Gaston County IT

HIPAA

Manual

Version 10-01-2018

Table of Contents

Action	Date
Reviewed and revised	10/01/2018

Introduction

This IT HIPAA Manual is a continuation of the Gaston County HIPAA Manual. The IT HIPAA Manual allows a more dynamic update process for the specific policies within this manual.

Title II of HIPAA comprises of five separate rules. This IT HIPAA Manual focuses only on the Security Rule of Title II of the HIPAA.

There are four types of Security Safeguards required for compliance of the Security Rule:

1. Administrative Safeguards.
2. Physical Safeguards.
3. Organizational Safeguards.
4. Policy & Procedures Safeguards.

• A required implementation specification is similar to a standard, in that a covered entity must comply with it. For example, all covered entities including small providers must conduct a "Risk Analysis" in accordance with Section 164.308(a)(1) of the Security Rule.

• For addressable implementation specifications, covered entities must perform an assessment to determine whether the specification is a reasonable and appropriate safeguard in the covered entity's environment. After performing the assessment, a covered entity decides if it will implement the addressable implementation specification; implement an equivalent alternative measure that allows the entity to comply with the standard; or not implement the addressable specification or any alternative measures, if equivalent measures are not reasonable and appropriate within its environment. ***Covered entities are required to document these assessments and all decisions.***

• Factors that determine what is "reasonable" and "appropriate" include cost, size, technical infrastructure and resources. While cost is one factor entities must consider in determining whether to implement a particular security measure, some appropriate measure must be implemented. ***An addressable implementation specification is not optional, and the potential cost of implementing a particular security measure does not free covered entities from meeting the requirements identified in the rule."***

Defining Protected Health Information (PHI).

Although there are a few exceptions, if any health care is provisioned (was provided or will be provided), any one of the eighteen 18 individual identifiers classifies it as Protected Health Information.

Identifiers

Data are "individually identifiable" if they include any of the 18 types of identifiers, listed below, for an individual or for the individual's employer or family member, or if the provider or researcher is aware that the information could be used, either alone or in combination with other information, to identify an individual:

- Name
- Address (all geographic subdivisions smaller than state, including street address, city, county, zip code)
- All elements (except years) of dates related to an individual (including birth date, admission date, discharge date, date of death and exact age if over 89)
- Telephone numbers
- Fax number
- Email address
- Social Security number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate/license number
- Any vehicle or other device serial number
- Device identifiers or serial numbers
- Web URL
- Internet Protocol (IP) address numbers
- Finger or voice prints
- Photographic images
- Any other characteristic that could uniquely identify the individual

HIPAA Documentation.

Full HIPAA documentation is comprised of the following:

1. Gaston County HIPAA Manual.
2. Gaston County Personnel Policies and Procedures Manual.
3. Gaston County Disaster Recovery Plan.
4. Gaston County IT HIPAA Manual (this document).
5. Gaston County IT HIPAA Support Documentation.
6. Gaston County IT HIPAA Audits & Review Documentation.

IT HIPAA Policy Reference & Naming Convention

All documents start with the letters ITSP representing IT Security Policy.
The next three digits refer to the HIPAA section starting with the number after the decimal.
The final three digits refer to plus the 1st digit being the consecutive count plus each sub-section counting by ten's.

For example the HIPAA section - Information Access Management - Section: § 164.308(a)(4) with the sub category of Isolating Health Care Clearinghouse Functions would result in a policy number of
ITSP - 308-1-10

Gaston County IT HIPAA Security Matrix

Administrative Safeguards	Required or Addressable
Security Management Process - Section: § 164.308(a)(1)	
• Risk Analysis See Gaston County IT HIPAA Audits & Review Documentation dated 09/08/2008	R
• Risk Management Defined, Gaston County HIPAA Manual, Policy 02-001	R
• Sanction Policy Defined, Gaston County HIPAA Manual, Policy 02-013	R
• Information System Activity Review Defined, Gaston County HIPAA Manual, Policy 03-001	R
Assigned Security Responsibility - Section: § 164.308(a)(2)	
• Assign Security Responsibility Defined, Gaston County HIPAA Manual, Policy 01-001, HIPAA Compliance Officer	R
Workforce Security - Section: § 164.308(a)(3)	
• Authorization and/or Supervision Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 308-3-10.	A
• Workforce Clearance Procedure Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 308-3-20.	A
• Termination Procedures Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 308-3-30.	A

Information Access Management - Section: § 164.308(a)(4) • Isolating Health Care Clearinghouse Functions Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 308-4-10. • Access Authorization Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 308-4-20. • Access Establishment and Modification Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 308-4-30.	R A A
Security Awareness and Training - Section:§ 164.308(a)(5) • Security Reminders Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 308-5-10. • Protection from Malicious Software Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 308-5-20. • Log-in Monitoring Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 308-5-30. • Password Management Defined, Gaston County Personnel Policy, Chapter 26	A A A A
Security Incident Procedures- Section:§ 164.308(a)(6) • Response and Reporting Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 308-6-10.	R

Contingency Plan - Section: § 164.308(a)(7) • Data Backup Plan Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 308-7-10. • Disaster Recovery Plan Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 308-7-20. • Emergency Mode Operation Plan Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 308-7-30. • Testing and Revision Procedures Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 308-7-40. • Applications and Data Criticality Analysis Defined Gaston County Disaster Recovery Plan.	R R R A A
Evaluation - Section: § 164.308(a)(8) • Evaluation Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 308-8-10.	R
Business Associate Contracts and Other Arrangements - Section: § 164.308(b)(1) • Written Contract or Other Arrangement Defined, Gaston County HIPAA Manual, Policy 02-004	R

Physical Safeguards	Required or Addressable
Facility Access Controls - Section: § 164.310(a)(1) • Contingency Operations Defined Gaston County Disaster Recovery Plan. • Facility Security Plan Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 310-1-20. • Access Control and Validation Procedures Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 310-1-30. • Maintenance Records Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 310-1-40.	A A A A
Workstation Use - Section: § 164.310(b)	

• Define Workstation Use Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 310-2-10.	R
Workstation Security - Section: § 164.310(c) • Define Workstation Security Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 310-3-10.	R
Device and Media Controls - Section: § 164.310(d)(1) • Disposal Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 310-4-10. • Media Re-use Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 310-4-20. • Accountability Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 310-4-30. • Data Backup and Storage Existing Data Backup Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 310-4-40.	R R A A

Technical Safeguards	Required or Addressable
Access Control - Section: § 164.312(a)(1) • Unique User Identification Defined, Gaston County Personnel Policy, Chapter 26 • Emergency Access Procedure Defined, Gaston County Personnel Policy, Chapter 26 • Automatic Logoff Defined, Gaston County HIPAA Manual, Policy 03-02 • Encryption and Decryption Defined, Gaston County HIPAA Manual, Policy 03-02	R R A A
Audit Controls - Section: § 164.312(b)	

• Audit Control Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 312-2-10.	R
Integrity - Section: § 164.312(c)(2) • Mechanism to Authenticate Electronic Protected Health Information Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 312-3-10.	A
Person or Entity Authentication – Section: § 164.312(d) • Person or Entity Authentication Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 312-4-10.	R
Transmission Security – Section: § 164.312(e)(1) • Integrity Controls Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 312-5-00. • Encryption Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 312-5-00.	A A

Organizational Requirements

Business associate contracts or other arrangements - Section: § 164.314(a)(1) • Business associate contracts Defined, Gaston County HIPAA Manual, Policy 02-004 • Other Arrangements	R R
Requirements for Group Health Plans - Section: § 164.314(b)(1) • Implementation Specifications Defined, Gaston County HIPAA Manual, Policy 03-02	R

Policies, Procedures and Documentation Requirements	
Policies and Procedures - Section: § 164.316(a) • Creation and Maintenance Defined, Gaston County HIPAA Manual, Policy 01-001	R
Documentation - Section: § 164.316(b)(1) • Time Limit Defined, Gaston County HIPAA Manual, Policy 01-001 • Availability Defined, Gaston County HIPAA Manual, Policy 01-001 • Updates Defined, Gaston County HIPAA Manual, Policy 01-001	R R R

Gaston County IT HIPAA Manual Policies

Policy Enforcement

Any employee found to have violated this policy may be subject to disciplinary action. Any third party provider found to have violated this policy may be subject to termination of service.

Requirements

Any documentation is to be placed in the document “IT HIPAA Support Documentation” under the section titled to correspond with the policy number (eg. ”ITSP - 308-3-10”).

This should include dates of the review process and note any reasons, limitations or exceptions to the policy at the given date, the maintenance of lists or any other documentation related to the policy. Any changes made should be dated along with the changes.

Definitions

Electronic Protected Health Information (ePHI) - Individually Identifiable Health Information (IIHI) that is transmitted by electronic media; maintained in electronic media, such as magnetic tape, disc, optical file; or transmitted or maintained in any other form or medium.

Health Care Clearinghouse - a public or private entity, including a billing service, re-pricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions:

1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity. [45 CFR 160.103]

Secure Location - a secure location would minimally be defined as one that is not routinely accessible to the public, particularly if authorized personnel are not always available to monitor security.

Workstation - is defined in the rule as “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.”

Policy: # ITSP – 308-3-10

IT Security Policy – Authorization and/or Supervision

HIPAA: Workforce Security - Section: § 164.308(a)(3)

1. Purpose

The purpose of this policy is to define a method to authorize and/or supervise the workforce members who work with ePHI (Electronic Protected Health Information) or in locations where it might be accessed.

2. Scope

This policy applies to all Gaston County employees, agents, vendors, and third party entities that have access to EPHI on Gaston County systems.

3. Policy
   - 3.1 Role-Based Access – Department Heads or their designees shall create and maintain a role-based list to determine who has the authority to determine who will have access ePHI , including employees, agents, vendors, and third party entities.
   - 3.2 This list must be documented.
   - 3.3 Review Cycle - The list should be reviewed and updated annually.

4. Revision and Examination History
   09/14/2010; 10/01/2018

Policy: # ITSP – 308-3-20

IT Security Policy – Workforce Clearance Procedure

HIPAA: Workforce Security - Section: § 164.308(a)(3)

1. Purpose

The purpose of this policy is to implement procedures to determine that the access of a workforce member to ePHI (Electronic Protected Health Information) is appropriate.

2. Scope

This policy applies to all Gaston County employees, agents, vendors, and third party entities that have access to EPHI on Gaston County systems.

3. Policy

3.1 Review Role-Based Access Identification – Information Technology shall create and/or modify Role-Based Active Directory created Groups that places ePHI members in an identifiable group that is consistent with the job functions of the workforce and have access to the necessary information.

3.2 Review Cycle - The specific groups and methods should be reviewed and updated annually.

4. Revision and Examination History

09/10/2010; 10/01/2018

Policy: # ITSP – 308-3-30

IT Security Policy – Termination Procedures

HIPAA: Workforce Security - Section: § 164.308(a)(3)

1. Purpose

The purpose of this policy is to implement procedures for terminating access to ePHI (Electronic Protected Health Information) when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a) (3) (ii) (B) of this section, which is the Workforce Clearance Procedure (see ITSP – 308-3-20).

2. Scope

This policy applies to all Gaston County employees, agents, vendors, and third party entities that have access to EPHI on Gaston County systems.

3. Policy

3.1 Termination of ePHI Access – When any member of the workforce no longer requires access of ePHI to perform their job functions, termination of access to the ePHI is required.

3.2 Termination of Physical Access – When any member of the workforce has been terminated, physical access, whether key card, ID card, etc. must be discontinued.

3.3 Authorization to Terminate Access – authorization for termination is initiated by authorized personnel, whether a supervisor of ePHI, Human Resources, or Gaston County IT.

3.4 Timing of Termination of Access – Termination to the ePHI is required in a timely manner.

4. Revision and Examination History

09/10/2010; 10/01/2018

Policy: # ITSP – 308-4-10

IT Security Policy – Isolating Health Care Clearinghouse Functions

HIPAA: Information Access Management - Section: § 164.308(a)(4)

1. Purpose

The purpose of this policy is to define servers containing ePHI data, access standards for these servers internally and by third party providers, and methods to isolate these servers.

2. Scope

This policy applies to all Gaston County servers containing ePHI data.

3. Policy
   - 3.1 Server Identification – Create and maintain a list of servers containing ePHI data.
   - 3.2 Access Identification – Create and maintain a list of third party entities, including vendors, who access these systems.
   - 3.3 Third Party Process – Create and maintain a list of the process each third party entity uses to access the Gaston County ePHI.
   - 3.4 Isolation Identification – Document methods to isolate the ePHI internally.
   - 3.5 Review Cycle - The specific lists and methods should be reviewed and updated annually.

4. Revision and Examination History
   09/10/2010; 10/01/2018

Policy: # ITSP – 308-4-20

IT Security Policy – Access Authorization

HIPAA: Information Access Management - Section: § 164.308(a)(4)

1. Purpose

The purpose of this policy is to define the procedure for granting access to the ePHI (Electronic Protected Health Information) for example, through access to a workstation, transaction, program, process, or other mechanism.

2. Scope

This policy applies to all Gaston County employees that have access to EPHI on Gaston County systems.

3. Policy

3.1 Each employee is required to sign the Gaston County Confidentiality Agreement and have this Agreement placed in their Personnel file prior to access to ePHI.

3.2 Access Authorization Request - Defined in the effective Gaston County Personnel Policies titled, "USE OF INFORMATION TECHNOLOGY RESOURCES" located under the "Security" section subsections "Network and System Access" of the "Procedures Manual Section." This policy requires the department director's or appointee's approval.

3.3 Employees must receive HIPAA and security awareness training prior to obtaining access to ePHI.

4. Revision and Examination History

09/10/2010; 10/01/2018

Policy: # ITSP – 308-4-30

IT Security Policy – Access Establishment and Modification

HIPAA: Information Access Management - Section: § 164.308(a)(4)

1. Purpose

The purpose of this policy is to administer initial user access, review existing access, and maintain changes in user access and to document these activities.

2. Scope

This policy applies to all Gaston County employees, agents, vendors, and third party entities that have access to EPHI on Gaston County systems.

3. Policy

3.1 Establishment and modification of access - When any member of the workforce requires access of ePHI to perform their job functions or changes to their level of access, a documented request by an authorized ePHI authority (see ITSP - 308-3-10) is required.

3.2 Access Identification – The ability to generate a report of authorized users of ePHI and their access level is required to allow review of authorization of access to ePHI.

3.3 Review Cycle - The access should be reviewed and updated annually.

4. Revision and Examination History

09/10/2010; 10/01/2018

Policy: # ITSP – 308-5-10

IT Security Policy – Security Reminders

HIPAA: Security Awareness and Training - Section: § 164.308(a)(5)

1. Purpose

The purpose of this policy is to define the policy to implement a security awareness and training program of ePHI for all members of its workforce, including management.

2. Scope

This policy applies to all Gaston County employees that have access to ePHI on Gaston County systems.

3. Policy

3.1 In addition to the initial HIPAA, and Security Awareness training received prior to obtaining access to ePHI as defined in ITSP-308-4-30, each employee must receive periodic training on HIPAA and Security Awareness. Training will be developed and maintained by either Gaston County IT, Human Resources or both. Training may be instructor led, on-line or in book form.

3.2 Additional awareness informational alerts regarding changes to HIPAA policies and procedures, as well as security notices or updates regarding current threats will be made available via email, Intranet, or other methods. This information should be made available periodically.

3.3 Documentation of all HIPAA training related activities is required and must be placed in the employee's Personnel File or HIPAA related repository.

4. Revision and Examination History

12/09/2010; 10/01/2018

Policy: # ITSP – 308-5-20

IT Security Policy – Protection from Malicious Software

HIPAA: Security Awareness and Training - Section: § 164.308(a)(5)

1. Purpose

The purpose of this policy is to define the requirements to guard against, detect, and report malicious software, such as computer viruses, Trojan horses, spyware, and other similar items.

2. Scope

This policy applies to all Gaston County computers that have access to ePHI on Gaston County systems.

3. Policy

3.1 Information Technology shall create and maintain a method to install, maintain, and track Operating System and Application Software security related patches and updates.

3.2 Have a method to install, maintain, and track Anti-Virus and Anti-Spyware along with updates to the definitions.

4. Revision and Examination History

12/09/2010; 10/01/2018

Policy: # ITSP – 308-5-30

IT Security Policy –Log-in Monitoring

HIPAA: Security Awareness and Training - Section: § 164.308(a)(5)

1. Purpose

The purpose of this policy is to define procedures for monitoring log-in attempts and reporting discrepancies.

2. Scope

This policy applies to all Gaston County employees, agents, vendors, and third party entities that have access to ePHI on Gaston County systems.

3. Policy

3.1 Logging for Gaston County ePHI Servers – Information Technology shall create a centralized logging system to consolidate all attempts, both successful and failed, of login of the servers that contain ePHI as defined in the Gaston County IT HIPAA Manual Policy #ITSP – 308-4-10.

3.2 Discrepancy Reporting – Information Technology shall create a report based on failed login attempts.

3.3 Account Lockout – Windows Domain failed login attempts exceeding a limited number of attempts will automatically lock the account for set time period to prevent brute force attacks.

3.4 Review and Document – Review the Discrepancy Report on a timely basis.

3.5 Applications that are not in the scope of control by Gaston County are excluded, such as North Carolina ITS applications. It is the responsibility of that entity to maintain logging for their systems. Any application exceptions should be noted as established herein of this policy.

3.6 Retention Cycle - The logs must be retained for seven years from the date of creation as defined by HIPAA.

4. Revision and Examination History

12/09/2010; 10/01/2018

Policy: # ITSP – 308-6-10

IT Security Policy – Response and Reporting

HIPAA: Security Incident Procedures - Section: § 164.308(a)(7)

1. Purpose

The purpose of this policy is to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

2. Scope

This policy applies to all Gaston County servers identified as containing ePHI.

3. Policy

3.1 Members of the IT Department, Managers, Directors, Supervisors or any County employee that has been made aware of an ePHI security issue should notify the Service Desk, who would open a ticket for tracking and resolving the security event. Examples of security incidents include:

- Stolen or otherwise inappropriately obtained passwords that are used to access ePHI.
- Corrupted backup tapes that do not allow restoration of ePHI.
- Virus or spyware attacks that interfere with the operations of information systems with ePHI.
- Physical break-ins leading to the theft of media with ePHI.
- Failure to terminate the account of a former employee that is then used by an unauthorized user to access information systems with ePHI.
- Providing media with ePHI, such as a PC hard drive or laptop, to another user who is not authorized to access the EPHI prior to removing the ePHI stored on the media.

3.2 Gaston County may or may not engage third-party security monitor. Security incidents that occur outside the network may have separate tracking by third-party vendors

4. Revision and Examination History

11/7/2017; 10/01/2018

Policy: # ITSP – 308-7-10

IT Security Policy – Data Backup Plan

HIPAA: Contingency Plan - Section: § 164.308(a)(7)

1. Purpose

The purpose of this policy is to establish and implement procedures to create and maintain retrievable exact copies of ePHI (Electronic Protected Health Information).

2. Scope

This policy applies to all Gaston County servers identified as containing ePHI.

3. Policy
   - 3.1 Backup for Gaston County ePHI Servers – Information Technology shall perform backups of data for the servers that contain ePHI, which are identified in the Gaston County IT HIPAA Manual Policy #ITSP – 308-4-10, must be performed daily for a five business day week.
   - 3.2 Backup Solution Details – Backups can reside on tape or disk, using the Backup application listed in the ITSP-308-7-10-Support-Documentation, which also needs to include detailed information on what is being stored and how.
   - 3.3 Retrievable State – Backups must be able to restore data as retrievable exact copies.
   - 3.4 Backup Storage – Backups must be stored in a secure environment.
   - 3.5 Backup Solution End-of-Life – In the event a backup solution has reached its end-of-life, the information must still be retrievable for seven years. If the new solution does not support access to the backup format or media type, third-party services can be used for this conversion on an as-needed basis.
   - 3.6 Retention Cycle - ePHI backups must be able to be retrievable for seven years.

4. Revision and Examination History
   11/7/2017; 10/01/2018

Policy: # ITSP – 308-7-20

IT Security Policy – Disaster Recovery Plan

HIPAA: Contingency Plan - Section: § 164.308(a)(7)

1. Purpose

The purpose of this policy is to establish (and implement as needed) procedures to restore any loss of data. Since a Gaston County Disaster Recovery Plan exists, this policy will address the details of the location, how to access, who can access, and any other vital information that defines the resources, action, and data required to re-instate critical business processes that have been damaged because of a disaster.

2. Scope

This policy applies to all Gaston County employees, agents, vendors, and third party entities who would be involved in the reinstatement of the critical business processes that have been damaged because of a disaster.

3. Policy
   - 3.1 Departments in conjunction with Information Technology shall create a list of the ePHI that must be backed up.
   - 3.2 Location of the Gaston County Disaster Recovery Plan – a list defining the location of the Gaston County Disaster Recovery Plan in electronic and paper format.
   - 3.3 Updates to the Location of the Plan – any updates to the location of the Gaston County Disaster Recovery Plan will need to be updated in the "IT HIPAA Support Documentation," as soon as possible.
   - 3.4 How to Access – a detailed process must be created and maintained to clarify the steps to access the data, any specific computer hardware or software needed, and keys or access codes.
   - 3.5 Access to the Gaston County Disaster Recovery Plan – a list must be created and maintained for the persons or entities that have access to the Gaston County Disaster Recovery Plan.

4. Revision and Examination History
   12/09/2010; 10/01/2018

Policy: # ITSP – 308-7-30

IT Security Policy –Emergency Mode Operation Plan

HIPAA: Contingency Plan - Section: § 164.308(a)(7)

1. Purpose

The purpose of this policy is to establish procedures that enable continuation of critical business processes of the security of ePHI systems while operating in an emergency mode, such as a natural disaster, system failure, etc.

2. Scope

This policy applies to all Gaston County employees, agents, vendors, and third party entities that have access to ePHI on Gaston County systems.

3. Policy
   - 3.1 Physical Safeguards – an Emergency Mode site and computers must continue to maintain the physical safeguards to protect ePHI. Physical systems need to continue to be protected behind a locked door.
   - 3.2 Logging for Gaston County ePHI Applications – the County shall continue logging of physical access to servers that contain ePHI regardless of Emergency Mode site – refer to Gaston County IT HIPAA Manual, Policy # ITSP - 310-1-20.
   - 3.3 Transporting ePHI Servers, Backup Tapes, or Other Media – the physical transportation of ePHI to restore a site or maintain a site that is in Emergency Mode requires attention to security. The media that contains ePHI data should not be left unattended and the vehicle should always be locked.
   - 3.4 Connectivity to the Emergency Mode site - security to connect to the Emergency Mode site with other sites require a secure physical network or an encrypted VPN tunnel to protect data during transportation as well as the ePHI servers from unauthorized access.
   - 3.5 Contact List – the Emergency Mode Operation Plan must include a list of personnel with contact information needed for the restoration process.

4. Revision and Examination History
   12/09/2010; 10/01/2018

Policy: # ITSP – 308-7-40

IT Security Policy –Testing and Revision Procedures

HIPAA: Contingency Plan - Section: § 164.308(a)(7)

1. Purpose

The purpose of this policy is to implement procedures for periodic testing and revision of contingency plans. This includes the steps of what, how, documenting the success or failures, and how often the ePHI systems are tested for a simulation of a Disaster Recovery. This will also include revision procedures - the process of updating the Disaster Recovery Plan.

2. Scope

This policy applies to all parties involved with the testing of a disaster, including Gaston County employees, agents, vendors, and third party entities that have access to ePHI on Gaston County systems.

3. Policy

3.1 Systems Defined to Simulate a Disaster – Systems that will be tested are the servers that contain ePHI as defined in the Gaston County IT HIPAA Manual Policy #ITSP – 308-4-10. If testing requires non-ePHI systems to access this information, the non-ePHI systems will need to be simulated as well.

3.2 Security Access to Application/Server – the person and/or group defined to test the environment may need temporary security access, as determined by Departments in conjunction with Information Technology, to the application or server in order to make a successful test.

3.3 Documentation of Test Results – a list of each ePHI server along with an inventory of each of the applications tested shall be documented. The results of the success or failure on the server level then on the application level shall be logged.

3.4 Test Cycle - The simulation testing must occur at least once every two years.

3.5 Revision Process – If additions, improvements, or changes are needed to the Disaster Recovery Plan from a result of the tests, a list of the changes will be placed in the support documentation for this policy and the Disaster Plan revised to reflect the change.

4. Revision History

12/09/2010; 10/01/2018

Policy: # ITSP – 308-8-10

IT Security Policy – Evaluation

HIPAA: Evaluation - Section: § 164.308(a)(8)

1. Purpose

The purpose of this policy is to establish procedures that define how often to periodically evaluate HIPAA compliance.

2. Scope

This policy applies to all Gaston County employees, agents, vendors, and third party entities that have access to ePHI on Gaston County systems.

3. Policy

3.1 Frequency of HIPAA Compliance Evaluation – an internal review of HIPAA Compliance should occur every two years.

4. Revision History

12/09/2010; 10/01/2018

Policy: # ITSP – 310-1-20

IT Security Policy – Facility Security Plan

HIPAA: Facility Access Controls - Section: § 164.310(a)(1)

1. Purpose

The purpose of this policy is designed to safeguard the facility and the equipment therein from unauthorized physical access, tampering and theft.

2. Scope

This policy applies to all Gaston County employees, agents, vendors, and third party entities that have access to ePHI on Gaston County systems.

3. Policy
   - 3.1 Systems and electronic media containing ePHI are to be located in physically secure locations.
   - 3.2 Secure locations must have physical access controls, such as Card Key, door locks, etc.
   - 3.3 Facility Security Plan – Information Technology shall create and maintain a list of ePHI Server Locations at Gaston County where the ePHI servers reside and how they are protected, such as card key or door lock.

4. Revision and Examination History
   12/09/2010; 10/01/2018

Policy: # ITSP – 310-1-30

IT Security Policy – Access Control and Validation Process

HIPAA: Information Access Management - Section: § 164.310(a)(1)

1. Purpose

The purpose of this policy is to 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.

2. Scope

This policy applies to all Gaston County employees, agents, vendors, and third party entities that have access to ePHI on Gaston County systems.

3. Policy

3.1 Access Plan for ePHI facilities – each facility must define roles or function-based access control, including access for visitors and service providers. This access control and validation procedure will be closely aligned with the Facilities Security Plan as defined by Gaston County IT HIPAA Manual Policy #ITSP – 308-1-20.

3.2 Periodic Review – review and implement termination procedures annually to ensure accuracy of allowable access authorization.

4. Revision and Examination History

12/09/2010; 10/01/2018

Policy: # ITSP – 310-1-40

IT Security Policy – Maintenance Records

HIPAA: Information Access Management - Section: § 164.308(a)(8)

1. Purpose

The purpose of this policy is to implement procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

2. Scope

This policy applies to all Gaston County employees, agents, vendors, and third party entities that have access to ePHI on Gaston County systems.

3. Policy
   - 3.1 Physical Maintenance – Information Technology shall create and maintain logs via card-swipe system that tracks maintenance personnel access to the physical environment where servers are, that contain ePHI, as defined in the Gaston County IT HIPAA Manual Policy #ITSP – 308-1-10. This applies to the HVAC systems, door locks, Uninterruptable Power Supplies (UPS), lighting, sprinkler systems, flooring, electrical work, or any other physical maintenance.
   - 3.2 Log Content – the information logged must include at least the location, date, time, name of person, vendor company name (if any).
   - 3.3 Retention Cycle - The logs must be retained for seven years from the date of creation as defined by HIPAA.

4. Revision and Examination History
   12/09/2010; 10/01/2018

Policy: # ITSP – 310-2-10

IT Security Policy – Define Workstation Use

HIPAA: Information Access Management - Section: § 164.310(d)(1)

1. Purpose

The purpose of this policy is to implement 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 surroundings of a specific workstation or class of workstation that can access ePHI. This will allow the protection of an ePHI designated workstation from being exposed to possible security violations due to accessing unnecessary non-ePHI applications.

2. Scope

This policy applies to all Gaston County workstations that contain or have contained ePHI.

3. Policy

3.1 Workstation Identification – create a method to classify ePHI workstations.

3.2 Workstation Roles – create a list of roles assigned to ePHI workstations.

3.3 Unencrypted ePHI – no unencrypted ePHI will reside on ePHI designated workstations.

3.4 Remote Access - any designated ePHI workstations that are remotely accessed will utilize encryption to access.

4. Revision and Examination History

12/09/2010; 10/01/2018

Policy: # ITSP – 310-3-10

IT Security Policy – Define Workstation Security

HIPAA: Information Access Management - Section: § 164.310(d)(1)

1. Purpose

The purpose of this policy is to implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.

2. Scope

This policy applies to all Gaston County workstations that contains or has contained ePHI.

3. Policy

3.1 Refer to idendification of ePHI workstations in "Define Workstation Use" (ITSP – 310-2-10), for devices that access ePHI.

3.2 Non-Portable Devices – Employees should prevent and report any unauthorized access to law enforcement and the Gaston County IT Department.

3.3 Portable Devices – Employees of Gaston County using Laptops, wireless devices, PDA's, etc., must make reasonable efforts to prevent theft or accidental loss of these devices.

4. Revision and Examination History

12/09/2010; 10/01/2018

Policy: # ITSP – 310-4-10

IT Security Policy – Device and Media Controls – Disposal

HIPAA: Information Access Management - Section: § 164.310(d)(1)

1. Purpose

The purpose of this policy is to clarify how all hardware or electronic media containing, or having contained, ePHI, should be destroyed.

2. Scope

This policy applies to all Gaston County workstations that contains or has contained ePHI.

3. Policy

3.1 Authorized Personnel to dispose of ePHI – only authorized personnel of ePHI are allowed to handle equipment for disposal.

3.2 Disposal of ePHI equipment – Information Technology shall be responsible for disposal of any device that contains or has contained ePHI.
Hard Disk – Hard drives are required to be wiped at minimum with a DOD approval 7 format. Alternatively, Hard Drives can be placed with one of the approved vendors that specialize in document and media disposal. If for whatever reason a DOD format will not work, the drive will be physically destroyed.
Tape, floppy, CD, DVD, or thumb drive – These media are to be wiped or destroyed in a manner which data is unrecoverable.

3.3 Record of Disposal – A record of disposal of ePHI is necessary. Refer to Gaston County IT HIPAA Manual Policy #ITSP – 310-4-30.

4. Revision and Examination History
12/09/2010; 10/01/2018

Policy: # ITSP – 310-4-20

IT Security Policy – Device and Media Controls – Media Re-use

HIPAA: Information Access Management - Section: § 164.310(d)(1)

1. Purpose

The purpose of this policy is to implement the removal of electronic protected health information from electronic media before the media are made available for re-use.

2. Scope

This policy applies to all Gaston County equipment that contains or has contained ePHI.

3. Policy

3.1 Re-use of ePHI Media by device:

Hard Disk – Hard drives are required to be wiped at minimum with a DOD approval 7 format before re-use.

Tape or Memory Stick – must be overwritten with software for this purpose or degauss the media.

Floppy, CD or DVD – This media is not acceptable for re-use and should be disposed in accordance with the Gaston County IT HIPAA Manual, Policy # ITSP - 310-4-10.

4. Revision and Examination History

12/09/2010; 10/01/2018

Policy: # ITSP – 310-4-30

IT Security Policy – Device and Media Controls – Accountability

HIPAA: Information Access Management - Section: § 164.310(d)(1)

1. Purpose

The purpose of this policy is to maintain a record of the movements of hardware and electronic media and any person responsible therefor.

2. Scope

This policy applies to all Gaston County physical storage that contains or has contained ePHI.

3. Policy

3.1 Logging of ePHI Storage Devices – Information Technology shall create and maintain a log to track all ePHI storage device history. This history should include from purchase to destruction. If device has been prepared for re-use, the date of the preparation as required in HIPAA IT Security Policy ITSP – 310-4-20, will be considered the date of (data) destruction. The devices include servers, PC's, and any other equipment that contain hard disks, tapes, CD's, DVD's, memory sticks or any other electronic device that stores or has stored ePHI.

3.2 Log Format - The log should at minimum state the media type, dates of purchase, date of destruction and method of disposal.

3.3 Log Retention – The log will be maintained for six years.

4. Revision and Examination History

12/09/2010; 10/01/2018

Policy: # ITSP – 310-4-40

IT Security Policy – Data Backup and Storage Existing Data Backup

HIPAA: Information Access Management - Section: § 164.310(d)(1)

1. Purpose

The purpose of this policy is to document the creation of a retrievable, exact copy of ePHI before movement of equipment, reallocating or destroying device media.

2. Scope

This policy applies to all Gaston County employees, agents, vendors, and third party entities that have access to EPHI on Gaston County systems.

3. Policy

3.1 Movement of Equipment – Before the movement of equipment that serves as the primary storage for ePHI, a backup of the ePHI must be made that would allow a retrievable, exact copy.

3.2 Reallocating or Destroying Device Media - Before the reallocation (re-use) or destruction of device media that serves as the primary storage for ePHI, a backup of the ePHI must be made that would allow a retrievable, exact copy.

4. Revision and Examination History

12/09/2010; 10/01/2018

Policy: # ITSP – 312-1-20

IT Security Policy – Emergency Access Procedure

HIPAA: Information Access Management - Section: § 164.312(d)(1)

1. Purpose

The purpose of this policy is to establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. This is an emergency plan that facilitates the exceptions to the normal operations policy in regards to accessing PHI, given that a recovery team may be deployed, which would not normally need access to PHI.

2. Scope

This policy applies to all Gaston County employees, agents, vendors, and third party entities that have access to ePHI on Gaston County systems.

3. Policy

3.1 Access Exception to ePHI – To facilitate the Gaston County Disaster Plan, access to ePHI is allowed for the recovery team for those on the team, who would not have access to ePHI in a normal operation mode.

4. Revision and Examination History

12/09/2010; 10/01/2018

Policy: # ITSP – 312-2-10

IT Security Policy – Audit Control

HIPAA: Information Access Management - Section: § 164.312(b)

1. Purpose

The purpose of this policy is to document the implementation of hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain ePHI.

2. Scope

This policy applies to all Gaston County employees, agents, vendors, and third party entities that have access to ePHI on Gaston County systems.

3. Policy
   - 3.1 Capturing ePHI activity – Information Technology shall ensure that the systems' capabilities are being used to capture ePHI activity.
   - 3.2 Examination of ePHI activity – Create a system and/or procedure for examination of ePHI activity logs.
   - 3.3 Review Cycle – If an automated alert system is in place, no specific review cycle is needed. Otherwise, a review must be done periodically.

4. Revision and Examination History
   12/09/2010; 10/01/2018

Policy: # ITSP – 312-3-10

IT Security Policy – Mechanism to Authenticate

HIPAA: Information Access Management - Section: § 164.312(c)(2)

1. Purpose

The purpose of this policy is to implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

2. Scope

This policy applies to all Gaston County employees, agents, vendors, and third party entities that have access to ePHI on Gaston County systems.

3. Policy

3.1 All verification/digital signature/checksum capabilities available with the software systems utilized will be implemented.

3.2 Laptops containing ePHI – since laptops cannot be assured of physical protection, laptops containing ePHI are required to maintain hard disk encryption to protect any data from alteration during use and storage.

4. Revision and Examination History

12/09/2010; 10/01/2018

Policy: # ITSP – 312-4-10

IT Security Policy – Person or Entity Authentication

HIPAA: Information Access Management - Section: § 164.312(e)(1)

1. Purpose

The purpose of this policy is to implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

2. Scope

This policy applies to all Gaston County employees, agents, vendors, and third party entities that have access to ePHI on Gaston County systems.

3. Policy
   - 3.1 Authentication Mechanism – Gaston County requires an Active Directory and/or i5/OS account with safeguards in place, such as password expiration, and limited number of log on attempts, to access ePHI systems.
   - 3.2 Each User must be provided with a unique account that may not be shared.
   - 3.3 Each User must log in with their given account and may not log in with another user's account.
   - 3.4 User credentials must be encrypted where stored.

4. Revision and Examination History
   12/09/2010; 10/01/2018

Policy: # ITSP – 312-5-00

IT Security Policy – Integrity Controls & Encryption

HIPAA: Information Access Management - Section: § 164.312(d)

1. Purpose

The purpose of this policy is to implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

2. Scope

This policy applies to all Gaston County employees, agents, vendors, and third party entities that have access to ePHI on Gaston County systems.

3. Policy

3.1 Wireless Transmission – Any wireless transmission of ePHI via Gaston County's network requires a tunnel using AES or higher encryption.

3.2 Internet – Any transmission through the Internet of ePHI requires the use of an SSL, ipsec tunnel or similar protection.

3.3 Email – Any transmission of email containing or an attachment that contains ePHI to the email requires the use of an SSL based solution or another encrypted method.

3.4 Laptops – Any laptop that contains ePHI must have the drive encrypted.

4. Revision and Examination History

12/09/2010; 10/01/2018

Policy: # ITSP – 400-1-10

IT Security Policy – Data Breach Policy

1. Purpose

The purpose of this policy is to define procedures to follow in the event of a data breach involving personally identifying information (PII) or other confidential information maintained on personal computers, agency networks, or internet programs used by staff and volunteers.

2. Scope

This policy applies to all Gaston County employees, agents, vendors, and third party entities that have access to ePHI on Gaston County systems.

3. Policy

Gaston County has implemented the following procedures to follow in the event of a data breach involving personally identifying information (PII) or other confidential information maintained on personal computers, agency networks, or internet programs used by staff and volunteers.

The following staff have key responsibility for implementing and executing the data breach procedures:

- First point of contact: HIPAA Compliance Officer: Sam Shames, Asst. County Attorney, 704-866-3194
- Second point of contact: HIPAA Privacy Official: Steve Eaton, DHHS, Div. of Public Health, 704-853-5271
- Third point of contact: HIPAA Security Officer: Ricky Johnson, Chief Information Officer, 704-866-3117

In an effort to prevent a breach of data and PII, Gaston County has implemented the following measures to prevent the breach of data:

- Technical Service Provider: Gaston County IT
- Anti-Virus/Intrusion Protection: McAfee Antivirus and Next Gen Firewalls at the perimeter.
- Personnel Access to Agency Computers: AD access for network and Application access for PHI data
- Law Enforcement Support to locate and apprehend perpetrators: County Police Department

Gaston County has identified the following items as critical systems and files that will be uploaded to a back-up system on an interval basis as described below:

- CLIENT DATA FILES, Daily
- CLIENT CASE FILES, Daily
- AGENCY FINANCIAL RECORDS, Daily
- OTHER CRITICAL/CONFIDENTIAL INFORMATION, Daily

In the event of a data breach or imminent breach of PII data, in order to contain the data breach and minimize the extent of the intrusion, the following actions will be taken:

- The affected and related systems or networks will be disconnected from internet access.
- The first, second, and third responders will be contacted to notify them of the data breach or imminent breach of PII data.
- The date and time the breach occurred will be documented, as well as what files the user was accessing at the time of the breach, the breach team member contacted, and actions taken to secure data.
- The technical support service provider will be contacted to detect and remove the malware or other information related to the breach.
- The Grants Manager at GCC will be notified within 24 hours of the breach occurrence or detection of the breach/recognition of imminent breach. Within 24 hours of the breach the Project Director must notify the GCC VOCA Administrator of the data breach, to forward the information to appropriate staff at the U.S. Office for Victims of Crime. If no Project Director is designated, the HIPAA Compliance Office shall make the appropriate notifications.
- The virus/malware/other protective software will be reviewed to assess system vulnerabilities and increase the level of protection for the system.
- If possible, the system will be reimaged and/or restored from backup files.

Following the incident, Gaston County staff will review procedures to determine if any actions by the user or the team contributed to the data breach. Staff will be updated on policies to protect against data breaches or imminent breaches of PII data.

A computer technician will review software, updates, and software/data protection programs to improve the security of the data and operating system to prevent further incidents. Information related to the data breach will be documented on the incident log, repairs or modifications implemented will be included on the log and kept in a secure location.

If necessary, the management team will review procedures and make necessary changes to the procedures to improve the security of PII and other secure information.

4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action. Any third party provider found to have violated this policy may be subject to termination of service.

5. Definitions

Electronic Protected Health Information (ePHI).). Individually identifiable health information (IIHI) that is transmitted by electronic media; maintained in electronic media, such as magnetic tape, disc, optical file; or transmitted or maintained in any other form or medium.

6. Revision History
   1.0 – 09/13/2018