**RingCentral Data & Privacy Terms and Conditions for Premier Service (245D-Compliant) **

1. INTRODUCTION These Terms and Conditions govern the use of RingCentral communication systems by Premier Service (“the Agency”) for 245D Home and Community-Based Services (HCBS). This document outlines how client data, staff data, call information, text messages, voicemails, and other communication records are protected, stored, accessed, and disclosed.

2. PURPOSE RingCentral is used strictly for service coordination, scheduling, case management communication, crisis response, remote support, and other authorized 245D activities. All data handled through RingCentral must comply with: - Minnesota Statutes, Chapter 245D; - Minnesota Data Practices Act (Minn. Stat. §13); - HIPAA Privacy & Security Rules; - DHS HCBS and 245D licensing requirements; - Premier Service internal privacy policies.

3. DATA COLLECTED Through RingCentral, the Agency may collect and store: - Phone call logs (incoming, outgoing, missed) - Voicemails, call recordings (if enabled) - SMS/MMS messages - Video meetings and remote support sessions - Staff and client contact information - Metadata such as timestamps and call duration

No data unrelated to service delivery or operational needs may be collected.

4. USE OF DATA Data is used only for: - Documenting service-related communication; - Verifying service delivery for 245D compliance; - Emergency assistance or crisis response; - Quality assurance, audits, or supervision; - DHS-required documentation and incident reporting; - Billing verification when applicable.

5. DATA STORAGE & SECURITY RingCentral data is stored in encrypted cloud servers. Premier Service enforces: - multi-factor authentication for all staff; - Role-based access control; - Password and device security requirements; - Encrypted communication channels for all RingCentral activity.

No client information may be downloaded, exported, or stored on personal devices unless explicitly approved and secured.

6. ACCESS TO DATA Access is limited to: - Authorized Premier Service staff; - Licensing bodies (DHS, county, state auditors) when legally required; - The client or their legal representative upon written request.

Unauthorized access or sharing of RingCentral data is strictly prohibited.

7. DATA RETENTION Data will be retained according to: - 245D documentation requirements (minimum 3 years); - DHS audit and record-keeping standards; - HIPAA retention guidelines.

Recordings or communication data not required for compliance will be deleted on a routine schedule.

8. CLIENT PRIVACY & CONSENT Clients are informed that: - Communication may occur via phone, text, or video through RingCentral; - Remote support sessions may be recorded only with consent; Emergency use of communication systems may occur without prior notice when safety is at risk.

9. STAFF RESPONSIBILITIES All staff must: - Use only agency-issued RingCentral accounts; - Avoid texting or calling clients on personal numbers; - Document all service-related communication per 245D rules; - Report any privacy breaches immediately.

10. BREACH OF PRIVACY A privacy breach includes unauthorized access, disclosure, loss, or misuse-of data. Premier Service will: - Notify affected individuals; - Follow DHS 245D incident-reporting rules; Correct vulnerabilities and implement safeguards.

11. THIRD-PARTY DISCLOSURES RingCentral may act as a Business Associate under HIPAA. No third-party vendor or subcontractor may access client data without a valid agreement consistent with DHS and HIPAA requirements.

12. MODIFICATIONS Premier Service may update these Terms and Conditions to remain compliant with DHS and federal law. Updated versions will be posted on the website.

13. CONTACT INFORMATION Premier Service Data Privacy & Compliance Department [www.premierservicellc.com] [Info@premierservicellc.com] [612-843-4747]

These Terms and Conditions meet 245D and HIPAA privacy requirements as applicable to communication technology systems.