Secure Client Record Keeping Policy

Document Version: 1.0
Effective Date: 02/12/2025
Review Date: 18/12/2026
Approved By: Tegan Elza Banks - The Director/Lead Therapist

1. Purpose

This policy outlines Forge Clarity's approach to secure client record keeping for our private telehealth/remote counselling practice. It ensures compliance with:
- National Disability Insurance Scheme (NDIS) Practice Standards
- Privacy Act 1988 (Cth)
- Australian Privacy Principles (APPs)
- Health Records Act (state-specific where applicable)
- Professional standards for mental health practitioners

2. Scope

This policy applies to:
- All counselling and mental health practitioners who volunteer, are employed by or contracted to Forge Clarity
- All client records created during telehealth/remote counselling sessions
- Digital and physical record keeping systems
- Free Zoom Grief Support Group records
- All staff and volunteers involved in service delivery

3. Core Principles

3.1 Client Confidentiality
- Client privacy is paramount in all record-keeping activities
- Access to identifiable information is strictly limited, only the Director/Lead Therapist has access to client records. Volunteers only take notes based on whichever name the individual chooses to have shown on their Zoom screen
- Physical and digital security measures protect client data. For instance no client full names are used outside of the Client Liability Waiver & Agreement unless required due to emergency or being legally mandated to provide documents in accordance with the law.

3.2 De-identification System
- Digital client records use unique client codes only
- Client legal names are not stored in digital systems except for the signed pdf copy of the Client Liability Waiver & Agreement. Which is once a month printed and stored in a locked cabinet and behind three passcodes. These passcodes are to the laptops, to the system, and to the file that holds the Client Liability Waiver & Agreements.
- The link between legal names and codes is maintained separately in physical format only that is also kept in a locked cabinet

3.3 Minimum Necessary Access
- Only the Director/Lead Therapist can access information necessary for the task required. Volunteers use the client name they choose to display via Zoom during the free grief support group
- Role-based access controls limit exposure of sensitive information

4. Client Code System

4.1 Code Structure
- Each client is assigned a unique alphanumeric code upon intake (e.g., 0001)
- Codes follow the format: 0001 or 0002 etc
- Codes are never reused, even after client discharges for over seven years (seven years is the legal minimum requirement for records about clients to be kept)

4.2 Code Assignment Process
1. New client contacts Forge Clarity
2. Intake staff, the Director/Lead Therapist, creates new entry in Physical Client Ledger
3. Sequential client code is assigned
4. Client legal name, code, emergency contact information, and date of first contact are recorded in ledger only
5. All digital records use client code exclusively

4.3 Physical Client Ledger

Contents:
- Client legal full name
- Assigned client code
- Date of first contact
- Emergency contact information (name and phone only)

Security Measures:
- Ledger stored in locked filing cabinet
- Cabinet located in secure office area
- Access limited to authorised parties only
- Key control log maintained
- Ledger never leaves premises
- No photocopying or digital photography permitted of the physical ledger - if the ledger is damaged or stolen, clients are notified as soon as possible.

Access Protocol:
- Only the Director/Lead Therapist can sign ledger access log with date, time, and purpose
- Ledger returned to locked cabinet immediately after use
- Cabinet checked and locked at end of each business day

5. Digital Record Keeping

5.1 Information Stored Digitally
All digital records use client codes only and may include:
- Session notes and progress reports
- Treatment plans and goals
- Risk assessments
- Consent forms (signed with client code)
- Communication logs
- Billing and payment records (linked by code)

- Outcome measurement tools and scores
- Referral documentation
Only the Director/Lead Therapist has access to these documents/systems.

5.2 Prohibited Digital Information
The following information is NEVER stored digitally:
- Client legal full names in a file outside of the original copy of the Client Liability Waiver & Agreement
- Specific home addresses (locality/suburb/post code/country unless part of the session notes)
- Date of birth (year only if clinically necessary or part of the client session notes)
- Medicare/Centrelink/NDIS participant numbers (unless required specifically for that document, for instance an NDIS audit, or an official document that requires said details. Review: https://forgeclarity.com.au/documents)
- Photos of clients. At no point will Forge Clarity, the staff or volunteer team ever ask for photos of clients. If this occurs we encourage everyone who witnessed anything to come forward. This falls under the Whistle Blower Protection Policy and you can make an anonymous report here: https://forgeclarity.com.au/documents in the Anonymous Feedback section.
- Audio/video recordings without explicit consent and encryption. At no point will Forge Clarity, the staff or volunteer team ever ask for photos of clients. If this occurs we encourage everyone who witnessed anything to come forward. This falls under the Whistle Blower Protection Policy and you can make an anonymous report here: https://forgeclarity.com.au/documents in the Anonymous Feedback section.

5.3 Digital Security Requirements

Access Controls:
- Multi-factor authentication (MFA) required for all systems
- Unique user credentials for the Director (volunteers do not have access to the system, they only assist in taking group notes and then pass those notes onto the Director. For additional layer of confidentiality the volunteers service in rotations so that they only provide support once a month.)
- Automatic logout after 10 minutes of inactivity
- Role-based access permissions

Data Protection:
- End-to-end encryption for data at rest and in transit
- Australian-based secure cloud storage with ISO 27001 certification
- Regular automated backups (encrypted)
- Secure password manager for credential storage

Device Security:
- Devices password-protected and encrypted
- Anti-virus and firewall software current
- Operating systems and applications regularly updated
- Devices never left unattended while logged in
- No use of public Wi-Fi for accessing client records - only private hotspotting/tethering from Director/Lead Therapist phone to device such as laptop.

6. Telehealth Session Documentation Template

6.1 Session Notes Content
Each session note includes:
- Client code
- Date and time of session
- Duration
- Service type (individual counselling, grief support, etc.)
- Session content summary
- Interventions used
- Client progress toward goals
- Risk assessment (if applicable)
- Plan for next session
- Practitioner name/credentials

6.2 NDIS-Specific Requirements
For NDIS participants, additionally document:
- Alignment with NDIS goals and plan
- Progress toward stated outcomes
- Any barriers to goal achievement
- Coordination with other supports
- Reasonable and necessary justification for service

6.3 Timeliness
- Session notes completed within 24 hours of session
- NDIS progress reports completed within required timeframes
- Urgent risk documentation completed immediately

7. Free Zoom Grief Support Group Records

7.1 Volunteer Access Limitations
Volunteers facilitating grief support groups:
- Do NOT have access to client records
- Do NOT see client codes
- Only see Zoom display names chosen by participants
- Cannot link participants to counselling clients serviced by the Director/Lead Therapist unless the client shares said details in group session.

7.2 Group Session Documentation

Volunteer Responsibilities:
- Record date of group session
- Note number of attendees (no names or identifying info)
- Document topics discussed (general themes only)
- Record any resources shared and take notes of what each member shares
- Report any risk concerns to supervising practitioner immediately

Volunteer Notes Include:
- Session date and facilitator name
- Attendance count only (no identifiable information)
- General group themes and topics
- Resources or referrals provided
- Any critical incidents or risk concerns (described without identifying details)

Volunteer Notes Do NOT Include:
- Participant names (unless they choose to share it via Zoom or otherwise)
- Specific identifying stories or details - unless deeply relevant to the notes
- Connection to any client codes
- Personal information about participants (unless participants choose to share)

7.3 Risk Management for Support Groups
If a volunteer identifies a participant at risk:
1. Follow immediate risk protocols during session
2. Report to supervising practitioner using only general descriptions
3. Do not attempt to identify participant outside of session
4. Supervising practitioner determines if follow-up possible/appropriate
5. Documentation filed separately from client records

8. Record Access and Security

8.1 Authorised Access Levels

Level 1 - Full Access (Director/Lead Therapist):
- Physical ledger
- All digital client records
- System administration

Level 2 - (Director/Lead Therapist):
- Physical ledger (supervised access for intake/emergency only)
- Digital records for assigned clients only
- Can access other practitioners' client notes

Level 3 - Volunteer Access:
- No group attendance records only (de-identified)
- No access to client records or physical ledger
- No access to individual client information
- Only access to an empty “Grief Group Week Client Notes Template” that they use the nominated Zoom name of each attendee.

8.2 Audit Trail
- All digital system access logged automatically
- Physical ledger access recorded in access log
- Quarterly audit of access logs conducted

- Annual security review completed

9. Client Rights and Access

9.1 Client Access to Own Records
Clients have the right to:
- Request access to their records
- Receive explanation of information contained in records
- Request corrections to factual errors
- Understand how their information is used and stored
Which is outlined in the Client Liability Waiver & Agreement and Privacy Policy located: https://forgeclarity.com.au/documents

9.2 Access Request Process
1. Client submits written request
2. Identity verification completed (via phone or telehealth) In order to release the information Forge Clarity needs to confirm the clients identity. This involves asking them for their full legal name, phone number, address, birth date, emergency contact, NDIS number etc.
3. Records reviewed by practitioner for third-party information
4. Access provided within 30 days
5. Access method: confirm identity, Director accesses secure portal, encrypted email, or telehealth review

10. Record Retention and Disposal

10.1 Retention Periods
- Adult client records: 7 years from last contact
- NDIS records: 7 years from service delivery or as required by funding agreement
- Group session notes (volunteer): 7 years

10.2 Secure Disposal
Digital Records:
- Securely deleted using data wiping software
- Confirmed deletion from backups and cloud storage
- Disposal documented in destruction log. The only record kept of the past client is their unique client code and the details “As services to X were ended at Y and it has now passed the seven year minimum requirement the details of this client and their care are no longer available or retrievable.”

Physical Ledger Entries:
- Shredded using cross-cut shredder after retention period
- Disposal recorded in the Digital Client Ledger - only client code and detail of the destruction of records is left
- Ledger pages destroyed (never discarded whole)

11. Date Breach Response

11.1 Breach Definition
Any unauthorised access, disclosure, loss, or theft of:
- Physical client ledger
- Digital client records
- Client codes and associated information
- Volunteer notes containing participant information

11.2 Immediate Response Protocol
1. Contain breach and prevent further unauthorised access
2. Assess scope and severity
3. Document breach details thoroughly & contact Police as needed
4. Notify Office of the Australian Information Commissioner (OAIC)/ NDIS / ACA if required
5. Notify affected clients if serious harm likely
6. Implement corrective actions
7. Review and update security measures

11.3 Notification Requirements
Notify OAIC and affected clients if breach:
- Involves sensitive information
- Likely to result in serious harm
- Affects privacy in significant way

12. NDIS Compliance Requirements

12.1 NDIS Practice Standards Alignment
This policy supports compliance with:
- Core Module: Rights and responsibilities
- Core Module: Governance and operational management
- Supplementary Module: High Intensity Daily Personal Activities
- NDIS Code of Conduct requirements

12.2 NDIS-Specific Documentation
For NDIS participants, records demonstrate:
- Services aligned with participant NDIS plan
- Progress toward NDIS goals
- Choice and control respected
- Reasonable and necessary service delivery
- Safeguarding measures in place

12.3 NDIS Commission Requests
- Records provided to NDIS Commission within required timeframes
- De-identified data may be shared for quality/safeguarding purposes
- Client code system maintained for privacy during audits
- Physical ledger secured during Commission site visits

13. Staff and Volunteer Training

13.1 Mandatory Training
All staff and volunteers complete training on:
- This record keeping policy and procedures
- Privacy obligations and client confidentiality
- Client code system and ledger security
- Digital security and access protocols
- Role-specific record keeping requirements
- Data breach recognition and reporting

13.2 Training Frequency
- Initial training during onboarding
- Annual refresher training
- Additional training after policy updates
- Incident-specific training as needed

13.3 Training Documentation
- Training attendance recorded
- Competency assessment completed
- Training certificates filed
- Acknowledgment of policies etc is signed in the Liability Waiver for Volunteers

14. Policy Compliance

14.1 Staff Responsibilities
All staff members must:
- Follow this policy without exception
- Use client codes exclusively in digital systems
- Protect physical ledger security
- Report suspected breaches immediately
- Complete required training
- Maintain confidentiality at all times

14.2 Volunteer Responsibilities
All volunteers must:
- Document only de-identified group information
- Never attempt to identify participants outside sessions
- Report risk concerns without identifying details
- Complete confidentiality training
- Acknowledge access limitations

14.3 Consequences of Non-Compliance
- Retraining requirement
- Supervised practice period

- Access restrictions
- Performance management
- Termination of employment/volunteer role
- Professional body notification if applicable
- Legal consequences if warranted

15. Policy Review and Updates

15.1 Review Schedule
- Annual policy review by Practice Director/Lead Therapist
- Review after any data breach or security incident
- Review following changes to legislation or NDIS requirements
- Review following client complaints related to privacy

15.2 Update Process
1. Review conducted and changes drafted
2. Staff consulted on practical implications
3. Updated policy approved by Practice Owner
4. All staff and volunteers notified of changes
5. Training provided on updates
6. New acknowledgment forms signed

16. Related Policies and Documents

As located at https://forgeclarity.com.au/documents