision ILP Pty Ltd*

15.0 PRIVACY COLLECTION NOTICE

Bright Hearts Ltd (ABN 54 672 467 711)

Last updated: 1 July 2026 | Next review: 7 July 2027

15.0.1 This Privacy Collection Notice describes how Bright Hearts Ltd (ABN 54 672 467 711) (we, us or our) collects and handles your personal information when you make an enquiry with us or engage our services, including when you complete clinical intake documentation such as informed consent forms, service agreements, or referral forms.

15.0.2 We collect personal information from you so that we can respond to your enquiry and for related purposes set out in our Privacy Policy, which is provided to you as a link in your clinical documentation and is available on our website or on request.

15.0.3 We may also collect personal information through our clinical operations, including via our cloud-based practice management system (Splose), AI-assisted clinical scribing (Heidi AI) where explicit written consent has been provided, and clinic video infrastructure including general safety CCTV and targeted clinical video recording where explicit written consent has been provided. Full details of these technologies, their purposes, data storage arrangements, retention periods, and your rights — including your absolute right to opt out — are set out in the Governance section of our Privacy Policy.

15.0.4 We may disclose personal information to third parties, including our personnel, related entities, technology and data service providers operating under formal data processing agreements, and as otherwise set out in our Privacy Policy.

15.0.5 We store personal information in Australia. Where we disclose your personal information to third parties, those third parties may store, transfer or access personal information outside of Australia, in accordance with the Australian Privacy Principles.

15.0.6 If you do not provide your personal information to us, it may affect our ability to do business with you or provide services to you or your Dependent.

15.0.7 Please see our full Privacy Policy for information about how we collect, store, use and disclose your personal information, including details about overseas disclosure, your rights of access and correction, how to make a privacy-related complaint, and our complaint-handling process.

15.0.8 If you have questions about our privacy practices, please contact us at:
connect@brighthouse.org.au

15.0.9 By providing your personal information to us, you agree to the collection, use, storage and disclosure of that information as described in this Privacy Collection Notice and our Privacy Policy.