Client Data Privacy & Secure Access Protocol

Client Name: __ *Date:* _____

Section 1: Establishing Your Secure Health Fortress

Functional medicine involves highly sensitive data, including **genomic markers, microbiome signatures, and deep lifestyle insights**. To protect your privacy and ensure compliance with HIPAA and GDPR standards, we use a closed, encrypted ecosystem.

Our Security Standards: * **AES-256 Bit Encryption:** The same level of security used by the US government. * **Business Associate Agreements (BAA):** All our software partners are legally bound to protect your data. * **End-to-End Encryption (E2EE):** Ensuring our video consultations remain private.

Section 2: Your Secure Access Points

Please complete this checklist during our onboarding session to ensure you have access to your protected health information (PHI).

Platform Type	Name of Service	Action Required	Status
Secure Client Portal (EHR)	_____	Create password & enable 2-Factor Auth (2FA)	☐
Encrypted Messaging	_____	Download app for all clinical questions	☐
Functional Lab Portal	_____	Register to view genomic/biometric trends	☐
Telehealth Room	_____	Test link (Ensure HIPAA-compliant version)	☐

Section 3: Data Privacy Preferences & Rights

Functional health data is uniquely identifiable. Please initial your preferences below:

1. **Explicit Consent:** I consent to the collection of genomic and biometric data for the purpose of health coaching. ____ (Initial)

2. **Right to Portability:** I understand I may request a digital export of my records at any time. ____ (Initial)
3. **Right to Erasure (GDPR):** I understand that upon termination of care, I may request the deletion of my data (subject to legal record retention requirements). ____ (Initial)
4. **Communication Boundary:** I agree NOT to send lab results or sensitive health data via standard email or SMS. ____ (Initial)

Section 4: Security Readiness Reflection

Security Score: (Count the "Yes" answers) _ / 5

1. Do you have a unique, strong password for the health portal? (Yes/No)
2. Is 2-Factor Authentication (2FA) enabled on your primary email? (Yes/No)
3. Do you promise to avoid accessing your health portal on public Wi-Fi? (Yes/No)
4. Do you have a private space for our telehealth consultations? (Yes/No)
5. Are you aware that genomic data is 95% identifiable even without your name? (Yes/No)

Practitioner Observations:

Next Steps:

1. Complete the secure portal registration sent to your email.
2. Upload any past lab results **only** through the encrypted "Documents" tab.
3. Our next session is scheduled via the secure telehealth link: _____

AccrediPro Standards Institute Certified Tool Compliant with HIPAA 45 CFR § 164.514 & GDPR Article 17
