Privacy and Security Oversight Plan

PURPOSE:

To establish a plan for oversight of the privacy and security of protected health information in compliance with federal and state regulations.

POLICY:

The access, use or disclosure of GRH PHI/e-PHI that is created, received, maintained or transmitted is secured for privacy and confidentiality to meet legal and regulatory compliance. Great River Health (GRH) Privacy and Security (P&S) Plan provides the foundation for the privacy and security of protected health information according to HIPAA Privacy and Security Rules, HITECH federal regulations and any additional state or local regulatory requirements.

OPERATIONAL DEFINITIONS:

HIPAA: Health Insurance Portability and Accountability Act of 1996.

HITECH: Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009.

Protected Health Information [PHI, electronic/e-PHI]: Any individually identifiable health information created, received, maintained, or transmitted by GRH, or its business associate(s), in any form or media, whether verbal, paper, or electronic, in accordance to 45 CFR Part 160 Subpart A, Section 160.103.

PROCEDURE:

Privacy & Security Team

A. GRH has established a Privacy and Security (P&S) Team, under the oversight of the Ethics and Compliance Program and the Data Governance Committee that is responsible for:

1. Incident response;
2. Risk assessment/management/oversight;
3. Annual review of this plan and risks;
4. Review, development, and revision of related policies/procedures; and
5. Providing recommendations for compliance, education, and/or action plans.

B. The P&S Team is composed of:

1. Privacy Officer
    a. The Privacy Officer, who will establish and maintain a privacy management program that includes:
        i. Written policies and procedures that place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI;
        ii. Training for workforce members of privacy policies and procedures as necessary and appropriate to carry out their job functions;
        iii. Reasonable safeguards to protect PHI from any intentional or unintentional use or disclosure that is in violation of law, and limit incidental uses or disclosures;
        iv. Processes to report complaints or concerns about privacy, and steps to investigate, mitigate, and document all complaints or concerns;
        v. Enforcement of the program and sanctions against workforce members who fail to comply with privacy policies and procedures;
        vi. Mitigation, to the extent practicable, of any harmful effect of a use or disclosure of PHI in violation of GRH policies and procedures, or in violation of law by GRH or its business associates;
        vii. Protection for personnel who make reports or participate in an investigation in good faith against intimidation, threats, coercion, discrimination against, or any other retaliatory action as consequence;
        viii. Protection of patient rights to file a complaint with the Secretary of Health and Human Services without affecting the provision of treatment or payment;
        ix. Maintenance of all documentation in written or electronic format related to and/or required by HIPAA for six (6) years from the date of creation, or the date it was last in effect, whichever is later.

b. The Manager-Compliance, or other designees as determined by the Privacy Officer, will be authorized to execute responsibilities designated to the Privacy Officer.

2. Information Security Officer
    a. The Information Security Officer, who acts as the designated point of contact for HIPAA Security Rule, Payment Card Industry Data Security Standards (PCI DSS), and other state and federal regulations, and is responsible for the development and implementation of security policies and procedures, will establish and maintain a security management program that includes:
        i. Security awareness and training for all workforce members;
        ii. An inventory of all information systems, assets, and components;
        iii. Confidentiality, integrity, and availability classifications for all information systems;
        iv. Identification, monitoring, and mitigation of threats and vulnerabilities to all information systems;
        v. Periodic risk analysis of information systems and security controls;
        vi. Establishment, documentation, and distribution of security incident response and escalation procedures;
        vii. Development and management of emergency and disaster recovery plans and procedures, and ensuring backup, recovery, and retention capabilities meet business requirements;
        viii. Evaluation of information system products and services acquisitions, and review of business associates and service providers that may interact with ePHI or the cardholder data environment (CDE) prior to the granting of access;
        ix. Coordination and documentation of security processes into human resources functions;
        x. Administration of user accounts, including additions, deletions, and modifications;
        xi. Monitoring and control of all access to sensitive data;
        xii. Establishment of secure communication methods to protect ePHI, or other sensitive information, and maintaining integrity with its source;
        xiii. Definition of the physical and logical security controls and the proper use of workstations;
        xiv. Protection of media through safe handling and usage controls;
        xv. Restriction of physical access to secure facilities and protecting critical hardware;
        xvi. Monitoring and analysis of security alerts and events and distribution to appropriate personnel.

b. The Information Security Officer will provide regular updates on the status of the program to the Chief Compliance Officer.

3. Additional team members include but are not limited to Manager-Compliance; Manager-Health Information Management; Vice President-Information Services; Director-Clinical Informatics, Chief Compliance Officer, and other administrative/management members as needed.

C. P&S Team members maintain knowledge base of professional association information, regulatory requirements, and local/state/national guidance and provide appropriate recommendations for GRH compliance.

Monitoring and Auditing

A. Walk-through audits are conducted periodically for ongoing monitoring in all areas with patients and PHI/ePHI accessible. Results are documented and reported to the Compliance Oversight Committee.

B. Equipment that creates, receives, maintains, or transmits PHI/ePHI has security assessments/tracers periodically conducted.

C. Routine, random, and specific assessments are conducted based on access audit trail reports from the electronic health record for proactive, concurrent, or ad hoc monitoring.

D. P&S Team supports review of HIPAA Business Associate Agreement compliance.

Incident Management

A. All reports of HIPAA privacy and/or security concerns are promptly investigated and managed per established HIPAA privacy and security policies and procedures.

B. Data collection and analysis of data is completed by the Chief Compliance Officer and/or other members of the P&S Team.

C. Action plans, education, or process improvement determinations are made based on regulatory guidance, high risk areas or outcomes, and data analysis.

D. All reported concerns are documented in the electronic reporting system. Documentation will include investigative activity, findings, and resulting action plans.

Reporting

A. The Chief Compliance Officer is responsible for reporting the activity of the P&S Team to the Compliance Oversight Committee and to the Board of Directors on a quarterly basis.

B. Reports regarding P&S Team activity related to data protection and other relevant initiatives will be provided to the Data Governance Committee periodically.