CAHMI's Cycle of Engagement
Child & Adolescent Health Measurement Initiative
Real engagement, *for real health*

Summary of Data Collection and Storage Procedures and Policies for the CAHMI's Cycle of Engagement Well Visit Planner Approach

I. Introduction: The Child and Adolescent Health Measurement Initiative (CAHMI) takes the responsibility of ethical data stewardship seriously and invests considerable time and resources to assure that all the data we collect is protected and secured. As a "Business Associate"—as defined under the Health Information Portability and Accountability Act of 1996 (HIPAA)—CAHMI is required to comply with the HIPAA Security Rule, Breach Notification Rule, the use and disclosure provisions of the Privacy Rule, and be prepared to honor a covered entity's request concerning patient rights. Since 2020, CAHMI has partnered with a third-party consultant (Gazelle Consulting, LLC) to make certain that CAHMI's data is protected according to HIPAA compliance standards and to elevate CAHMI's security in the domains of people, processes, data, technology, and documentation to ensure that CAHMI remains a leader in safeguarding patient privacy.

II. Data Collection & Storage: CAHMI's Cycle of Engagement Well Visit Planner (COE/WVP) model and digital tools were created for use by clinicians, providers, practices, organizations, and families to promote high quality well child care services and promote child and family health. Designed with data security and user privacy in mind, the COE/WVP tools collect the minimum data necessary to advance these goals. Certain identifiable information is collected with consent from families (e.g., child's first and last name or child's initials, birth month and year). These data are encrypted, isolated, and stored on dedicated hardware-encrypted drives housed in a physically secure data center with continuous monitoring, badge and biometric access controls, redundant power/communication/environmental controls, and fire and flood prevention. Access control for CAHMI staff and contracted developers is governed by standardized procedures, which are regularly reviewed to ensure the correct level of information access is being granted, especially as it pertains to PII and system administrator-level access.

III. Data Transport Security: All CAHMI web traffic passes through a corporate firewall equipped with intrusion protection, application control, gateway anti-malware, SSL/TLS v3, inspection, and URL filtering. Servers run a built-in firewall included with the operating system. Antivirus scanning software is configured for real-time scanning on all devices; library definitions are updated daily; full system scans are performed weekly with results recorded in system logs reviewed weekly by IT personnel.

IV. Data Backup: CAHMI's operating systems, its file systems, and its databases are protected by an automated backup server with encrypted local and cloud-based replication. CAHMI maintains an Incident Response and Business Continuity Plan with procedures to ensure a consistent and effective approach to security events including but not limited to a data breach.

V. Conclusion: It is CAHMI's mission to maximize the security and integrity of the data entrusted to us while protecting user confidentiality in the event of a data breach. However, no policy or procedure is capable of eliminating every potential data security incident or attempt at malicious data theft. Users should exercise standard data security precautions and review CAHMI's Use Agreement and Privacy Notice. To this end, we make every reasonable effort to protect and secure your data and mindfully develop our business models and strategy in a manner consistent with the belief that everyone has a right to privacy-protection and confidentiality.

If you have questions about CAHMI's compliance, privacy, or security, please contact the Security Team at data_security@cahmi.org.