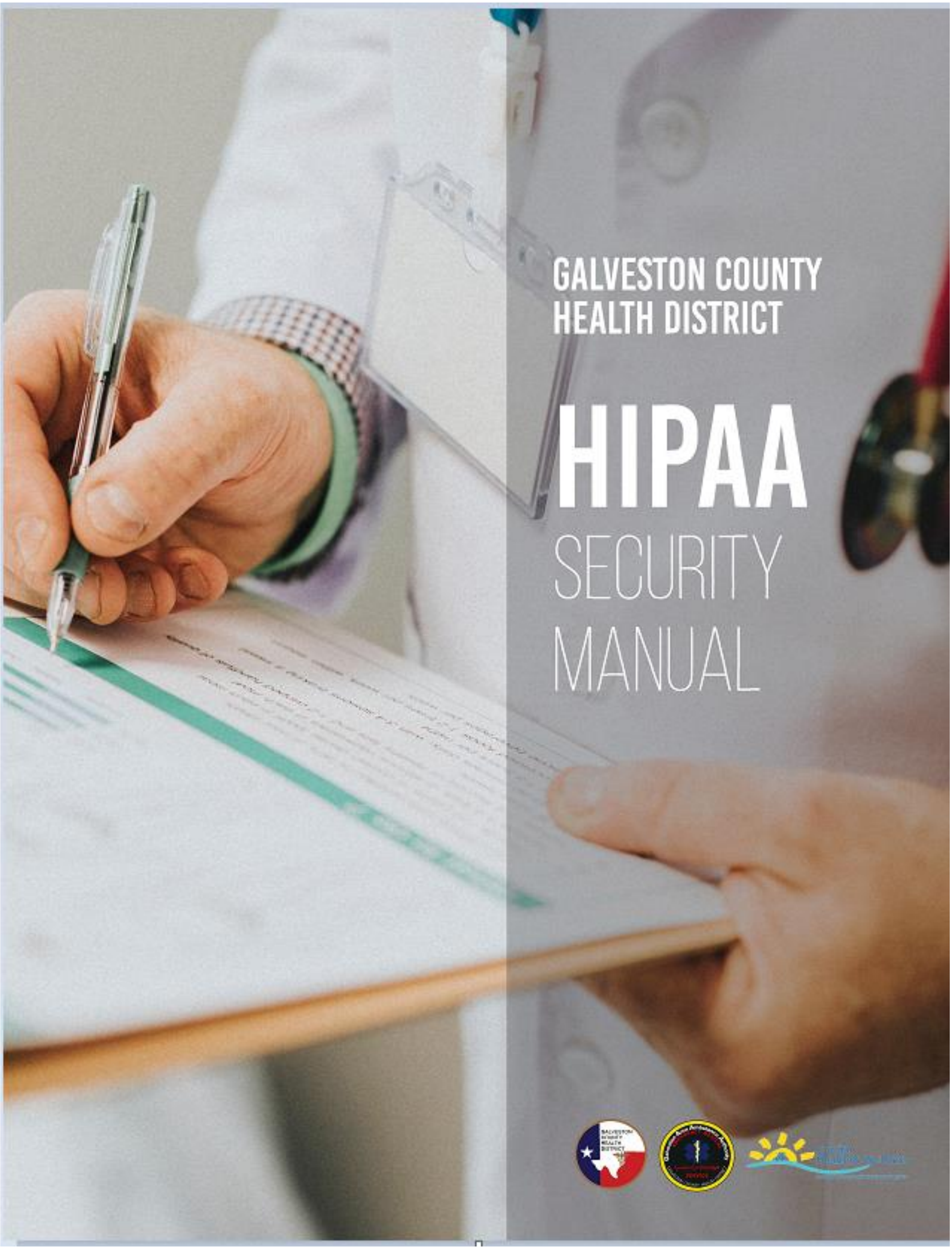

GALVESTON COUNTY HEALTH DISTRICT

HIPAA SECURITY MANUAL

TABLE OF CONTENTS

Galveston County Health District

HIPAA Security Manual

OVERVIEW

The purpose of this manual is to provide a framework for Galveston County Health District's (including Coastal Health & Wellness and Galveston Area Ambulance Authority) compliance with the Security Standards required under the Health Insurance Portability and Accountability Act (HIPAA) and state laws and regulations.

This manual is organized according to three safeguards: Administrative, Physical and Technical. Each safeguard consists of standards and implementation specifications. The specifications are divided into those that are required and those that are addressable.

GCHD will decide whether an addressable implementation specification is a reasonable and proper security measure to apply within the security framework. The decision will depend on several factors, such as, among others, GCHD's risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation.

The policies and procedures that make up this manual apply to all employees, volunteers, students, contractors and others who perform a service at GCHD. The policies and procedures are to ensure the confidentiality, integrity, and availability of electronic protected health information GCHD creates, receives, maintains, and transmit. GCHD will protect against reasonably anticipated threats or hazards to the security or integrity of our information systems and uses or disclosures to of such information that is not permitted.

Section 2.1	**Definitions**	**Effective Date:** 9/26/2013
		Revised: 06/14/2019

DEFINITIONS

1. *Access* means the ability or the means necessary to read, write, modify, or communicate data or information, or otherwise use any system resource.

2. *Administrative safeguards* are administrative action, and policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the Covered Entity's workforce in relation to the protection of that information.

3. *Authentication* means the corroboration that a person is the one claimed.

4. *Availability* means the property that data or information is accessible and useable upon demand by an authorized person.

5. *Business associate* means a person or organization who performs a function or activity on behalf of a Covered Entity or who performs a specified service regardless of whether it involves performing a service on behalf of a Covered Entity. The specified services where disclosure personally identifiable health information is considered routine include legal, actuarial, accounting, consulting, management, administrative accreditation, data aggregation, and financial services. When a Covered Entity discloses protected health information to a business associate, a business associate agreement between the Covered Entity and the person or organization performing functions on behalf of the Covered Entity or specified services is required to protect the use and disclosure of protected health information.

6. *Confidentiality* means the property that data or information is not made available or disclosed to unauthorized persons or processes.

7. *Covered entities* are those entities covered by the HIPAA Privacy and Security Standards.

8. *Disclosure* means the release, transfer, provision of, access to, or divulging in any other manner of protected health information outside the entity holding the information.

9. *Electronic protected health information* means protected health information (see definition below) which is maintained in or transmitted by electronic media.

10. *Encryption* means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

11. *Facility* means the physical premises and the interior and exterior of a building(s).

12. *Information system* means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

13. *Integrity* means the property that data or information has not been altered or destroyed in an unauthorized manner.

14. *Malicious software* means software, for example, a virus, designed to damage or disrupt a system.

15. *Minimum necessary* means a Covered Entity must make reasonable efforts to limit use and disclosure of protected health information to the minimum necessary to accomplish the intended purpose of the use or disclosure.

16. *Password* means confidential authentication information composed of a string of characters.

17. *Physical safeguards* mean physical measures, policies, and procedures to protect a Covered Entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

18. *Protected health information* means individually identifying health information that is transmitted by or maintained in any form or medium.

19. *Security or Security measures* encompass all the administrative, physical, and technical safeguards in an information system.

20. *Security incident* means any attempted or successful unauthorized access, use, disclosure, modification, or destruction of information, or interference with system operations in the information system.

21. *Technical safeguards* are the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

22. *User* means a person or entity with authorized access.

23. *User ID* means a unique identifier given to an individual allowing the individual access to a computer system. A user ID is usually accompanied by a password.

24. *Employee* means employees, volunteers, interns, and other persons whose conduct, in the performance of work for a Covered Entity, is under the direct control of such entity, whether they are paid by the Covered Entity.

25. *Workstation* means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

Section 2.2	**Hybrid Entity**	**Effective Date:** 9/26/2013
		Revised: 06/14/2019

POLICY

GCHD is recognized to be a hybrid entity. GCHD will develop policies and procedures to ensure compliance with the requirements for hybrid entities. The health care components of GCHD must comply with the Security Standards and safeguarding electronic protected health information and non-covered components will be treated as is they were separate and distinct legal entities.

PROCEDURE

1. With rare exceptions, the following GCHD departments are not regulated under the Health Insurance Portability and Accountability Act (HIPAA): Environmental Health Programs, Vital Statistics, and Animal Services. The remaining services of GCHD are health care components, including Coastal Health & Wellness and the Galveston Area Ambulance Authority.

2. If one of the aforementioned departments creates, receives, maintains or transmits electronic protected health information on behalf of a health care component, the department must comply with the HIPAA Security Standards as set forth under this manual.

REFERENCE

45 C.F.R. § 164.105(a)

Section 2.3	Affiliated Covered Entity	Effective Date: 9/26/2013
		Revised: 06/14/2019

POLICY

GCHD is a covered entity comprised of affiliated groups that utilize a shared staff system. GCHD will develop policies and procedures to ensure compliance with the requirements HIPAA Security Standards.

PROCEDURE

1. The following entities are legally separate entities which employ shared staff: Galveston County Health District, Galveston Area Ambulance Authority, and Coastal Health & Wellness. These entities have been designated as a single affiliated covered entity for purposes of the Health Insurance Portability and Accountability Act (HIPAA) and will be identified as "Galveston County Health District (GCHD)."

2. GCHD's creation, receipt, maintenance, transmission, use and disclosure of electronic protected health information will comply with the HIPAA Security Standards.

REFERENCE

45 C.F.R. § 164.105(b)

Section 2.4	**Business Associate Agreement**	**Effective Date:** 9/26/2013
		Revised: 06/14/2019

POLICY

GCHD follow appropriate procedures when sharing protected health information ("PHI") with business associates who create, receive, maintain or transmit electronic protected health information on GCHD's behalf to safeguard such information.

PROCEDURE

1. *Agreement*. Business associates must sign a Business Associates Agreement to safeguard protected health information. The agreement will meet the requirements of the HIPAA Security Standards and requires the business associate to:

    a. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic protected health information that it creates, receives, maintains, or transmits on behalf of GCHD.

    b. Ensure that any agent, including a subcontractor, to whom GCHD provides such information contractually agrees to implement reasonable and appropriate safeguards to protect it.

    c. Report to GCHD any security incident of which it becomes aware of.

    d. Terminate the contract and mandate that all shared PHI be returned or permanently discarded if GCHD discovers that the business associate has violated a material term of the contract.

2. *Material Breach*. If GCHD knows of a pattern of activity or practice of the business associate that constitutes a material breach or violation of the business associate's obligation under the agreement, GCHD must take reasonable steps to cure the breach or end the violation. If these steps are unsuccessful, GCHD must terminate the agreement if feasible, or, if termination is not feasible, report the problem to the Office of the Inspector General.

REFERENCE

45 C.F.R. §164.314(a)

Section 2.5	Maintenance of Policies and Procedures	Effective Date: 9/26/2013 Revised: 06/14/2019

POLICY

GCHD will implement reasonable and appropriate policies and procedures to comply with standards, implementation specifications, or other requirements of the HIPAA Security Standards.

PROCEDURE

1. Documentation. GCHD will document all policies and procedures. A written record will be maintained by the Security Officer if an action, activity or assessment that is required by this Security Manual or the HIPAA Security Standards.

2. Retention. GCHD will retain the documentation of the policies and procedures set forth in this Security Manual and any action, activity or assessments required by the HIPAA Security Standards for six (6) years from the date of its creation or the date when it last was in effect, whichever is later. This retention schedule will be a part of the GCHD retention guidelines.

3. Availability. GCHD will make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

4. Updates. Manager of Information Technology or Security Officer or their respective designees will review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

REFERENCE

45 C.F.R. §164.316(a) and (b)

Section 3.1	**Security Management Process**	**Effective Date:** 9/26/2013
		Revised: 06/14/2019

POLICY

GCHD will protect the confidentiality, integrity, and availability of its information systems containing electronic protected health information. GCHD will implement reasonable and appropriate procedures and controls to prevent, detect, contain, and correct security violations.

PROCEDURE

1. Risk Analysis. Routinely, GCHD will conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by GCHD. The results of the risk assessment will be used to implement security measures sufficient to such to mitigate or eliminate unacceptable risks and vulnerabilities to a reasonable and appropriate level. A Risk Mitigation Proposal will document recommendations to management.

2. Risk Management. GCHD will monitor and manage the risks identified in the risk analysis process to ensure security measures are sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

   a. *Controls*. GCHD will select appropriate controls that were identified in the risk analysis process to minimize risks to electronic protected health information. These controls will be based upon the feasibility and effectiveness after taking into consideration GCHD's structure and resources, and the results of a cost-benefit analysis. Technical, management, and operational security controls may be considered.

   b. *Control examples include, but are not limited to, the following*:

      i. Supportive controls: unique user IDs; system security; and system protections.
      ii. Preventive controls: authentication controls (such as passwords, personal identification numbers); access control enforcement (such as data encryption methods, virtual private network).
      iii. Detection controls: periodic system audits and ongoing risk management.
      iv. Operational controls: physical access control; facility security; regular data and system backups; off-site storage; and environmental security.

3. Sanctions. Workforce personnel who violate GCHD's security policies and procedures or violate the HIPAA Security Rule will be disciplined in accordance GCHD personnel policies.

   a. *Employees*. GCHD employees who either intentionally or unintentionally violate the security policies and procedures are subject to appropriate corrective disciplinary action, up to and including suspension, probation, or dismissal. Managers or supervisors may also be disciplined if their lack of diligence or supervision contributed to the violation.

   b. *Non-Employees*. Independent contractors and volunteers who are not who either intentionally or unintentionally violate the security policies and procedures are subject to appropriate corrective disciplinary action, up to and including suspension, probation, or dismissal. Similarly, GCHD's business associates will be contractually informed that they may lose any privileges or contractual rights if they violate security policies or the terms of the business associate agreement.

4. Information System Activity Review. GCHD will implement procedures to regularly review records of information system activity.

   a. *Audit Logs*. GCHD will create audit logs which will record activities related to access of the GCHD system by its users. Audit logs will be reviewed on an on-going basis by the Security Officer or designee.

   b. *Access Reports*. GCHD will create access reports listing each actual or attempted access of the system by its users. Access reports will be reviewed on an on-going basis to identify any actual or attempted unauthorized access or security incidents.

   c. *Tracking Reports*. Any actual or attempted unauthorized access or security incident event will be tracked and reported. GCHD will review on a routine basis unauthorized access and security incident tracking reports. Executive staff or assigned designee(s) will determine the mitigation, response and/or sanction, if any, required to respond to the events noted in the tracking report.

   d. *Controls Audit*. GCHD will perform internal audits of operational and technical controls/procedures to prevent a HIPAA security breach.

REFERENCES

AS 3.4.1, Access Authorization
AS 3.5.1, Workforce Training
AS 3.5.4, Log-in Monitoring
AS 3.7.1, Data Backup
AS 3.7.5, Applications and Data Criticality Analysis
TS 5.2, Audit Controls
OR 2.4, Business Associate Agreement
45 C.F.R. §164.308 (a)(1)

Section 3.2	**Assigned Security Responsibility**	**Effective Date:** 9/26/2013
		Revised: 06/14/2019

POLICY

GCHD will perform the duties set forth in this policy. GCHD will designate an individual as the Security Officer who will be responsible for ensuring that GCHD complies with the security policies and procedures. The Security Officer shall report to the Manager of Information Technology and, in certain cases, the Chief Compliance Officer.

PROCEDURE

1. Security Officer. GCHD's Security Officer is responsible for protecting the confidentiality, integrity, and availability of GCHD's information systems containing electronic protected health information ("ePHI"), as well as to ensure compliance with applicable state and federal laws and regulations.

    a. *Designation*: GCHD's Security Officer is the IT Network Security Engineer.

    b. *Responsibilities*. The Security Officer's responsibilities include, but are not limited to, the following:

        i. Consult with and advise the Manager of Information Technology, Chief Compliance Officer and Chief Executive Officer concerning security-related administrative decisions and the implementation of security-related policies and procedures.

        ii. Develop, regularly update, and disseminate policies and procedures to assure compliance with the Security Standards.

        iii. Initiate and conduct internal reviews of GCHD's internal security controls, prepare reports regarding GCHD's security program, and track security incidents and violations.

        iv. Report to the Manager of Information Technology, Chief Compliance Officer and Chief Executive Officer concerning any issues regarding GCHD's compliance with the Security Standards.

        v. Consult with and advise the Manager of Information Technology, Chief Compliance Officer and Chief Executive Officer concerning the occurrence of security incidents as appropriate and provide recommendations concerning potential or recommended corrective or remedial actions.

vi. Serve as a resource for employees concerning security issues and GCHD's obligations under the Security Standards, this includes informing the workforce of threat and conducting needed trainings.

vii. The Security Officer shall coordinate with other GCHD directors and managers responsible for the protection of information systems to ensure that all aspects of information security are adequately addressed.

2. Covered Entity. GCHD will protect the confidentiality, integrity, and availability of GCHD's information systems containing electronic protected health information.

   a. *Responsibilities*. GCHD responsibilities include, but are not limited to, the following:

      i. Designating a Security Officer.

      ii. Implementing security policies and procedures overseen by the Security Officer and other management as deemed necessary.

      iii. Designate additional executive staff members to oversee aspects of information management security outside of the Security Officer's responsibilities.

      iv. Train all employees on the security policies and procedures.

      v. Take appropriate sanctions against an employee who violates a security policy or procedures.

      vi. If a security incident occurs, take any necessary corrective or remedial action.

      vii. Refrain from harassing or subjecting to adverse employment action any employee who reports a security incident or violation of a security policy that he or she, in good faith, believes has occurred.

      viii. Through the Contracts Analyst, maintain agreements with business associates that comply with the Security Standards.

REFERENCES

OR 2.4. Business Associate Agreement
AS 3.1.3, Sanctions
AS 3.5, Awareness and Training
As 3.6, Security Incident Procedures

45 C.F.R. § 164.308(a)(2)

Section 3.3	Workforce Security	Effective Date: 9/26/2013
		Revised: 06/14/2019

POLICY

GCHD will take reasonable and appropriate steps to ensure that employees who are allowed access to ePHI may be safely trusted with such access. GCHD will take the necessary steps to terminate physical or remote access to ePHI if an employee is no longer authorized to have access to such information.

PROCEDURE

1. Authorization and/or Supervision of Employees. No employee will be permitted access to ePHI unless access is determined to be necessary to perform the employee's job function, and the employee has followed GCHD's procedures for obtaining authorization for such access.

   a. The Security Officer and GCHD management will ensure that each employee's access to ePHI is appropriate and consistent according to HIPAA privacy and security guidelines.

   b. A employee may receive a password to access ePHI only with the authorization of his/her supervisor, Human Resources Department, or the Executive Management, in accordance with GCHD's policy. It is the responsibility of the Security Officer or designee and Human Resources:

      i. To verify that access to ePHI is necessary to perform the job, and that the employee's access is limited to the minimum necessary ePHI;

      ii. To ensure that the employee receives GCHD's training concerning the security and confidentiality of electronic protected health information;

      iii. To ensure that the employee signs any confidentiality agreement to attest to the employee's commitment not to disclose his or her password and/or other sensitive information; and

      iv. To address any instances of security misconduct by the employee.

   c. GCHD will take steps to minimize the likelihood that employees who do not have authorized access to ePHI will gain access to such information because they perform their duties in areas in which such information is present. Steps may include, but are not necessarily limited to, the following:

i. Ensuring computer users log off the computer system when they are not using the computer system;

ii. Providing immediate supervision in work areas containing ePHI; and

iii. Using automatic screen savers or privacy screens.

2. Clearance Procedures. All employees at GCHD are required to have an employment background check as required for their job position. Human Resources and the hiring supervisor will identify the information security responsibilities of the employee and the type of supervision and access required for the position. Each GCHD employee will sign a confidentiality statement to protect the confidentiality, integrity and availability of GCHD information systems.

3. Termination of Access Procedures. The Security Officer or designee, Human Resources and other designated staff will perform the following procedures for terminating access to ePHI when an employee's authorization or employment ends, or the position does not require the same level of access:

i. Ensure that such person no longer has physical or remote access to sensitive areas containing electronic protected health information.

ii. Recover or reprogram all keys, identification badges/cards, and any other object that allows physical access to property, buildings, and equipment.

iii. Recover any other information or property of GCHD that may be in such person's possession, such as uniforms, cell phones, equipment, etc.

iv. Deactivate and disable such person's user identification numbers, passwords, electronic codes, etc., and access to VPN service, and any other remote access systems.

v. Change combination locks, safe combinations, keypad codes etc., such person had access to.

REFERENCES

AS 3.1.2, Risk Management
AS 3.4.1, Access Authorization

AS 3.5, Awareness and Training
PS 4.1.2, Facility Security Plan
PS 4.1.3, Access Control and Validation Procedures
PS 4.4.1, Disposal

45 C.F.R. § 164.308(a)(3)

Section 3.4	Information Access Management	Effective Date: 9/26/2013
		Revised: 06/14/2019

POLICY

GCHD will grant access to ePHI to employees whose job responsibilities require such access and will document, review, and modify an employee’s right of access to ePHI as provided in this policy.

PROCEDURE

1. Access Authorizations.

   a. GCHD will document the employees who have access to electronic protected health information based on job responsibilities. Employees will have access to only that information required to perform their job responsibilities. Employees’ access will be reviewed on a continual basis to ensure access continues to reflect the current need for electronic protected health information.

   b. Employees must sign a current confidentiality statement to be granted access to ePHI.

   c. All employees will attend trainings that will include security-related topics such as access control and documentation, maintenance of proper security measures, and the consequences of security incidents or deviations from GCHD policies and procedures.

   d. All employees will adhere to GCHD’s policies concerning remote access and workstation access and use.

   e. Access to PHI in any form by individuals or entities other than employees, such as patients, law enforcement personnel, or public health officials, will be granted in accordance with GCHD’s policies along with state and federal law, and, if applicable, stipulations set forth under business associate agreements entered into between GCHD and the third-party.

2. Access Establishment and Modification.

   a. Potential employees shall undergo employment background checks and other measures deemed necessary by GCHD’s management prior to hiring. Results of such measures shall be reviewed by GCHD’s management before the employee is granted access to electronic protected health information.

b. All employees who access ePHI will be given a user ID and be required to establish a password in accordance with GCHD’s guidelines in order to gain such access.

c. Physical access controls, such as keycards and combinations, will be used to restrict access to areas containing electronic protected health information to authorized users only, as appropriate.

d. GCHD will develop and document an emergency access procedure to allow access to electronic protected health information by certain specified employees under unanticipated or urgent circumstances.

e. GCHD will allow modification of an employee’s access to ePHI where appropriate, such as where the employee has changed job function or status.

f. GCHD will terminate an employee’s access to the system upon the dismissal or separation of an employee from his/her position, in the event of a security incident involving the employee, if the employee violates GCHD’s policies or procedures, or if access is no longer necessary to perform the employee’s job responsibilities.

REFERENCES

AS 3.5, Awareness and Training
PS 4.1.3, Access Control and Validation Procedures
TS 5.1.1, Unique User Identification
TS 5.1.2, Emergency Access Procedure
TS 5.4, Authentication of Entity or Person

45 C.F.R. § 164.308(a)(4)

Section 3.5	Awareness and Training	Effective Date: 9/26/2013
		Revised: 06/14/2019

POLICY

GCHD employees will receive security awareness and training with respect to safeguarding ePHI.

PROCEDURE

1. Workforce Training Program. GCHD will implement a security awareness and training program for all employees, including management.

   a. *General Orientation*. All employees will receive a general orientation covering the policies included in this manual and will be given the name of the Security Officer. For new employees, such information will be included in the orientation materials.

   b. *Basic Security Training*. All employees will receive basic security training. Training will be updated on continuing basis. Basic security training will include a review of the policies that apply to all employees using the information system, such as:

      i. Policies on proper password management and the necessity of maintaining the confidentiality of the employee's access code and password;
      ii. Proper use of the computer system including e-mail and the Internet
      iii. Procedures for saving data to network drives;
      iv. Prohibition on attempting access to electronic protected health information without authorization;
      v. Prohibition on improper copying of files and programs, or loading of unauthorized programs on the information system;
      vi. Precautions against malicious software, and procedures to follow if the employee suspects that malicious software has been introduced;
      vii. Reporting problems with access to the system; and
      viii. Reporting security incidents.

   c. *Additional Training*. Additional training will be provided periodically, but at a minimum annually, to employees in response to operational changes or security incidents. Training for these employees will include, but will not be limited to, the following:

   d. *Documentation*. GCHD will maintain documentation on security awareness and training of employees in the personnel files.

2. Security Reminders. GCHD will periodically provide security reminders to employees informing them of changes in policies and procedures, and to generally reinforce security awareness and training.

3. Protection from Malicious Software. GCHD will undertake strong measures to protect against the introduction of malicious software into its information system. Security training will educate employees on guarding against, protecting from and reporting of malicious software, which may include:

   a. The danger of malicious software or any other agent that can destroy or alter data;

   b. The use of ant-virus protection software;

   c. Not opening or downloading files from an unknown or suspicious source; and

   d. External files being loaded on to the computer through a USB drive or other source.

4. Log-In Monitoring. Security training will educate employees on monitoring log-in attempts and reporting discrepancies if the employee becomes aware of such discrepancies.

5. Password Management. Security training will educate employees on creating, changing and safeguarding passwords. GCHD will require any employee who has access to GCHD's information system(s) to use a unique password, keep the password confidential, change it according to GCHD's set timeframes, and utilize safeguards to prevent misappropriation of passwords.

REFERENCES

AS 3.1.1, Risk Analysis
AS 3.1.4, Information System Activity Review
AS 3.6, Response and Reporting of Security Incidents

45 C.F.R. § 164.308(a)(5)

Section 3.6	Security Incident Procedures	Effective Date: 9/26/2013
		Revised: 06/14/2019

POLICY

GCHD responds to suspected or known security incidents and violations of organizational security policies and procedures; mitigates harmful effects of security incidents that are known to GCHD, and documents security incidents and their outcomes.

PROCEDURE

1. All employees have a duty to promptly report any security incidents and violations of GCHD's security policies and procedures (including those involving business associates) to the Security Officer, Manager of Information Technology, Chief Compliance Officer, Executive Management or their respective designee.

2. Any employee who knowingly fails to report a security incident or violation of GCHD's security policies and procedures may be subject to discipline.

3. No retaliation shall be tolerated against an employee who has filed a report based on a good faith belief that another employee has committed an actual or suspected violation subject to the reporting requirements of this policy. Any employee who takes or attempts to take retaliatory action against an employee who reported an actual or suspected violation will be subject to discipline.

4. The Security Officer, Chief Compliance Officer, or their respective designee shall be responsible for investigating all security incidents and security policy violations to determine the potential causes, whether the security incident has resulted in any unauthorized disclosure of ePHI, corruption or unauthorized modification of data, or loss of data and, with Human Resources to recommend and implement appropriate measures, if any, to prevent further incidents.

5. Remedial measures will be taken to mitigate the effects of the security incident to the extent possible. If an unauthorized disclosure of protected health information has occurred, the Chief Compliance Officer and/or Human Resources Director shall be consulted, if appropriate, and GCHD's policies concerning mitigation of violations of privacy policies of shall be followed.

6. The Security Officer, Chief Compliance Officer, or their respective designee will document the investigation of the reported incident, whether the incident was determined to be a security incident, and any action taken in response to the incident.

REFERENCES

AS 3.1.3, Sanctions
AS 3.2.1, Security Officer

45 C.F.R. § 164.308(a)(6)

Section 3.7	**Contingency Plan**	**Effective Date:** 9/26/2013 **Revised: 06/14/2019**

POLICY

GCHD will establish procedures for responding to an emergency or other occurrence that damages GCHD's information systems that contain electronic protected health information.

PROCEDURE

1. Data Backup Plan. GCHD will maintain backup copies of ePHI information so data can be retrieved if lost or corrupted.

    a. *Data Backup*. The Security Officer and Manager of Information Technology will establish specific backup schedules and procedures for GCHD's networks and computer systems. All software, applications, files, data, and messages related to healthcare operations stored on GCHD's networks and other information systems will be backed up to appropriate storage area networks.

    b. *Backup Validation*. Backup and restoration procedures will be reviewed periodically to ensure that procedures are appropriate and efficient, and that GCHD's ability to restore data remains intact and relevant

    c. *Onsite Storage*. The storage media from the previous day or current week shall be stored onsite in a secured area.

    d. *Offsite Storage*. Certain data backups will be stored in a secure, off-site location. Data backups must be maintained for a minimum of one year. The Security Officer shall maintain documentation of the location of the off-site storage site(s).

    e. All data backups will be logged, and data backups will be disposed of in accordance with GCHD's record retention policies.

2. Disaster Recovery Plan. GCHD will follow written procedures to restore data lost through occurrence of a disaster.

    a. *Disaster Assessment*. Once a disaster has occurred, GCHD will assess the effect of the disaster on GCHD's information systems and determine if there is any lost functionality and loss of data. If data has been lost the Disaster Recovery Plan will be implemented.

    b. *Securing Facilities*. In the event of a catastrophic event, GCHD will immediately ensure that all facilities housing GCHD's information systems remain secure under the circumstances. Access to the facilities will be limited to personnel assisting in the disaster recovery.

c. *Restoring Backup Data*. GCHD will restore software, applications, information and data to appropriate information systems as soon as possible.

d. *Testing*. Backup systems are tested daily to ensure the network and computer systems are operating correctly.

3. Testing and Revision Procedure. GCHD will periodically test protocol and revise its information system contingency plan.

   a. The tests will be designed to simulate potential threats to the information system but will be conducted in a controlled environment.

   b. The tests will evaluate adequacy of back-up and recovery systems, and time required to return the system to a normal operating environment.

   c. If the tests reveal vulnerabilities or inadequacies of back-up and recovery systems, appropriate modifications will be made in the Data Backup Plan and the Disaster Recovery Plan.

   d. The Security Officer shall be responsible for the oversight of and documentation of back-up testing procedures, and will notify the Manager of Information Technology immediately should flaws be detected.

4. Applications and Data Criticality Analysis. GCHD will assess the relative criticality of specific applications and data in formulating its contingency plan.

   a. GCHD will determine which applications and data are essential to maintain patient care, life safety, and other essential functions.

   b. In evaluating the criticality of information, GCHD will consider, among other things, the difficulty of replicating the data if lost, sensitivity of the data, and consequences to patients if data is unavailable or corrupted.

   c. Those applications and databases identified as critical to GCHD's patient care mission will be given priority in the contingency plan.

   d. GCHD will devote appropriate resources to recovering critical functions in the event of a disaster.

REFERENCES

AS 3.1.1, Risk Analysis
AS 3.1.2, Risk Management
PS 4.1.1, Contingency Operations
PS 4.4.4, Data Back-up and Storage
TS 5.1.2, Emergency Access Procedure

45 C.F.R. § 164.308(a)(7)

Section 3.8	**Evaluation**	**Effective Date:** 9/26/2013
		Revised: 06/14/2019

POLICY

GCHD will perform periodic technical and non-technical evaluations to establish the extent that GCHD's security policies and procedures meet the requirements of the Security Rule (*45 CFR Part 160 and Subparts A and C of Part 164*) based upon the standards implemented under the Security Rule and in response to environmental or operational changes affecting the security of electronic protected health information.

PROCEDURE

1. GCHD will perform periodic evaluations of its information system components to determine the level of security employed by GCHD. These evaluations may be conducted as part of GCHD's on-going risk analysis activities. Evaluations may be conducted through an external accreditation body or other outside entity.

2. The Security Officer or designee will document the outcome of the evaluation and make recommendations to management concerning any policy revisions or other changes needed to be incompliance.

REFERENCES

AS 3.1.1, Risk Analysis
AS 3.1.2, Risk Management
AS 3.7.4, Testing and Revision Procedures

45 C.F.R. § 164.308(a)(8)

Section 4.1	**Facility Access Controls**	**Effective Date:** 9/26/2013
		Revised: 06/14/2019

POLICY

GCHD will implement policies and procedures to limit physical access to its electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed.

PROCEDURE

1. Contingency Operations**.** In the event of an emergency, GCHD will implement as necessary, procedures to allow access to systems to support restoration of lost data. GCHD will establish operational contingencies to assist in the recovery of data and restoration of operations in the event of an emergency, including:

   a. Applications and data criticality analysis;

   b. Data Backup Plan;

   c. Disaster Recovery Plan;

   d. Emergency Mode Operation Plan;

   e. Testing and revision procedure;

2. Facility Security Plan. GCHD shall establish a plan to safeguard all facilities and equipment from unauthorized physical access, tampering or theft.

   a. GCHD will employ security personnel, security equipment, appropriate locking mechanisms, and/or alarms to protect all GCHD facilities during non-business hours.

   b. All employees will wear GCHD issued identification.

   c. Any sensitive equipment (servers, etc.) will be housed in a secure location and access to such equipment will be restricted to certain authorized personnel.

   d. Off-site equipment or files will be maintained in a secure location by GCHD or by an approved contractor who will certify that adequate security is maintained.

   e. Asset tags will be placed on all equipment and a log of all equipment shall be kept and updated quarterly by the department’s designated asset custodian.

f. Paper files containing sensitive or confidential information shall be securely retained in file cabinets, rooms, or off-site storage facilities.

g. Only authorized maintenance personnel will be allowed to service electronic equipment.

h. Appropriate documentation or logging protocols will be completed whenever hardware is transported.

i. Only hardware, software and equipment authorized by the Information Technology department shall be used within GCHD facilities.

j. Maintenance records on all equipment shall be kept and in accordance with record retention guidelines.

3. <u>Access Control and Validation Procedures</u>. GCHD will implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

a. *Physical Safeguards*. GCHD will implement the following physical safeguard procedures regarding verification of access authorization before granting physical access.

i. Unattended exterior doors will be protected by locks or badge readers.
ii. Visitors shall be prohibited from accessing facility areas designated solely for employees. Contract workers or other individuals requiring access to these areas shall always be accompanied by an authorized GCHD employee and at no time will be issued their own key or badge to access restricted areas.
iii. Electronic information systems or devices containing ePHI, including computer screens and printers will be shielded from the view of patients or visitors.

b. *Technical Security*. GCHD will implement technical security mechanisms to limit access control to employees. Technical security mechanisms will include user-based access controls to protect sensitive communication transmissions, and will be made available solely to those employees who require such access to fulfill their professional responsibilities.

c. *Reporting Unauthorized Access*. Employees who observe a person attempting to enter GCHD facilities or systems by bypassing security measures in an unauthorized manner must report this information immediately to his/her supervisor, Manager of Information Technology, or Security Officer.

4. Maintenance Records. GCHD will document repairs and modifications to the physical components of GCHD’s facilities which are related to security (for example, hardware, doors, and locks). These documents will be retained according to GCHD’s record retention guidelines and procedures.

REFERENCES

AS 3.1.4, Information Systems Activity Review
AS 3.3, Workforce Security
AS 3.5.4, Log-In Monitoring
AS 3.6, Security Incident Procedure
AS 3.7, Contingency Plan
AS 3.8. Evaluation
TS 5.1.2, Emergency Access Procedure
TS 5.2, Audit Controls

45 C.F.R. § 164.310(a)

Section 4.2	Workstation Use	Effective Date: 9/26/2013
		Revised: 06/14/2019

POLICY

GCHD will implement an adequate level of security procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the workstations that can access ePHI. This applies to all devices that have access to ePHI, including computers, laptops, tablets, smart phones, etc.

PROCEDURE

1. All employees will monitor their computers and report any potential threats to the computer and to the integrity and confidentiality of data contained in the computer system to the Manager of Information Technology, Security Officer or their immediate supervisor. All employees will take appropriate measures to protect computers and data from damage or destruction to the greatest possible extent. As part of every employee's orientation and, if appropriate, in ongoing security training sessions, all employees shall familiarize themselves with GCHD's emergency response plans and related policies and procedures as directed by management.

2. Employees will ensure that computer monitors are placed so the screen is not visible to unauthorized persons to prevent unauthorized persons from viewing electronic protected health information. Workstations displaying ePHI that may be visible to non-authorized individuals shall be equipped with screen protectors.

3. Workstations will have a password protected screensaver. Computer employees logging onto the system will ensure that no one observes entry of their password. Employees will neither log onto the system using another person's password nor permit another person to log onto the system with their password. Employees are responsible for all actions taken under their passwords.

4. Virus software will be installed on all computers as directed by the Manager of Information Technology or the Security Officer. Employees must ensure that the virus software is active at all times, unless directed to deactivate the software by the Manager of Information Technology or the Security Officer.

5. ePHI may only be accessed on a need to know basis. Employees will only have access to the information required to perform their job functions.

6. No employee will disclose ePHI unless authorized to do so in accordance with GCHD policies.

7. Employees will not leave printers unattended when PHI is being printed. PHI will be printed only when necessary and in accordance with the “minimum necessary” under GCHD’s HIPAA policy, and shall be promptly disposed of according to GCHD’s record retention guidelines (i.e., by shredding, secured disposal bins, etc.) when no longer needed for the purpose for which it was printed.

8. Employees must log off the system when leaving their computer or workstation unattended. Computers will be with a “time-out” feature that will activate after a certain period of idleness.

9. Employees are responsible for the accuracy of data input into systems and applications. Supervisors will monitor the processes used by employees for data entry.

10. Employees will not attempt to evade access rights granted or attempt to access networks, systems, applications, or data to which the employee has not been granted access.

11. Employees will not download data from the computer system onto diskette, CD, hard drive, fax, scanner, any network drive or any other hardware, software or paper without the express permission of the employee’s supervisor, the Manager of Information Technology, or the Security Officer.

12. Employees will not download software they’re unfamiliar with without first consulting their supervisor, the Manager of Information Technology, or Security Officer.

13. Employees violating this policy may be subject to disciplinary action up to and including termination.

REFERENCES

AS 3.5.5, Password Management
AS 3.6, Security Incident Procedures
PS 4.3, Workstation Security

45 C.F.R. § 164.310(b)

Section 4.3	**Workstation Security**	**Effective Date:** 9/26/2013
		Revised: 06/14/2019

POLICY

GCHD shall implement physical safeguards for all workstations that access ePHI to restrict access to authorized users. This applies to all devices that provide access to ePHI, including computers, laptops, tablets, smart phones, etc.

PROCEDURE

1. Each employee's workstation shall be configured in such a way as to promote the confidentiality and security of ePHI.

2. Computer monitors should be placed so that the screen is not visible to unauthorized persons to prevent unauthorized persons from viewing electronic protected health information.

3. Printers should not be placed in a location where there is a risk of unauthorized individuals having access to printed materials. Information shall be printed only when necessary and shall be promptly stored and/or disposed of according to GCHD's record retention and/or disposal policies.

4. Computer users logging onto the system will ensure that no one observes entry of their password. Employees will neither log onto the system using another person's password nor permit another person to log onto the system with their password. Employees are responsible for all actions taken under their passwords.

5. ePHI may only be accessed on a need to know basis. Employees will only have access to the information required to perform their job functions.

6. Portable devices, including laptops, portable storage devices, smart phones, etc., will be secured when not in use.

7. If an employee accesses ePHI from a portable device, the device must be password protected and encrypted, and the ePHI cannot be viewable to others.

8. Computers will have a time-out feature after a certain period of inactivity and a password protected screensaver.

9. Employees violating this policy may be subject to disciplinary action, up to an including termination.

REFERENCES

AS 3.5.1, Workforce Training
AS 3.5.3, Protection from Malicious Software
AS 3.5.5, Password Management
AS 3.6, Security Incident Procedures
AS 3.7, Contingency Plan
PS 4.2, Workstation Use
PS 4.4.1, Disposal
TS 501, Integrity Controls

45 C.F.R. § 164.310(c)

Section 4.4 **Device and Media Controls** **Effective Date:** 9/26/2013

Revised: 06/14/2019

POLICY

GCHD will implement reasonable and appropriate controls that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

PROCEDURE

1. Disposal. ePHI will be disposed of in a proper and secure manner to prevent unauthorized or accidental disclosure of such information.

    a. Disposal and/or destruction of items shall be conducted in accordance with GCHD's record retention, inventory and/or disposal guidelines.

    b. *Retained Hardware or Electronic Media*. The Manager of Information Technology or designee is responsible for completely removing ePHI from hardware that will be reused within GCHD.

    c. *Disposed Hardware or Electronic Media.* The Manager of Information Technology or designee is responsible for the final disposition of hardware that contains ePHI. All ePHI will be completely removed from the hardware before the hardware is sold or destroyed. Hardware will then be physically destroyed and rendered functionally unusable, and destruction certificates will be attained when appropriate.

2. Media Reuse. The Manager of Information Technology or designee will remove ePHI from electronic media before the media is made available for reuse. Employees may store ePHI solely in manners and on devices approved by the Manager of Information Technology or the Security Officer.

3. Accountability. GCHD will maintain a record of the transfer, disposal and other movement of hardware and electronic media. The organization shall also keep a record of the person currently in possession of such media.

    a. *Hardware*. GCHD will use inventory controls and take a quarterly inventory of each piece of GCHD owned hardware. The inventory will track the equipment's location and department. Hardware may only be removed from a GCHD facility with authorization from Executive Management or Manager of Information Technology. Removal will be logged.

    b. *Electronic Media*. Electronic media may only be removed from a GCHD facility with authorization from Executive Management or Manager of

Information Technology. Such removals or disposals will be appropriately logged.

4. Data Backup and Storage. Systems shall remain in-place to retrieve data, when needed, before the transfer of any equipment. The data backup procedures will be reviewed and tested periodically by the Manager of Information Technology of their designee. The backup data will then be stored in a secure location or restored on to equipment.

REFERENCES

AS 3.1.1, Risk Analysis
AS 3.7, Contingency Plan
PS 4.1, Contingency Operations

45 C.F.R. § 164.310(d)

Section 5.1	**Access**	**Effective Date:** 9/26/2013
		Revised: 06/14/2019

POLICY

GCHD will implement procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights.

PROCEDURE

1. Unique User Identification. All employees will be assigned a unique username and number for identifying and tracking user identity.

    a. Each computer user shall be assigned a unique username and number ("user ID"). The user ID, as well as a password chosen by the employee in accordance with GCHD password policy, will be required to access any GCHD system. An individual may be assigned the same user ID for access to multiple systems.

    b. The Manager of Information Technology or designee will provide the computer user with a user ID. A record of all user IDs will be maintained in a secure setting.

    c. User IDs will be immediately deactivated, and user access will be revoked upon the resignation or termination of an employee.

2. Automatic Log off. GCHD will implement electronic procedures that terminate an electronic session after a predetermined period of time.

    a. Password-protected screensavers will activate at all workstations if there is no activity at a workstation for a set period of time.

3. Encryption and Decryption. GCHD has determined that it is appropriate to implement encryption software on systems that contain ePHI.

    a. All employees who transmit ePHI via email must encrypt the email before sending the information to a party outside of the GCHD network.

    b. Employees are prohibited from sending ePHI over non-secured networks.

REFERENCES

AS 3.3.3, Termination Procedure
AS 3.5.5, Password Management
AS 3.7, Contingency Plan
PS 4.1.1, Contingency Operations
PS 4.2, Workstation Use
PS4.3, Workstation Security
TS 5.2, Audit Controls
TS 5.3, Integrity Controls
TS 5.4, Authentication of Entity or Person
TS5.5.2, Encryption

45 C.F.R. § 164.312(a)

Section 5.2 **Audit Controls** **Effective Date:** 9/26/2013
Revised: 06/14/2019

POLICY

GCHD will implement hardware, software, and/or procedural mechanisms that record and examine activity occurring on organizational information systems that contain or use ePHI.

PROCEDURE

1. *Audit Control Mechanism*. The Security Officer is responsible for conducting audits on information systems that track user access. The computer system will have hardware/software or another procedural mechanism in-place whereby individual employees can be tracked.

2. *Activities to be Tracked*. These audits, which shall occur if there's reason to believe an employee has impermissibly accessed ePHI or as directed by the Chief Compliance Officer or Chief Executive Officer, will examine specific tracking records created by employees accessing and documenting confidential information. Such activities will include, but are not limited to, unsuccessful log-in attempts and unauthorized access.

3. *Review and Response*. Audits will be conducted at least semi-annually. The audit results will be reported to the Chief Executive Officer, Chief Compliance Officer, Manager of Information Technology, and Human Resources to further assess potential security weakness or further investigation. Such audits will be conducted to:

   a. Ensure integrity, confidentiality and availability of information and resources;

   b. Investigate possible security incidents and ensure conformance with security policies; and to

   c. Monitor user or system activity when appropriate.

4. *Audit Trails and Reports*. The Security Officer or their respective designee will be responsible for maintaining these audit trails and reports. These reports will be maintained in a secure location according to GCHD record retention guidelines.

REFERENCES

Policy AS104, Information Systems Activity Review
Policy AS 3.4, Information Access Management
Policy AS 3.5.4, Log-in Monitoring
Policy AS 3.5.5, Password Management
Policy PS 4.1.3, Access Control and Validation
Policy TS 5.1, Access

45 C.F.R. § 164.312(b)

Section 5.3	**Integrity of Electronic PHI**	**Effective Date:** 9/26/2013 **Revised: 06/14/2019**

POLICY

GCHD will implement procedures to protect ePHI from improper alteration or destruction.

PROCEDURE

1. The Manager of Information Technology or designee will implement policies and procedures to protect ePHI from improper alteration or destruction.

2. The Security Officer, Manager of Information Technology and Chief Compliance Officer will review policies and procedures on an annual basis to determine whether there is a need to impose electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. Determination will be considered in light of the current threats, available solutions, and costs and given to the Chief Compliance Officer or Chief Executive Officer for review.

REFERENCES

AS 3.1.4, Information Systems Activity Review
TS 5.2, Audit Controls

45 C.F.R. § 164.312(c)

Section 5.4	Authentication of Entity or Person	Effective Date: 9/26/2013 Revised: 06/14/2019

POLICY

GCHD will implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.

PROCEDURE

1. *Person Authentication*.

   a. A user ID and appropriate password will be required to access GCHD's information system.

   b. Users will be responsible for keeping their user IDs and passwords confidential.

   c. If a user becomes aware that someone has improperly accessed his or her user ID and/or password, the user must immediately notify their supervisor, the Manager of Information Technology and/or the Security Officer.

2. *Entity Authentication*.

   a. The Manager of Information Technology or designee will assign each entity needing access to GCHD's electronic information systems containing protected health information a unique user ID. A unique user ID and password will only be assigned to those entity personnel on a "need to know basis" to perform the task or service required.

   b. Entities (e.g. UTMB) will be responsible for keeping their user IDs and passwords confidential. Entities will not make their user ID and password available companywide.

   c. Entities must follow GCHD policies and procedures, including those listed in this Security Manual.

   d. Entities must immediately notify the GCHD Manager of Information Technology and Security Officer if they become aware that someone has improperly accessed his or her user ID and/or password.

REFERENCES

AS 3.4, Information Access Management
AS 3.5, Awareness and Training
TS 5.1.1, Unique User Identification
TS 5.2, Audit Controls

45 C.F.R. § 164.312(d)

Section 5.5	**Transmission Security**	**Effective Date:** 9/26/2013
		Revised: 06/14/2019

POLICY

GCHD will implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

PROCEDURE

1. Integrity Controls. GCHD will implement, where appropriate, security measures to ensure that ePHI is not modified by unauthorized users.

    a. A user ID and appropriate password will be required to access GCHD's information system.

    b. Audit controls will be established to track access to the system and any modifications to ePHI and tracking records will be reviewed by the Manager of Information Technology, the Security Officer, and the Chief Compliance Officer on at least an annual basis.

    c. The ePHI will be protected from unauthorized Internet access through the use of firewalls and authentication devices.

2. Encryption. GCHD will implement, where appropriate, a mechanism to encrypt ePHI.

    a. All employees who transmit protected health information via email must encrypt the email before sending the information outside GCHD.

3. *Security Protection*. The Security Officer or designee will implement procedures to protect ePHI that is transmitted over an electronic communications network.

REFERENCES

Policy PS 4.1.3, Access Control and Validation Procedures
Policy TS 5.1, Access
Policy TS 5.3, Integrity of Electronic PHI
Policy TS 5.4, Authentication of Entity or Person

45 C.F.R. § 164.312(e)