TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF CUIMC DATA

Columbia University Irving Medical Center (CUIMC) implements robust organizational measures to ensure the security, confidentiality, and integrity of managed data. These measures are designed to align with legal and regulatory requirements, including HIPAA, GDPR, and other applicable standards. Columbia University Medical Center's IT Security Risk and Privacy programs provide a framework that guides the organization in protecting institutional data and establishes clear responsibilities on required best practices ensuring compliance with regulatory requirements.

To protect sensitive and personal data, Columbia University employs advanced encryption and pseudonymization techniques. A minimum protocol of TLS 1.3 for data in transit and AES-256 encryption for data at rest is required to protect sensitive information, ensuring strong defenses against unauthorized access. Sensitive data at the institution is pseudonymized where required to minimize the risk of identification while preserving its usability. The de-identification of health information is guided by the standards outlined in the HIPAA Privacy Rule, ensuring compliance with federal regulations for safeguarding patient privacy. CUIMC employs both the Safe Harbor Method, which involves the removal of 18 specific identifiers, and the Expert Determination Method, leveraging statistical and scientific expertise to minimize re-identification risks. These policies enable the secure use of health data for research, public health initiatives, and operational purposes, ensuring that patient confidentiality is maintained.

CUIMC has in place strong access control measures to protect data from unauthorized access. Role-Based Access Controls (RBAC) requirements at CUIMC and Multi-factor authentication (MFA) apply authentication and authorization restriction ensuring that only approved personnel access data. Access permissions at CUIMC are granted based on a least privilege basis and are centrally managed through an Enterprise identity and access management system. CUIMC utilizes comprehensive logging mechanisms to capture infrastructure activities, including data access, modifications, and transfers. Additionally, these logs are routinely reviewed to detect anomalies and ensure compliance.

The University's IT infrastructure is fortified through a layered security approach that includes both system and network protections Firewalls and intrusion detection/prevention systems (IDS/IPS) monitor network traffic, while Next

Generation Layer 7 application inspections provide additional security against common web-based threats

Endpoint security is strengthened through comprehensive baseline hardening and advanced Endpoint Detection and Response (EDR) capabilities. Hardening involves configuring endpoints with industry-standard security measures, including disabling unnecessary services, enforcing strong authentication protocols, applying broad access controls, and ensuring all software and operating systems are up-to-date with the latest security patches. Endpoint devices are further strengthened with encryption and secure boot configurations. Information tagging and Data Loss Prevention measures are implemented to support controls for data transfers and to prevent unintentional or unauthorized data access.

CUIMC's Enterprise Systems are designed for resilience. Our environment incorporates processes for backups and disaster recovery to maintain continuity of operations. A technical vulnerability management program backed with an administrative sanction policy ensures that all systems and applications remain updated with the latest security patches to address potential exploitation proactively.

Strong retention policies are defined at the institution, ensuring that data is only kept as necessary to meet regulatory and operational requirements. Data destruction guidelines and institutional policies, require the secure wiping or physical destruction of storage devices before disposal or reuse. The destruction aligns with industry standards and maintain the confidentiality of sensitive information. 3-Pass Wipe procedures are recommended where (DoD) 5220.22 requirements are necessary.

Columbia University maintains a comprehensive incident response framework to address potential security breaches. A dedicated incident response team monitors systems in real-time and promptly addresses any suspected breaches. In the event of a breach, affected parties and regulatory authorities are notified in accordance with HIPAA and other regulatory requirements.

Physical security measures further protect data stored on-site. Physical access to data centers and storage facilities is restricted using card readers ensuring only authorized personnel can enter. These facilities are equipped with fire suppression systems, climate controls, and uninterruptible power supplies to protect against environmental disruptions and ensure the safe operation of data storage systems.

CUIMC's Organizational and governance measures ensure continuous program oversight and accountability in data security and privacy practices. It's Security Program is governed by a formalized charter with clear institutional roles for Security and Privacy established. Workforce member IT responsibilities are set through policy and reinforced in regular training sessions to educate on best practices for safeguarding data and maintaining compliance.

Cyber Security frameworks to include HiTrust, NIST 800-53. ISO 27001 are used as the foundation of Columbia University Medical Center's IT Risk Assessment Program which evaluates the institution's IT practices for regulatory compliance and supports the effective management of cybersecurity risks. The institution leverages a centralized platform for identifying, assessing, and mitigating risks to demonstrate Columbia University's commitment to maintaining high standards of information security. With evolving regulatory requirements, periodic internal and external audits assess the effectiveness of implemented measures and identify areas for improvement.

The university recognizes the importance of data portability and secure deletion for the purposes of this Data Use Agreement (DUA). Secure methods for transferring data will be implemented to comply with portability requests while maintaining its integrity. At the end of the retention period or upon request, data will be securely erased using industry-standard methods, certifying it cannot be recovered.

For specific **controller-to-controller transfers**, data exchanged between parties will be encrypted and logged, with access restricted to authorized personnel. For **controller-to-processor transfers**, CUIMC data requester will adhere to security requirements, and activities will be monitored by the Principal Investigator. For **processor-to-processor transfers**, sub-processors are contractually obligated to implement equivalent security measures, and regular audits ensure compliance with these requirements.