Gaston County HIPAA Manual

Includes Gaston County IT Manual

Action	Date
Reviewed and Revised	**December 2012**

Gaston County HIPAA Policy Manual has be updated and combined with the Gaston County IT Manual.

Privacy Policy Development & Approval Process

Purpose:

The purpose of this policy is to establish the need and acknowledge the intent to develop and implement specific policies to protect the privacy of individually identifiable health information.

I. Introduction

Gaston County is a hybrid entity and also has three covered departments that are designated covered health care components: Community Development and Technology, Department of Social Services and Health Department. The only covered component in Community Development and Technology is the Information Technology Division. Also, the Department of Social Services only has one section which is the Adult Services that is a covered component. All sections at the Health Department are designated as covered components with the exception of Environmental Health.

Employees of Adult Services at the Department of Social Services, Gaston Emergency Medical Services, Human Resources, Public Health, and Sheriff/Jail Departments shall comply with this policy. In addition to these departments which are covered health care components, other departments such as the Attorney's Office, Finance, and Information Technology Division of Community Development and Technology have access to individually identifiable health information and will comply with this policy.

In addition, all entities of Gaston County Organized Health Care Agreements (OHCA) must comply with all policies and procedures developed and implemented by the Gaston County Health Insurance Portability and Accountability Act (HIPAA) Compliance Committee. These entities are responsible for assuring compliance and providing training and documentation relating to these policies and procedures within their entity.

The health information created and maintained by Gaston County must be protected from misuse and unauthorized disclosure. While the HIPAA Privacy Rule was the initial incentive to develop a privacy manual, it is apparent that all health information created and maintained by Gaston County should be protected. Therefore, Gaston County is establishing its requirements for protecting the health information of its clients in Gaston County Privacy Policy and Procedure Manual to reflect all privacy rules.

The following describes the process that will be used by Gaston County in the development and approval process for Gaston County privacy policies. This process reflects state and federal laws, county rules and regulations, and current business practices.

II. Privacy Policy/Procedure Development Process

The process for policy/procedure development, approval, and review for Gaston County shall be as follows:

- The designated Compliance and Privacy Official for Gaston County, a representative of each of its health care components, County Attorney, and Assistant County Manager, will become part of Gaston County HIPAA Compliance Committee. Members of this committee will be asked to serve as members of a team to draft and review Privacy Policies and Procedures required for compliance with the Health Insurance Privacy and Portability Act (HIPAA) of 1996.

- Original HIPAA policies and procedures will go to the Gaston County Board of Commissioners for initial approval of future authority given to the Privacy Official to approve revisions and/or additions in order to maintain HIPAA compliance.

- The Privacy Official will serve as lead person for the Gaston County HIPAA Compliance Committee.

- A draft policy and procedure will be developed within a policy category based on the HIPAA requirements and reviewed against existing policies and procedures within the hybrid entity of its designated health care components.

- A designated individual in each department that is designated as a health care component of Gaston County as well as entities of a Gaston County Organized Health Care Agreement will be responsible for submitting approved policies and procedures to the Privacy Official for Gaston County. Each of these departments must document their procedure for approving policies and procedures by completing a Privacy Policy/Procedure Development & Approval Process form.

- The Gaston County Privacy Official will incorporate any suggested changes and discuss them with the designated individual for each department. Revisions may also be discussed by members of the committee if the topic would be beneficial to other members.

- The designated employee in each covered department should submit individual policy/procedures to the Gaston County Privacy Official for review. If no revisions are necessary, members of the committee will review each policy prior to forwarding to the County Manager for final approval.

- After the County Manager reviews and approves policies/procedures, final drafts will be sent to the County Attorney for review from a legal perspective to ensure compliance with HIPAA requirements and to review the findings based on preemptive legal analysis. Attorney approval must be received before the policy is final.

III. Privacy Policy/Procedure Approval Process

Some policies/procedures will apply to all Gaston County departments who have access to individually identifiable health information and some will apply only to departments that must comply with all rules and regulations of HIPAA.

The process for Gaston County's final review and approval of the proposed privacy policies and procedures will be as follows:

- In the case of a hybrid entity, some policies and procedures may apply to all departments within the hybrid entity and some will apply only in the covered health care components. The Gaston County HIPAA Compliance Committee will make recommendations on policy and procedure scope based on best practice and cost analysis. The County Manager will make the final scope determinations of which departments must implement these policies and procedures.

- As policies and procedures are approved, the Privacy Official will be responsible for establishing and maintaining a policy and procedure manual and ensuring that all departments designated as health care components of Gaston County as well as entities of a Gaston County Organized Health Care Agreement are notified of the policy and procedure. The Privacy Official will also be responsible for revising the policy and procedure manual as needed following the steps outlined in the Privacy Policy Development Process.

- The Privacy Official is responsible for providing and documenting training to staff on approved policies and procedures.

Policy No: 01-020

Administrative Requirements for the Implementation of HIPAA

Purpose:

To issue instructions to all Gaston County Departments, entities covered by an Organized Health Care Agreement (OHCA) and workforce members regarding Gaston County's obligations relating to the implementation of the Health Insurance Portability and Accountability Act (HIPAA) based upon regulations 45 CFR. Parts 160 and 164.

Policy:

Personnel Designations: Gaston County must designate and document designations of the following:

- **Compliance Officer**: Gaston County must designate an individual responsible for overall compliance with HIPAA, including implementation and on ongoing compliance with all Administrative Simplification issues.

- **Privacy Officer:** Gaston County must designate an individual to serve as the Privacy Officer for the entire county. This individual is responsible for the development and implementation of county-wide policies and procedures relating to the safeguarding of Protected Health Information (PHI). Also responsible for supervising duties and responsibilities of subsidiary privacy officers when related to HIPAA.

  Subsidiary Privacy Officers will be appointed for departments within Gaston County that are designated as covered health care components of the county. Entities with an Organized Health Care Agreement with Gaston County will assign a subsidiary privacy officer or contact person for each site. It is the responsibility of the Subsidiary Privacy Officer to assure adequate training within their entity.

  The above individuals will receive directions from the County Privacy Official, serve on the Gaston County HIPAA Compliance Committee, and be responsible for receiving complaints relating to PHI and for providing information about privacy practices.

Training Requirements: The county departments designated as covered healthcare components, and entities of Gaston County Organized Health Care Agreements must document the following training actions:

- On or before the effective date of the HIPAA privacy regulations (04-14-03), all Gaston County employees and other workforce members must receive training on applicable policies and procedures relating to PHI as necessary and appropriate for such persons to carry out their functions.

- Each new workforce member shall receive training as described above within a reasonable time after joining the workforce.

- Each workforce member, whose functions are impacted by a material change in the policies and procedures relating to PHI, or by a change in position or job description, must receive the training as described above within a reasonable time after the change becomes effective.

Safeguards: Each Gaston County department designated as a health care component and entities of a Gaston County Organized Health Care Agreement must have in place appropriate administrative, technical, and physical safeguards to reasonably safeguard PHI from intentional or unintentional, unauthorized use or disclosure.

Complaint Process: Each Gaston County department designated as a covered health care component and entities of a Gaston County Organized Health Care Agreement must have in place a process for individuals to make complaints about the entity's HIPAA policies and procedures and/or the entity's compliance with those policies and procedures. Staff must document all complaints received including the disposition of each complaint. Documentation on all complaints must be forwarded to the Gaston County Privacy Official. (See Complaint/Grievance Process for Alleged Violations of Rights Relating to PHI).

Sanctions: Each Gaston County department designated as a covered health care component and entities of a Gaston County Organized Health Care Agreement must have in place procedures to document sanctions against workforce members who fail to comply with HIPAA policies and procedures. Sanctions must correspond with the Gaston County Personnel Policies. (Note - there are exceptions for disclosures made by workforce members who qualify as whistle blowers or certain crime victims).

Mitigation Efforts Required: Each Gaston County department designated as a covered health care component and entities of a Gaston County Organized Health Care Agreement must mitigate, to the extent practicable, any harmful effects of unauthorized uses or disclosures of PHI by workforce members of the covered department or any of its business associates.

Intimidating of Retaliatory Acts and Waiver of Rights Prohibited:
Prohibition on Intimidating or Retaliatory Acts: No member of Gaston County or entities of a Gaston County Organized Health Care Agreement shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise of his/her rights or participation in any process relating to HIPAA compliance. This includes filing a complaint with the Secretary of the US Department of Health and Human Services, participating in a

HIPAA related investigation, compliance review or hearing, or engaging in reasonable opposition to any act or practice that the person in good faith believes to be unlawful under HIPAA regulations as long as the action does not involve disclosure of PHI in violation of the regulations.

- **Prohibition on Waiver of Rights**: No member of the Gaston County or entities of a Gaston County Organized Health Care Agreement workforce shall require individuals to waive any of their rights under HIPAA as a condition of treatment, payment, enrollment in a health plan or eligibility for benefits.

Policies and Procedures: Gaston County, departments designated as covered health care components, and entities of a Gaston County Organized Health Care Agreement must document the following actions relating to its policies and procedures.

- **Required Policies and Procedures:** Gaston County as well as departments designated as covered health care components and entities of a Gaston County Organized Health Care Agreement shall review, revise, and implement policies and procedures to assure appropriate safeguarding of PHI in its operations. Each covered health care component of Gaston County as well as entities of an Organized Health Care Agreement may develop policies and procedures specific to their entity, however all policies and procedures must be in compliance with Gaston County's Policies and Procedures and must be submitted to the Gaston County Privacy Officer. Each covered health care components as well as entities of a Gaston County Organized Health Care Agreement are responsible for implementation, training, and compliance documentation relating to such policies and procedures.

- **Changes to Policies and Procedures**: Gaston County as well as departments designated as covered health care components and entities of a Gaston County Organized Health Care Agreement must change its policies and procedures as necessary and appropriate to conform to changes in law or regulation. Departments may also make changes to policies and procedures at other times as long as the policies and procedures are still in compliance with applicable law and are approved by the Gaston County Privacy Official. When necessary, Gaston County must make corrective changes in the Privacy Notice. Gaston County departments designated as covered health care components or entities of a Gaston County Organized Health Care Agreement may not implement a change in HIPAA policy or procedure prior to approval by the Gaston County Privacy Officer.

Documentation Requirements: Gaston County, departments designated as covered health care components, and entities of a Gaston County Organized Health Care Agreement must maintain the required policies and procedures in written or electronic form and must maintain written or electronic copies of all communications, actions, activities or designations as are required to be documented under the HIPAA regulations for a period of at least six (6) years from the later of the date of creation or the last effective date or a longer period if required under state or other federal law. Copies of all approved policies and procedures developed by each covered health

care component as well as entities of a Gaston County Organized Health Care Agreement must be submitted to the Gaston County Privacy Official to be retained permanently.

Management and Protection of Protected Health Information

Purpose:

To issue instructions to workforce members in Gaston County departments designated as covered health care components as well as entities of Gaston County Organized Health Care Agreements regarding the management and protection of individuals' health information.

Policy:

For details on specific requirements, refer to the appropriate policies in this manual as indicated in italics.

Generally, PHI shall not be used or disclosed except as permitted or required by law.

Designated Record Set: Each covered health care component and entities of Organized Health Care Agreements with Gaston County must establish and document a designated record set. The designated record set must include any medical and billing records relating to individuals maintained by or for a health care provider, the enrollment, payment, claims adjudication, and case or medical management systems maintained by or for a health plan, or , used, in whole or in part, by or for a covered entity to make decisions about individuals.

Notice of Privacy Practices Required: Individuals served must be given a Notice of Privacy Practice outlining the uses and disclosures of PHI that may be made, and notifying them of their rights and our legal duties with respect to PHI (*Notice of Privacy Practices*)

Permitted and Required Uses and Disclosures: PHI may or shall be disclosed as follows:
To the individual (*Individuals' Rights Related to PHI*)

- To carry out Treatment, Payment, and Operations (TPO) activities, within specified limits (*Use or Disclosure of PHI for TPO Purposes*).
- Pursuant to and in compliance with a current and valid Authorization (*Authorization for Use or Disclosure of PHI*).
- In keeping with a Business Associate (BA) arrangement (*Business Associate Agreements*).
- As otherwise provided for in the HIPAA privacy regulations (*Public Responsibility Uses and Disclosures of PHI*).

Minimum Necessary: Generally, when using or disclosing PHI, or when requesting PHI from another entity, reasonable efforts must be made to limit the PHI used or disclosed to the minimum necessary to accomplish the purpose of the use/disclosure (*Minimum Necessary Standard*).

Personal Representatives: A person acting in the role of personal representative must be treated as the individual regarding access to relevant PHI unless:

- The individual is an un-emancipated minor, but is authorized to give lawful consent, or may obtain the health care without consent of the personal representative, and minor has not requested that the person be treated as a personal representative, or the personal representative has assented to agreement of confidentiality between the provider and the minor

- There is a reasonable basis to believe that the individual has been or may be subjected to domestic violence, abuse, or neglect by the personal representative or that treating that person as a personal representative could endanger the individual, and, in the exercise of professional judgment, it is determined not to be in the best interest of the individual to treat that person as a personal representative.

Agreed Upon Restrictions: An individual has a right to request a restriction on any uses or disclosures of his/her PHI, though a covered entity is not required to agree to the requested restriction, and cannot agree to a restriction relating to disclosures required under law, i.e. disclosures to the U.S. Secretary of Health and Human Services for HIPAA enforcement purposes. (*Individuals' Rights Related to PHI*).

Confidential Communications: An individual has a right to request to receive communications of PHI by alternative means or at alternative locations, and reasonable requests must be accommodated (*Individuals' Rights Relating to PHI*).

Accounting for Disclosures: An individual has a right to an accounting of disclosure of his/her PHI for up to a six (6) year period. (*Accounting for Disclosures of PHI*).

Amendment to PHI: An individual has the right to request amendment to PHI or other information in the designated record set. (*Right to Request Amendment of PHI*)

De-identified PHI: Health information may be considered not to be individually identifiable in the following circumstances:

- A person with appropriate knowledge and experience with generally acceptable statistical and scientific principles and methods determines that the risk is very small that the information could be used, alone or with other reasonably available information, to identify the individual who is the subject of the information; or

- The following identifiers of the individual (and relatives, employers or household members) is removed; names; information relating to the individual's geographic subdivision if it contains fewer than 20,000 people; elements of dates (except year) directly related to the individual; and all ages and elements of dates that indicate age for individuals over 89, unless aggregated into a single category of age 90 and older; telephone numbers; fax numbers; email addresses; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate or license numbers; vehicle identifiers and serial numbers, including license plate numbers, device identifiers and serial numbers; Web Universal Resource Locators (URLs); Internet Protocol (IP) address numbers, biometric identifiers, full face photographic images; and, any other unique identifying number, characteristic or code.

Complaint Process: Each Gaston County department designated as a covered health care component and entities of Gaston County Organized Health Care Agreements must have in place a process for individuals to make complaints about the entity's HIPAA policies and procedures and/or the entity's compliance with those policies and procedures. (*Complaint/Grievance Process for Alleged Violations of Rights Related to PHI*)

Documentation: Each Gaston County department designated as a covered health care component and entities of Gaston County Organized Health Care Agreements must maintain written or electronic copies of all policies and procedures, communications, actions, activities or designations as are required to be documented under this manual for a period of at least six (6) years from the later of the date of creation or the last effective date or such longer period that may be required under state or other federal law.

Policy No: 01-031

Facsimile Transmission of Patient Health Information

Policy Statement:

Transmitting patient information via facsimile is only permitted when sending records by mail would result in a delay which could adversely affect the patient's care. Transmitting patient information via facsimile is also permitted in order to expedite payment for services rendered only when prior follow up is completed and information is requested by an identifiable individual at the third party carrier.

Gaston County's policy for release of information shall apply to the request for release of patient information and proper authorization from the patient obtained when required.

Procedure:

A. Location of fax machines

1. All facsimile machines used for sending and receiving information that include personally identifiable heath information will be located in secured areas. Only authorized personnel should have access to these designated areas.

B. Use of cover page

1. Any patient information being transmitted via facsimile will include a Gaston County facsimile cover page which will include the following:

a) Date and time of transmission
b) Gaston County Health Department's name, address, telephone, and appropriate facsimile numbers.
c) Authorized receiver's name
d) Number of pages transmitted
e) The following confidentiality statement:
The documents accompanying this transmission contain confidential health information that is legally privileged. This information is intended only for the use of the individual or entity named above. The authorized recipient of this information is prohibited from disclosing this information to any other party unless required to do so by law or regulation. The recipient accepts responsibility for properly safeguarding the confidentiality of this information in compliance with all applicable State and Federal Regulations. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited. If you have received this information in error, please notify the sender immediately and arrange for the return or destruction of these documents.

C. Recipient confirmation

1. All facsimile machines at the health department will be modified to print a confirmation receipt after completion of each facsimile. The confirmation receipt should be reviewed to verify transmission sent to appropriate number. Staff processing facsimile will attach cover sheets to information sent and file in the financial and/or medical record. The only exclusion from this policy is when a medical record is sent by facsimile: instead of copying the record, note on the cover sheet the information transmitted.

D. Misdirected transmissions

1. Upon notification of a misdirected transmission staff should inform the receiver to properly destroy the document received. The sender should then re-transmit the information verifying information received by the appropriate recipient.

2. A Facsimile Error Report should be completed immediately and submitted to the Privacy Officer as well as a copy to the employee's immediate supervisor.

E. Receiving patient information via facsimile

1. Staff should monitor the facsimile machines upon notification of facsimile being transmitted by and/or upon ringing of facsimile machine and remove documents, forward information received to the appropriate staff

2. Staff receiving information via facsimile should verify and notify the sender immediately if the transmission is incorrect, incomplete, or information received in error.

3. Patient health information received via facsimile should be placed in the designated area of the patient's medical record or financial record.

Policy No: 01-040

Minimum Necessary Standard

Purpose:

To issue instructions to workforce members in the Gaston County departments designated as health care components and entities of a Gaston County Organized Health Care Agreement regarding obligations relating to the HIPAA requirement to use, disclose or request only the minimum amount of protected health information (PHI) necessary to accomplish the intended purpose of the use, disclosure or request.

Policy:

Gaston County will make reasonable efforts to ensure that the minimum necessary protected health information (PHI) is disclosed, used, or requested. Exceptions to the minimum necessary requirement include:

- disclosures to the individual who is the subject of the information
- disclosures made pursuant to an authorization
- disclosures to or requests by healthcare providers for treatment purposes
- disclosures required for compliance with the standardized HIPAA transactions
- disclosures made to HHS pursuant to a privacy investigation
- disclosures otherwise required by the HIPAA regulations or other law

Procedure:

The following procedures will be implemented to ensure that this policy is enforced effectively across all parts of Gaston County including Organized Health Care Arrangements. In addition to these procedures, Gaston County departments designated as healthcare components and entities of Gaston County Organized Health Care Agreements will implement additional procedures to assure compliance with HIPAA.

- Each user of a PHI System will be identified and the category or categories of PHI to which access is needed and any conditions appropriate to such access will be established. Final responsibility will be with the Information and Technology Department and the Gaston County HIPAA Privacy Official.

- Reasonable efforts will be made to limit each PHI user's access to only the PHI that is needed to carry out his/her duties. These efforts will include internal staff to staff use and disclosure of PHI.

- For situations where PHI use, disclosure, or request for information occurs on a routine and recurring basis protocols will be developed to assure that the PHI disclosed will be limited to the amount of information reasonably necessary to achieve the purpose of the use, disclosure or request. Access codes and staff assignments should be reviewed by the Gaston County Privacy Official to ensure that the access to PHI meets the Minimum Necessary standard.

- For non-routine disclosures (other than pursuant to an authorization, ex. to accrediting bodies, insurance carriers, research entities, funeral homes, etc.) criteria will be adopted for review by the Gaston County HIPAA Compliance Committee to limit the disclosure to that which is reasonably necessary to accomplish the purpose for which disclosure is sought. A request may be presumed to be limited to the minimum necessary if the request is from another CE, or is from a public official or a professional for the purpose of providing services to the CE, and the request states that the PHI requested is the minimum.

- Use/disclosure of the entire medical record should not be made unless use/disclosure of the entire record is specifically justified as the amount reasonably necessary to accomplish the purpose of the use or disclosure.

- All workforce members working in Gaston County departments designated as health care components and entities of Gaston County Organized Health Care Agreements must be trained on a regular basis regarding this policy.

- Questions regarding Minimum Necessary policies and procedures should be directed to the Gaston County Privacy Official.

Business Associate Agreement

Purpose:

To issue instructions to all workforce members in Gaston County and entities of Gaston County Organized Health Care Agreements regarding the necessity for and the required content of agreements with business associates relating to the business associate's receipt and use of protected health information (PHI) from or on behalf of Gaston County departments designated as covered health care components and entities of Gaston County Organized Health Care Agreements.

Policy:

Gaston County departments designated as health care components and entities of Gaston County Organized Health Care Agreements may disclose PHI to a BA, or allow a BA to create or receive PHI on the entity's behalf, if the entity first obtains adequate assurance that the BA will appropriately safeguard the PHI. This requirement does not apply with respect to disclosures made to a provider concerning the individual's treatment, or uses and disclosures made to another governmental agency for purposes of public benefit eligibility for enrollment determinations where such agency is authorized by law to make these determinations.

Entities must document these assurances through a written agreement or as follows. If the BA is another governmental entity, the entity may comply with this requirement by executing a Memorandum of Understanding or like document covering the required terms or, by relying on other law that imposes upon the BA the requirements specified herein. If the BA is required by law to perform a function, activity or service on behalf of the entity, the entity may disclose PHI to the extent necessary to comply with that mandate as long as the entity documents an attempt to obtain the required assurances and the reasons that such assurances could not be obtained.

Content Requirements: The agreement between the entity and the BA must meet the following requirements, as applicable:

- Establish permitted and required uses or disclosures of PHI that are consistent with those authorized for the entity, except that the agreement may permit the BA to use or disclose PHI for its own management and administration if such use or disclosure is required by law or the BA obtains reasonable assurance that the confidentiality of the PHI will be maintained.

- Provided that the BA will:
    - Not use or disclose the PHI except as authorized under the agreement or required by law
    - Use safeguards to prevent unauthorized use or disclosure
    - Report unauthorized uses or disclosures to the entity
    - Pass on the same obligations elating to protection of PHI to any subcontractors or agents
    - Make PHI available for access by the individual or his/her personal representative in accordance with relevant law and policy
    - Make information available for the provision of an accounting of uses and disclosures in accordance with relevant law and policy
    - Make its internal practices, books and records relating to its receipt or creation of PHI available to the Office of the U.S. Secretary of Health and Human Services for purposes of determining the entity's compliance with HIPAA regulations.
    - If feasible, return or destroy all PHI upon termination of contract, if any PHI is retained, continue to extend the full protections specified herein as long as the PHI is maintained.
    - Authorize termination of the agreement by the entity upon a material breach by the BA; this element of the agreement may be omitted if the BA is another governmental entity and the termination would be inconsistent with the statutory obligations of the entity or the BA.

Oversight Responsibilities: If the entity knows of a pattern or practice of the BA that amounts to a material violation of the agreement, the entity must attempt to cure the breach or end the violation, and if such attempt is unsuccessful, terminate the agreement, if feasible, and, if not, report the problem to the Office of U.S. Secretary of Health and Human Services.

Policy No: 01-060

Organized Health Care Agreements

Purpose:

To issue instructions to all workforce members in Gaston County and entities of Gaston County Organized Health Care Agreements regarding the necessity for and the required content of entities of a Gaston County Organized Health Care Agreement (OHCA) relating to the OHCA's use of protected health information (PHI) from or on behalf of Gaston County departments designated as covered health care components for the purpose of treatment, payment, and healthcare operations (See listing of current OHCA to identify entities in which have established OHCA with Gaston County)

Policy:

Gaston County departments designated as health care components may disclose/share PHI with an entity of a Gaston County Organized Health Care Agreement. Prior to this interaction, adequate assurance that the Organized Health Care Agreement entity will appropriately safeguard all PHI. This requirement does not apply with respect to disclosures made to a provider concerning the individual's treatment, or uses and disclosures made to another governmental agency for purposes of public benefit eligibility for enrollment determinations where such agency is authorized by law to make these determinations.

There must be a written agreement signed and approved by both Gaston County and the entity seeking an Organized Health Care entity which the Organized Health Care entity agrees to assure compliance with all Gaston County HIPAA Policies and Procedures. This agreement will state the requirements of the OHCA and how Gaston County will follow up regarding HIPAA. All OHCA must first be submitted to the Gaston County Privacy Official to determine necessity and approval, once approved by the Gaston County Privacy Official the Agreement must then be submitted to the County Attorney in order to review from a legal perspective. Once approved by the County Attorney the Agreement must receive final approval from the County Manager prior to implementation.

Content Requirements: The agreement between Gaston County and the entity seeking an OHCA must meet the following requirements, as applicable:

- Establish the basis for determining the need for an OHCA

- Provided that the OHCA will:
    - Not use or disclose the PHI except as authorized under the agreement or required by law

- Use safeguards to prevent unauthorized use or disclosure
- Appoint a Subsidiary Privacy Official to be designated as the contact person for receiving complaints relating to PHI and for providing information about privacy practices.
- Report unauthorized uses or disclosures to Gaston County Privacy Official
- Pass on the same obligations relating to protection of PHI to any Business Associates, subcontractors, or agents
- Comply with Gaston County Policies and Procedures including those of a Gaston County covered health care component in which the OHCA has been implemented.
- Assure proper documentation and training relating to HIPAA and submit such documentation to the Gaston County Privacy Official.
- Make PHI available for access by the individual or his/her personal representative in accordance with relevant law and policy
- Make information available for the provision of an accounting of uses and disclosures in accordance with relevant law and policy
- Make its internal practices, books and records relating to its receipt or creation of PHI available to the Gaston County Privacy Officer or designee for review and auditing compliance as well as the Office of the U.S. Secretary of Health and Human Services for purposes of determining the entity's compliance with HIPAA regulations.
- Gaston County retains the right to terminate the OHCA in the event of violation to policies and procedures or a breach of confidentiality occurs.

Oversight Responsibilities: If entity knows of a pattern or practice of the entity of a Gaston County OHCA that amounts to a material violation of the agreement, the entity must attempt to cure the breach or end the violation, and if such attempt is unsuccessful, terminate the agreement, if feasible, and, if not, report the problem to the Office of U.S. Secretary of Health and Human Services.

Provision of Privacy Notice

Purpose:

To issue instructions to all employees of Gaston County and entities of Gaston County Organized Health Care Agreements regarding the provision of a notice of privacy practices to all patients and clients.

Policy:

Pursuant to 45 CFR 164.520, an individual has a right to adequate notice of the uses and disclosures of his/her PHI that may be made by or on behalf of a Covered Entity (CE), and of the individual's rights and the CE's legal duties with respect to his/her PHI.

Content Requirements:

The notice of privacy practices must be written in plain language (both in English and Spanish) and must contain the following elements:

1. The following statement in a header or otherwise prominently displayed: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY".

   - A description, including at least one example, of the types of uses and disclosures that the CE is permitted to make for purposes of treatment, payment and health care operations, with sufficient detail to place an individual on notice of the uses and disclosures permitted or required.

   - A description of each of the other purposes for which the CE is permitted or required to use or disclose PHI without an individual's consent or authorization, with sufficient detail to place an individual on notice of the uses and disclosures permitted or required.

   - A statement that other uses or disclosures will be made only with the individual's written authorization, and that the authorization may be revoked in accordance with the policy on authorizations.

   - If providers intend to contact the individual for appointment reminders, treatment alternatives or other health related benefits, a separate statement describing such contacts.

- A statement of the individual's rights with respect to his/her PHI, and a brief description of how the individual may exercise those rights, including: the right to request restrictions on certain uses/disclosures of PHI, and the fact that the CE does not have to agree to such restrictions; the right to receive confidential communications of PHI; the right to inspect and copy PHI: the right to amend PHI; the right to receive an accounting of disclosures of PHI, and: the right to receive a paper copy of the privacy notice (each of the above in accordance with relevant notices)

- A statement of the CE's duties with respect to PHI, including statements: that the CE is required by law to maintain the privacy of PHI and to provide individuals with notice of its legal duties and privacy policies; that the CE is required to abide by the terms of the currently effective privacy notice, and: that the CE reserves the right to change the terms of the notice and make the new notice provisions effective for all PHI maintained, along with a description of how the CE will provide individuals with the revised notice.

- A statement that individuals may complain to the contact person in the department where they receive services, the Gaston County Privacy Official and to the Secretary of the U.S. Department of Health and Human Services about privacy rights violations, including a brief statement about how a complaint may be filed and an assurance that the individual will not be retaliated against for filing a complaint.

- The name, or title, and telephone number of the person or office to contact for further information.

- The effective date of the notice which may not be earlier than the date printed or published.

Revisions to Notice:

Gaston County will promptly revise and distribute the privacy notice whenever there is a material change to the uses or disclosures, the individual's rights, the county's legal duties, or other privacy practices described in the notice. Except when required by law, a material change to any term may not be implemented prior to the effective date of the notice reflection the change.

Gaston County HIPAA Compliance Committee will develop standardized Notice of Privacy Practices for Gaston County.

Provision of Notice:

Gaston County employees and entities of Gaston County Organized Health Care Agreements must provide individuals with the notice, and obtain the individual's written acknowledgment of receipt, or document attempts to obtain such acknowledgment no later than the date of the first service (after the effective date) provided. The receipt of acknowledgment will be maintained in the designated record set. Additionally, the notice in effect (original notice or any subsequent revisions) must be prominently posted and copies must be available for individuals to take at any sites where services are received.

The privacy notice will also be posted on the Gaston County web site and available electronically from the web site.

Documentation Requirements:

Gaston County will retain copies permanently of notices issued for a period of at least six years from the later of the date of creation or the last effective date and each department where services were received will retain documentation of individuals acknowledgment of receipt, or refusal to acknowledge receipt of the privacy notice for a period of at least six years. (Acknowledgment of Privacy Notice and Permission to Share Personal Health Information).

Policy No: 01-080

Individuals' Rights Related to Protected Health Information

Purpose:

To issue instructions to member of the workforce for Gaston County and entities of Gaston County Organized Health Care Agreements regarding Gaston County's obligations relating to patient/client rights relating to access to and use/disclosure of their protected health information (PHI).

Policy:

Right to Access PHI: Individuals have a right to access and obtain a copy of their PHI and any information in their designated records set except as set forth below:

- **Denial of Access without a right of review:** Access may be denied where;
  - Information was compiled in anticipation of ligation,
  - Information was collected in the course of research that includes treatment of the individual and the individual agreed to a suspension of the right of access during the research period.
  - Access can be denied in accordance with the Clinical Laboratory Improvement Amendments of 1988 (CLIA) or the Privacy Act (5 USA 552a).

- **Denial of Access with a right of review:** Access may be denied, though denial is subject to review where:
  - Access is determined by a licensed professional to be likely to endanger life or physical safety of the individual or another person; and such determination is documented.
  - Access is requested by a Personal Representative and a licensed professional determines that such access is reasonably likely to cause substantial harm to the individual or another person.

- **Right to Review:** If the basis for denial of access gives a right of review, the individual has a right to have the denial reviewed by another licensed professional who did not participate in the original denial decision. Such review must be completed within a reasonable period of time, and the department, facility or program must promptly: (1) provide the individual with notice of the reviewer's decision, and (2) comply with the determination to provide or deny access.

- **Timely Review:** The entity must act on a request for access no later than thirty (30) days after receipt unless the time period is extended as permitted below:
    - If the information to be accessed is not maintained or accessible on site, the entity must act on the request no later than sixty (60) days after receipt.
    - If the entity is unable to act on the request for access within the applicable 30 or 60 day period, it may extend the time for response by no more than thirty (30) days, provided that, within the original allotted time period, the entity gives the individual written notice of the reasons for the delay and the date by which a responsive action will be taken.

- **Provision of Access:** The entity must provide the individual with access to the information in the form or format requested if it is readily producible in such form or format, or in a readable hard copy or other form or format as mutually agreed to, whether by arranging for a convenient time and place for inspection and copying or mailing the information at the individual's request.
    - If the information is maintained in more than one place, the information need only be produced once in response to a current request for access.
    - The entity may provide a summary of the information in lieu of providing access, or may provide an explanation of the information to which access is provided if the individual, in advance, agrees.
    - The entity will follow Gaston County's directive when imposing a fee for copying information.

- **Denial of Access:** The entity must provide a timely, written denial of access to the individual, written in plain language, explain the basis for the denial, and any applicable right of review and describe how the individual may complain to the entity (including Name or title of contract, and phone number) or the U.S. Secretary of Health and Human Services.
    - To the extent possible, the individual must be given access to any information requested after excluding the information for which entity has grounds for denying access.
    - If the entity does not maintain the information for which access has been requested, but knows where it is maintained, the entity must inform the individual where to direct the request for access.

- **Documentation:** The entity must document and retain for at least six years from the date of its creation the designated record set subject to access and the names or titles of persons responsible for receiving and processing request for access.

Right to Request Restrictions on Uses/Disclosures of PHI, and to Request Confidential Communications

- **Requests for Restrictions on Uses/Disclosures:** The entity must permit an individual to request that the entity restrict uses and disclosures of PHI made for TPO or disclosures to

personal representatives or others involved in the individual's care, though the entity does not have to agree to the restriction requested.

- If the entity agrees to the requested restriction(s), it must document the agreed upon restriction in writing, and abide by the restriction unless the individual is in need of emergency treatment, the information is needed for the treatment, and the disclosure is to another provider only for purposes of such treatment. The entity must request that the provider agree not to further disclose the PHI.
- The entity cannot agree to restriction that prevents uses or disclosures permitted or required to the individual, or where the use of disclosure does not require the individual's permission.
- The entity may terminate an agreed upon restriction if the individual so agrees, as documented in writing, or the entity informs the individual and the termination is only effective as to PHI created or received after such notice.

- **Request for Confidential Communications:** The record keeping entity must permit individuals to request to receive communications of PHI by alternative means or at alternative locations, and must accommodate all reasonable requests.

Right to Request Amendment of PHI:

- **Requests for Amendment of PHI:** An individual has the right to request the entity amend PHI or other information in the designated record set for as long as the entity maintains the information. The entity must act on the request within sixty (60) days of receipt, or within ninety (90) days if the entity notifies the individual within the first 60 days of the reasons for delay and the date by which action will be taken. The Privacy Official may deny the request if it determines that the record was not created by the entity (unless the individual provides reasonable basis to believe that the originator of the record is no longer available to act on the request); is not part of the designated record set; would not be available for inspection; or is accurate and complete.
- **Accepting the Amendment:** If the Privacy Official accepts the amendment, in whole or in part, it must:
  - Make the amendment by, at minimum, identifying the affected records and appending or otherwise providing a link to the location of the amendment.
  - Timely inform the individual that the amendment is accepted, and obtain his/her identification of an agreement to have the entity notify relevant persons with a need to know.
  - Make reasonable efforts to inform and timely provide the amendment to those persons and others, including business associates, that the entity knows to have the affected PHI and that may have relied, or be foreseen to rely, on that information to the detriment of the individual.
- **Denying the Amendment:** If the entity denies the amendment, in whole or part if must:
  - Provide the individual with a timely denial, written in plain language and including the basis for denial, notice of the individual's right to submit a written statement of disagreement, and instructions on how to file the statement, or to

request that future disclosures of the PHI include copies of the request and the denial, and a description of how the individual may complain about the decision to the entity or to the U.S. Secretary of Health and Human Services.

- Permit the individual to submit a statement of disagreement (but entity may reasonably limit its length);
- Provide a copy of any rebuttal prepared to the individual
- As appropriate, identify the part of the record subject to the disputed amendment and append or otherwise link the request, the denial and any statement of disagreement or rebuttal to the record;
- For future disclosures of the record, include any statement of disagreement or, in response to the individual's request, the amendment request and the denial (or an accurate summary of either of the foregoing). If standard transaction format does not permit the appending of the additional information, it must be transmitted separately to the recipient of the standard transaction.

If the entity is informed by another covered entity about an amendment to the record, the entity must amend the information in its record by, at a minimum, identifying the affected records and appending or otherwise providing a link to the location of the amendment.

The entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments.

Right to an Accounting of Disclosures: An individual has a right to receive an accounting of disclosures of his/her PHI in accordance with the policy "Accounting for Disclosure of Protected Health Information".

Policy No: 01-090

Complaint/Grievance Process for Alleged Violations of Rights Relating to PHI

Purpose:

To issue instructions to all workforce members in Gaston County and entities of Gaston County Organized Health Care Agreements regarding procedures for acceptance, documentation and response to patients/clients complaints about alleged violations of their rights relating to protected health information (PHI)

Policy:

HIPAA grants individuals specific rights relating to their health information, many of which overlap with patient/client rights mandated by state law. Specifically, in addition to privacy rights related to their PHI, individuals are granted the right to access their designated record set, to request that communications related to PHI be confidential, to request restrictions on uses or disclosures of their PHI, to request amendment of their designated record set, and to receive an accounting of disclosure of their PHI. (For details see individuals' Rights Related to Protected Health Information; Accounting for Disclosures of PHI; HIPAA also mandates that a process be in place for individuals to complain about an entity's privacy related policies and procedures and/or the entity's compliance with those policies and procedures.

Employees assigned as subsidiary privacy officers in each Gaston County department designated as a covered health care component and entities of a Gaston County Organized Health Care Agreement will be responsible for receiving complaints/grievances relating to individuals' privacy rights, and rights to access their designated record set, to request restrictions on the use or disclosure of their PHI, to request confidential communications of health related information, to request amendment of their designated record set, or to request an accounting of disclosures made of the PHI.

When a HIPAA related complaint/grievance is communicated to any workforce member, that individual shall immediately notify the subsidiary privacy official, and shall inform the grievant of the name and contact information for the Gaston County Privacy Official. If the subsidiary privacy official is a subject of the complaint/grievance, the grievant shall be referred directly to the Gaston County Privacy Official, who will act as representative of the department. The privacy official shall also give the grievant information about his/her right to file a complaint with the US Secretary of Health and Human Services.

The Privacy official shall investigate the circumstances of the alleged HIPAA rights violation and if appropriate, shall take all reasonable steps to mitigate the effects of any violation. In investigating and acting on the complaint/grievance, the subsidiary privacy official may consult with the Gaston County Privacy Official. Subsidiary privacy officials shall communicate the results of the investigation and resolution of the complaint/grievance to the grievant and to the Gaston County Privacy Official. If the grievant is dissatisfied with the result, he/she shall be informed of the right to file the complaint/grievance with the Gaston County Privacy Official and shall be given assistance in doing so, if requested.

The Gaston County Privacy Official shall consult with the HIPAA Compliance Committee in investigating, reviewing and acting upon complaints/grievances. The Gaston County Privacy Official shall communicate the results of the investigation and resolution of the complaint/grievance to the grievant within thirty (30) working days unless a greater amount of time is necessary to complete the investigation. If such greater time is necessary, the Gaston County Privacy Official shall, within thirty days notify the grievant of the delay and inform the grievant of the expected time frame for completion of the investigation.

If the results of the investigation indicate that a workforce member made an unauthorized use or disclosure of PHI, or otherwise violated HIPAA Policies and Procedures, the Gaston County Privacy Official will report such finding to the workforce member's supervisor.

The Gaston County Privacy Official shall document all HIPAA related complaints/grievances, their resolution, and any actions resulting from the investigation. This documentation must be maintained for a minimum period of six (6) years from the date of final resolution. Complete copies of this documentation shall be submitted to the Gaston County HIPAA Compliance Committee quarterly for review. The HIPAA Compliance Committee shall review the logs to determine if any pattern or systematic problems exist and if so, shall take necessary steps to address the problem.

There shall be no retaliation against any individual served, workforce member, or privacy official for having filed or assisted in the filing of a complaint/grievance, or for investigating or acting on a complaint/grievance. Any workforce member who becomes aware of any such retaliatory action shall immediately complete an incident report and notify the Gaston County Privacy Official.

Policy No: 01-100

Use or Disclosure of Protected Health Information for Treatment, Payment or Health Care Operations

Purpose:

To issue instructions to all Gaston County departments, entities of an Organized Health Care Organization and workforce members regarding the use and disclosure of protected health (PHI) and necessary documentation of authority for such use or disclosure for purposes of treatment, payment and health care operations (TPO).

Policy:

Generally, in compliance with HIPAA regulations (45 CFR part 160 and 164) and North Carolina laws, an individual's authorization (or authorization from a personal representative) must be obtained prior to using or disclosing protected health information to carry out treatment, payment or health care operations, except as specified below:

- PHI may be shared on a need to know basis with personnel within the Gaston County departments designated as covered heath care components and entities of an Organized Health Care Organization for activities related to treatment, payment, or health care operations.

- PHI may be used or disclosed to other health care providers for treatment, payment, and health care operations without authorization if an attempt has been made and documented to obtain the individual's consent to the disclosure.

- Limited PHI (medication information, summary of diagnoses and prognosis and list of services provided) may be disclosed to family members, other relatives or friends involved in the individual's care, or payment for that care, if the individual is notified and does not object to the disclosure.

- Limited PHI may be disclosed that identifies the individual as a patient in one of the Gaston County departments designated s a health care component or entities of an Organized Health Care Agreement and to disclose his/her location within the entity, and to report a general description of his/her condition to individuals who inquire about him/her by name, if the individual is notified and does not object to the disclosure.

- In emergency treatment situations, necessary information for treatment may be disclosed if an attempt is made and documented to obtain consent to the disclosure as soon as reasonably practicable after the delivery of treatment.

Public Responsibility Uses and Disclosures of PHI

Purpose:

To issue instructions to all individuals in the workforce of Gaston County and entities of Gaston County Organized Health Care Agreements regarding uses and disclosures of protected health information (PHI) permitted or required in context of the county's public responsibilities.

Policy:

State and federal law permit and/or require certain uses and disclosures of PHI for various purposes related to public responsibility. Such uses and disclosures may be made without the agreement or authorization of the individual. The following uses and disclosures fall within this category:

Health Oversight Activities:

PHI may be used or disclosed for activities related to oversight of the health care system, government health benefits programs, and entities subject to government regulation, as authorized by law, including activities such as audits, civil and criminal investigations and proceedings, inspections, and licensure and certification actions. Specifically excluded from the category are investigations of an individual that are not related to receipt of health care, or the qualification for, receipt of, or claim for public benefits.

Public Health Activities:

PHI may be used or disclosed to:

- A public health authority authorized by law to collect or receive information for the purpose of preventing or controlling disease, injury or disability, reporting vital events, conducting public health surveillance, investigations or interventions:
- A public health or other government authority authorized by law to receive reports of child abuse or neglect;
- A person subject to the jurisdiction of the Food and Drug Administration (FDA) regarding his/her responsibility for quality, safety or effectiveness of an FDA regulated product or activity, to report adverse events, product defects or problems, track products, enable recalls, repairs or replacements, or conduct post-marketing surveillance;
- PHI of potential organ/tissue donors may be disclosed to the designated organ procurement organization and tissue and eye banks.

Required by Law:

PHI may be used or disclosed to the extent such use or disclosure complies with and is limited to the requirements of such law:

- Abuse and Neglect: Except for reports of child abuse or neglect, PHI about an individual believed to be a victim of abuse, neglect, or domestic violence may be disclosed to a governmental authority authorized to receive such reports if the individual agrees or the reporting entity believes in the exercise of professional judgment, that the disclosure is necessary to prevent serious physical harm. If the individual lacks the capacity to agree, disclosure may be made if not intended for use against the individual and delaying disclosure would materially hinder law enforcement activity. The individual whose PHI has been released must be promptly informed that the report was made unless doing so would place the individual at risk of serious harm.

- Judicial Proceedings. PHI may be disclosed in response to a court order. Information may not be disclosed pursuant to a subpoena without proper patient authorizations. All subpoenas and court orders should be referred to the County Attorney for review and guidance prior to acting upon such subpoena or court order.

- Law Enforcement: PHI may be disclosed for the following law enforcement purposes and under these specified conditions:
    - Pursuant to court order or as otherwise required by law, i.e. laws requiring the reporting of certain types of wounds or injuries; or commission of a felony (but not reporting exceptions for certain privileged communications.
- Decedent's PHI may be disclosed to alert law enforcement of the death of an individual if the entity suspects that the death resulted from criminal conduct.

- Limited PHI (medication history, physical health status and history, summary of course of treatment, summary of treatment needs and discharge summary) of inmates of a correctional facility may be disclosed to the facility as requested in order to provide care for the individual or ensure safety of the individual or others, but only if the individual is told of the request to records and does not object to the disclosure.

- Compliance/Enforcement of privacy regulations. PHI must be disclosed as requested, to the Secretary of Health and Human Services related to compliance and enforcement efforts.

Serious Threats to Health or Safety:

Consistent with applicable law and ethical standards, PHI may be used or disclosed if the entity believes in good faith that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to a person or the public and disclosure is to someone reasonably able to prevent or lessen the threat, or the disclosure is to law enforcement authorities to identify or apprehend an individual who has admitted to violent criminal activity that likely caused serious harm to the victim or who appears to have escaped from lawful custody. Disclosures of admitted participation in a violent crime are limited to the individual's statement of participation and the following PHI: name, address, date and place of birth, social security number, blood type of injury, date and time of treatment, date and time of death, if applicable, and a description of distinguishing physical characteristics. Disclosures of admitted participation in a violent crime are not permitted when the information is learned in the course of treatment entered into by the individual to affect his/her propensity to commit the subject crime, or through counseling, or therapy or a request to initiate the same.

Research: See Uses/Disclosures of PHI for Research Purposes

Decedents:

PHI may be disclosed to coroners or medical examiners as necessary for carrying out their duties and to the designated organ procurement organization, and tissue and eye banks.

Specialized Government Functions:

- National Security and Intelligence. PHI may be disclosed to authorize federal officials for the conduct of lawful intelligence, counter intelligence, and other activities authorized by the National Security Act.
- Protective services. PHI may be disclosed so authorized federal officials for the provision of protective to the President, foreign heads of state, and others designated by law, and for the conduct of criminal investigations of threats against such persons.
- Public Benefits: PHI relevant to administration of a government program providing public benefits may be disclosed to another governmental program providing public benefits serving the same or similar populations as necessary to coordinate program functions or improve administration and management of program functions.

Workers' Compensation:

PHI may be disclosed as authorized and to the extent necessary to comply with laws relating to workers' compensation and other similar programs.

Documentation:

Documentation of disclosure made hereunder must be retained for a period of at least six years.

Policy No: 01-120

Authorization for Use or Disclosure of Protected Health Information

Purpose:

To issue instructions to all Gaston County departments designated as covered health care components and entities of a Gaston County Organized Health Care Agreements, regarding the use and disclosures of protected health information (PHI), and necessary documentation of authority for each use or disclosure, when use/disclosure is for purposes outside of those permitted by law relating to treatment, payment, or health care operations, or public responsibility

Policy:

In compliance with 45 CFR Part 164 and other laws, all uses and disclosures of PHI beyond those otherwise permitted or required by law require a signed authorization according to the provisions of this rule. An authorization is required for each entity that is to receive PHI.

The provision of treatment, payment, enrollment in a health plan or eligibility for benefits may not be conditioned on the individual's provision of an authorization for the use or disclosure of PHI except:

- Relating to the provision of research related treatment,
- Relating to the health care that is solely for the purpose of creating PHI for disclosure to a third party.

Content Requirements:

Each authorization for the use or disclosure of an individual's PHI shall be written in plain language and shall include at least the following information:

- A specific and meaningful description of the information to be used or disclosed
- The name or identification of the person or class of person(s) authorized to make the use or disclosure
- The name or identification of the person or person(s) to whom the requested use or disclosure may be made
- Purpose of the disclosure or statement that disclosure is at the request of the individual
- An expiration date, condition or event that relates to the individual or the purpose of the use or disclosure
- A statement of the individual's right to revoke the authorization in writing, and exceptions to the right to revoke, together with a description of how the individual may revoke the authorization. Upon written notice of revocation, further use or disclosure of PHI shall cease immediately except to the extent that the departments or employees have acted in reliance upon the authorization or to the extent that use or disclosure is other wide permitted or required by law

- Other statement that treatment, payment, enrollment or eligibility cannot be conditioned on individual signing the authorization or statement setting forth consequences of not signing
- A statement that the information may only be re-released with the written authorization of the individual, except as require by law
- The dated signature of the individual, and
- If the authorization is signed by a personal representative of the individual, a description of the representative's authority to act on behalf of the individual.

Copy to be Provided:

If the entity is seeking the authorization, a copy of the authorization must be provided to the individual.

Retention:

A written or electronic copy of the authorization must be retained for a period of at least six (6) years from the date of execution or the last effective date

Policy No: 01-130

Accounting for Disclosures of Protected Health Information

Purpose:

To issue instructions to all Gaston County departments designated as covered health care components and entities of a Gaston County Organized Healthcare Agreement, regarding the provision of an accounting of disclosures of protected health information (PHI).

Policy:

In compliance with 45 CFR 164.528, an individual has a right to receive an accounting of disclosure of PHI by Gaston County departments designated as covered health care components and entities of a Gaston County Organized Healthcare Agreement, during a time period specified up to six (6) years prior to the date of the request for an accounting except for disclosures:

To carry out TPO as permitted under law
To the individual about his/her own information
For a facility directory or to persons involved in the individual's care or other notification purposes permitted under law
Pursuant to the individual's authorization
For national security or intelligence purposes
To correctional institutions or law enforcement officials as permitted under law
That occurred prior to April 14, 2003

The individual's right to receive an accounting of disclosure of PHI to a health oversight agency or law enforcement official must be suspended for the time period specified by such agency or official if the agency or official provides a written statement asserting that the provision of an accounting would be reasonably likely to impede the activities of the agency or official and specifying a time period for the suspension. Such a suspension may be requested and implemented based on an oral notification for a period of up to thirty (30) days. Such oral request must be documented, including the identity of the agency or official making the request. The suspension may not extend beyond thirty (30) days unless the written statement described herein is submitted during that time period. Requests should be submitted in writing to the designated personnel in each Gaston County department listed as a covered health care component and entities of a Gaston County Organized Health Care Agreement.

Content Requirements:

The written accounting must meet the following requirements:
Other than as accepted above, the accounting must include disclosures of PHI that occurred during the six (6) years (or such shorter time period as is specified in the request) prior to the date of the request including disclosures by or to business associates.

The accounting for each disclosure must include

- Date of disclosure.
- Name of entity or person who received the PHI, and, if known, the address of entity or person.
- A brief description of the PHI disclosed
- A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or in lieu thereof, a copy of the individual's authorization or the request for a disclosure.

- If, during the time period for the accounting, multiple disclosures have been made to the same entity or person or a single purpose, or pursuant to a single authorization, the accounting may provide the information as set forth above for the first disclosure, and then summarize the frequency periodicity, or number of disclosures made during the accounting period and the date of the last such disclosure during the accounting period.
- If during the time period for the accounting, the entity has made disclosures of PHI for research purposes, for 50 or more individuals, the accounting may be disclosed if patient/client cannot be identified.

Provision of the Accounting:

The individual's request for an accounting must be acted upon no later than sixty (60) days after receipt, as follows:

- Provide the accounting requested, or;
- If unable to provide the accounting within sixty (60) days, the time for response may be extended by no more than thirty (30) additional days, provided that:
  * Within the first sixty (60) days, the individual is given a written statement of the reasons for the delay and the date by which the accounting will be provided; and,
  * There are no additional extensions of time for response.

- The first accounting in any twelve month period must be provided to the individual without charge. A reasonable, cost-based fee may be charged for additional accountings within the twelve month period, provided the individual is informed in advance of the fee, and is permitted an opportunity to withdraw or amend the request.

Documentation Requirements:

Gaston County departments designated as health care components and entities of a Gaston County Organized Health Care Agreement must document and retain documentation, in written or electronic format, for a period of at least six years.

- All information required to be included in an accounting of disclosures of PHI
- All written accountings provided to individuals, and;
- Titles of persons responsible for receiving and processing requests for an accounting from individuals.

Policy No: 01-140

Guidelines for Disciplinary Action

Purpose:

All Gaston County employees, entities of a Gaston County OHCA, Business Associates, volunteers, students, contractors, and any other person given access to PHI must comply with all Gaston County HIPAA Privacy and Security policies and procedures. This policy defines violations and addresses a formal process to be followed in the event a privacy and/or security violation has been identified. This policy applies to paper and electronic documents and systems as well as verbal communication. This policy is in compliance with HIPAA Administrative Simplification Sec. 164.530 (e) (1-2)

Policy:

Employees, volunteers, contractors and any other person given access to PHI will be held responsible for any transaction(s) associated with their access and will be held accountable for any privacy or security violation. Any employee, volunteer, student, contractor, BA, or OHCA entity that breaches confidentiality is subject to disciplinary action up to and including immediate termination.

A. **Information Systems Auditing:** Gaston County Information Technology Division will conduct internal audits of system activity maintained by Gaston County and report findings to the Gaston County Privacy Officer. The Gaston County Privacy Officer will inform the Subsidiary Privacy Officer who will be responsible for follow-up on the potential violation. System activity may include file login access, security incidents or investigations.

B. Reporting Privacy and Security Access Violations: The Gaston County Privacy Officer should be notified of suspected privacy and security violations. Employees, patients, etc. may report the issue informally by contacting the Privacy Officer. The Privacy Officer will investigate and verify the extent of the violation.

C. Violation Levels: Violation levels have been categorized in severity levels for use as a guideline to supervisors. They are defined below as follows:

Violation Level I: Represents a minor violation that is accidental, non malicious in nature, and/or due to lack of proper training.

Level I violation may include, but are not limited to:

1. Code Sharing

a. Giving his/her access code to another person
b. Signing on and allowing another person to use his/her code
c. Failing to sign off a given computer terminal or PC.

2. Accessing his or her, own record without following the proper process for completing an authorization.

3. Requesting another co-worker to access his/her own record without following the proper process for completing an authorization.

Violation Level II: Represents a moderate violation in which the intent of the violation is unclear and the evidence cannot be clearly substantiated as to malicious intent.

Level II violation may include, but are not limited to:

1. Accessing a record of a patient without legitimate reason. This includes accessing a co-worker, friend, relative, neighbor, etc.

2. Using another co-worker's access code without the co-worker's authorization.

3. Releasing patient data inappropriately.

Violation Level III - Represents a severe violation in which the employee purposefully violates Gaston County Policies and Procedures, in which evidence clearly establishes malicious intent and/or which there has been an unacceptable number of previous violations.

Level III violation may include, but are not limited to:

1. Releasing data for personal gain

2. Destroying or falsely altering data intentionally.

3. Releasing data with the intent to harm an individual or the organization.

D. Corrective Action:

1. It is the responsibility of the employee's direct supervisor in conjunction with the Subsidiary Privacy Officer and the Gaston County Privacy Officer to take corrective action of each violation. The violation and the action(s) taken must be documented and filed in the employee's personnel file.

2. Guidelines for corrective action to violation levels are, but not limited to, the following:

a. Level I Violations: Verbal/ written warning in addition to policies and procedures retraining.

b. Level II Violations: Written warning, EAP referral, with possible suspension

c. Level III Violations: Termination

Policy No: 01-150

Registration of Protected Health Information

Purpose:

The collection of and maintaining of Protected Health Information (PHI) is a very serious responsibility. Under the HIPAA regulations, all electronic sources of PHI must be identified and protected. Assuring that this information is secure and that uses/disclosures of this information conform to the appropriate confidentially laws and rules are a primary responsibility of Gaston County. All information systems and databases that contain PHI therefore **must** be registered with the Information Technology Division of Gaston County and the HIPAA Coordinating Committee and monitored by the Gaston County Privacy Officer.

Definitions:

Protected Health Information (PHI) means individually identifiable health information relating to the past, present or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual.

PHI System versus PHI Data: The distinction between a PHI System and PHI Data for the purposes of this policy is important. The following matrix shoes the distinctions between the two. All the information in either category is subject to the HIPAA rules and regulations for both Privacy and Security. In no way does this distinction mitigate the need for protection of PHI, regardless of its source, at all times. This distinction is simply used to determine which systems will require registration so that they can be more closely monitored.

Additionally, these PHI Systems will be subject to guidelines as established under the Security Rule.

The following matrix lists characteristics of both PHI Systems and PHI Data. The distinction is important because of the rigor that will be used to monitor these different types of PHI. To the degree possible, the use of electronic PHI Data should be limited in use and scope since it can easily be released either intentionally or unintentionally. When in doubt, the PHI should be treated as a system and therefore subject to all of the security controls and guidelines as defined under the HIPAA Security Rule.

PHI SYSTEM	PHI DATA FILE
System Characteristics	Data Files
· Maintained - Updated on a regular basis	· One time use
· Referenced: Saved for historical purposes	· Deleted after use (intermediate work files)
· Used as part of an ongoing operation or function	· Electronic report files
	· If stored, must be placed on a secured server with password protection (can not be stored on an individual workstation, i.e. C: drive)
Requirements	**Requirements**
· Must be registered	· Must follow PHI Privacy and Security standards
· Must meet all security requirements	· Must never be left on a non-secure environment
· Must be included in disaster recovery plans	· Must be destroyed when no longer used

Procedure:

Application for PHI System:

The attached form "Application for Protected Health Information (PHI) System" should be used for all PHI System requests prior to the development and implementation of the system to make a determination if the system is necessary.

The following information must be included with the application:

- Name of System
- Description/Purpose of the System
- Location of System
- System Components
- Developer of the System
- Number of Anticipated Users
- Primary Contact Person/PHI System Owner
- Source of PHI
- Use of PHI
- Specific Functions performed with PHI
- External Uses of PHI (if applicable)
- Business Associates Related to this PHI System

PHI System Owner:
The definition of the PHI System Owner is the person who will be held responsible and accountable for the information system. This person will be responsible for making sure that all HIPAA Privacy and Security requirements are met for this particular system and data. These requirements include password maintenance, user access in the system, application security, backups and disaster recovery. The PHI System Owner will be responsible for maintaining the PHI System Data Base regarding the status of this system and periodically updating the database.

Approval Process:
Before creating an automated PHI system, the "PHI System Owner" of the system must submit a "Protected Health Information System Registration" application for preliminary review and approval. The form must receive preliminary approval by the HIPAA privacy official and department director. After department approval, forward the application to the Gaston County HIPAA Coordinating Committee for final review and approval

Business Associate Agreement/Chain of Trust Agreement/Trading Partner Agreement:
If one or more of the above Agreements is required, then that individual organization must be clearly identified on the form with an explanation on how the Agreement(s) will be developed, executed and maintained. It will be the responsibility of the PHI System Owner to ensure that the appropriate Agreement(s) are in place at all times. Copies of these agreements must be filed with the Gaston County Privacy Officer.

Information Technology Review:
The Information and Technology staff will be available to review applications to insure that the request for the PHI System is necessary and appropriate, that sufficient safeguards for the protection of the PHI exist and that sufficient planning has taken place to assure that the integrity and accessibility of the data can be maintained.

PHI System Inventory Database:
Once the application is approved, the information regarding the PHI System will be entered into the PHI System Inventory database. The PHI System Owner will be responsible for maintaining the accuracy of the data in this system and for periodically updating the system regarding the status of the system.

Periodic Review:
Periodically, the Information and Technology staff and the Gaston County HIPAA Coordinating Committee may review PHI Systems within Gaston County to insure that this policy is being followed and that PHI Systems have been appropriately registered, reviewed and protected.

Policy No: 02-020

Security Administration

Purpose: To ensure the safeguarding of all EPHI (Electronic Protected Health Information) by following Gaston County's IT HIPAA policies as described below for authorization and/ or supervision, workforce member clearance and procedure for terminating workforce member upon termination. In addition, determining and monitoring access to our servers internally and by third party providers; granting access to ePHI through workstations, transactions, program processes or other mechanisms and to initiate access based upon job functions, review existing access, maintain changes in access and document activities around access. This will occur through security awareness training for all workforce members, protection from malicious software, monitoring of log-in attempts and reporting of discrepancies. All suspected or know incidents of security incidents will be identified and responded to as appropriate. Gaston County IT also will maintain data backup procedures and have a contingency plan, which is tested periodically and evaluated and revised as needed. Gaston County IT will safeguard the facilities and equipment housed with the facilities from physical access, tampering and/ or theft using procedures to control access from outside visitors, vendors and also to document repairs and / or modifications to the facility which are related to security.

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.

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.

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.

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.

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.

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 maintains 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.

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 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.

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, etc.

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.

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 stated in 4.2 of this policy.

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

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, and 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 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 (e.g. SecureWorks).

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 it the new solution does not support access to the backup format or media type, third-party services, such as Ontrack Recovery, 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.

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.

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.

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.

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.

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, door lock, etc.

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.

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 History
   4.1 – 12/09/2010

Information Technology Department Acceptable Use Policy

Overview

The Information Technology Department's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Gaston County's established culture of openness, trust and integrity. The Information Technology Department is committed to protecting Gaston County's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/ Extranet- related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing and FTP are the property of Gaston County. These systems are to be sued for business purposes in serving the interests of the taxpayers of the county, our clients and customers, in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Gaston County employee and affiliate who deals with information and/ or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Departments are charged with monitoring and enforcing the workplace rules. They may choose to establish and enforce standards that are more restrictive than the guidelines defined here.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Gaston County. The rules are in place to protect the employee and Gaston County. Inappropriate use exposes Gaston County to risks including virus attacks, compromise of network systems and services and legal issues.

Scope

The scope of this policy includes all temporary or permanent, full or part- time employees, contractors, consultants, volunteers and other workers at Gaston County, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Gaston County.

Policy

General Use and Ownership

1. While Gaston County's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the county's systems remains the property of Gaston County. Because of the need to protect Gaston County's network, management cannot guarantee the confidentiality of information stored on any network device belonging to Gaston County.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use Internet/Intranet/ Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or director.
3. Information Technology Department recommends that any information that users consider sensitive or vulnerable be encrypted.

4. For security and network maintenance purposes, authorized individuals within Gaston County may monitor equipment, systems and network traffic at any time.
5. Gaston County reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/ Extranet- related systems should be classified as confidential or non- confidential, as defined by county confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: personal health information and specific personnel data described in the Human Resources Policy as not subject to public scrutiny. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly; user level passwords should be changed every six months.
3. All PCs. Laptops and workstations should be secured with a password- protected screensaver with the automatic activation feature set at 10 minutes or less or by logging-off (control- alt- delete for Win2K users) when the host will be unattended.
4. Use encryption of information in compliance with Information Technology Department's Acceptable Encryption Use Policy.
5. Because information contained on portable computers is especially vulnerable, special care should exercised.
6. Postings by employees form a Gaston County email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Gaston County, unless posting is in the course of business duties.
7. All hosts used by the employee that are connected to Gaston County Internet/Intranet/ Extranet, whether owned by the employee or Gaston County, shall be continually executing approved virus- scanning software with a current virus database.
8. Employees must use extreme caution when opening e-mail attachments received from unknown senders , which may contain viruses, e-mail bombs, or Trojan horse code

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Gaston County authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Gaston Count- owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, installation or distribution of " pirated" or other software products that are not appropriately licensed for use by Gaston County.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Gaston County or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a Gaston County computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any Gaston County Account.
8. Making statements about warranty, expressly or implied, unless it is part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption' includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to Information Technology Department is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/ duty.
12. Circumventing user authentication or security of any host, network, or account.
13. Interfering with or denying service to any user other than the employee's host (for or example, denial of service attack).
14. Using any program/ script/ command, or sending messages of any kind, with the intent to interfere with , or disable a user's terminal session, via any means, locally or via the Internet/ Intranet/ Extranet.
15. Providing information about, or lists of, Gaston County employees to parties outside Gaston County.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Gaston County's networks of other Internet/Intranet/Extranet service providers in behalf of, or to advertise, any service hosted by Gaston County or connected via Gaston County's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment as outlined in section 18.1 of Gaston County's Personnel Policies and Procedures.

Definitions

Terms	**Definitions**
Spam	Unauthorized and/ or unsolicited electronic mass mailings.

References: Gaston County IT Policy: For more specific information on Gaston County IT policies.

ITSP – 310-2-10
IT Security Policy – Define Workstation Use
HIPAA: Information Access Management - Section: § 164.310(d) (1)

Policy: # ITSP – 310-3-10
IT Security Policy – Define Workstation Security
HIPAA: Information Access Management - Section: § 164.310(d) (1)
Policy: # ITSP – 310-4-10
IT Security Policy – Device and Media Controls – Disposal
HIPAA: Information Access Management - Section: § 164.310(d) (1)
Policy: # ITSP – 310-4-20
IT Security Policy – Device and Media Controls – Media Re-use
HIPAA: Information Access Management - Section: § 164.310(d) (1)

Policy: # ITSP – 310-4-30
IT Security Policy – Device and Media Controls – Accountability
HIPAA: Information Access Management - Section: § 164.310(d) (1)

Policy: # ITSP – 310-4-40
IT Security Policy – Data Backup and Storage Existing Data Backup

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

Policy: # ITSP – 312-1-20
IT Security Policy – Emergency Access Procedure
HIPAA: Information Access Management - Section: § 164.312(d) (1)
Policy: # ITSP – 312-2-10
IT Security Policy – Audit Control
HIPAA: Information Access Management - Section: § 164.312(b)

Policy No: 02-040

Password Policy

Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Gaston County's entire corporate network. As such, all Gaston County employees (including contractors and vendors with access to Gaston County systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Gaston County facility, has access to the Gaston County network, or stores any non-public Gaston County information.

Policy

General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.
- User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at Gaston County. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "Gaston County", "sanjose", "sanfran" or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for Gaston County accounts as for other non-Gaston County access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various Gaston County access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share Gaston County passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Gaston County information.

Here is a list of "don’ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")

- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers
- Don’t repeat the use of a password

If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, and Netscape Messenger).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months. (AS/400 passwords are systematically required to be changed every 60 days.)

If an account or password is suspected to have been compromised, report the incident to Information Technology Department and change all passwords. (As/400 user passwords and device will be disabled after five (5) invalid password attempts.)

Information Technology Department or its delegates may perform password cracking or guessing on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Pass-phrases for Remote Access Users

Access to the Gaston County Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong pass-phrase.

E. Pass-phrases

Pass-phrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the pass-phrase to "unlock" the private key, the user cannot gain access.

Pass-phrases are not the same as passwords. A pass-phrase is a longer version of a password and is, therefore, more secure. A pass-phrase is typically composed of multiple words. Because of this, a pass-phrase is more secure against "dictionary attacks."

A good pass-phrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good pass-phrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to pass-phrases.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment as outlined in section 18.1 of Gaston County's Personnel Policies and Procedures.

Definitions

Terms	Definitions
Application Administration Account	Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).

References: Gaston County IT Policy: For more specific information on Gaston County IT policies.

Policy: # ITSP – 312-3-10
IT Security Policy – Mechanism to Authenticate
HIPAA: Information Access Management - Section: § 164.312(c)(2)

Policy: # ITSP – 312-4-10
IT Security Policy – Person or Entity Authentication
HIPAA: Information Access Management - Section: § 164.312(e)(1)

Acceptable Encryption Policy

Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

Scope

This policy applies to all Gaston County employees and affiliates.

Policy

Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hillman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 56 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. Gaston County's key length requirements will be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by Information Technology Department. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment as outlined in section 18.1 of Gaston County's Personnel Policies and Procedures.

Definitions

Term	Definition
Proprietary Encryption	An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.

Symmetric Cryptosystem: A method of encryption in which the same key is used for both encryption and decryption of the data.

Asymmetric Cryptosystem: A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

References: Gaston County IT Policy: For more specific information on Gaston County IT policies.

Policy: # ITSP – 312-5-00
IT Security Policy – Integrity Controls & Encryption
HIPAA: Information Access Management - Section: § 164.312(d)

Policy No: 02-060

Automatically Forwarded Email Policy

Purpose
To prevent the unauthorized or inadvertent disclosure of sensitive information, personal health data, or non-public employee information..

Scope
This policy covers automatic email forwarding, and thereby the potentially inadvertent transmission of sensitive information by all employees, vendors, and agents operating on behalf of Gaston County.

Policy
Employees must exercise utmost caution when sending any email from inside Gaston County to an outside network. Unless approved by an employee's manager, Gaston County email will not be automatically forwarded to an external destination. Sensitive information will not be forwarded via any means, unless that email is critical to county business and is encrypted in accordance with the *Acceptable Encryption Policy*.

Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment as outlined in section 18.1 of Gaston County's Personnel Policies and Procedures.

Definitions

Terms	Definitions
Email:	The electronic transmission of information through a mail protocol such as SMTP. Programs such as Eudora and Microsoft Outlook use SMTP.
Forwarded email:	Email resent from internal networking to an outside point.
Sensitive information	Information is considered sensitive if it can be damaging to Gaston County or its customers' dollar value, reputation, or community standing.
Unauthorized Disclosure:	The intentional or unintentional revealing of restricted information to people who do not have a need to know that information.

Gaston County IT HIPAA Manual

Table of Contents

1. **Introduction**
2. **The Security Rule Guidelines**
3. **Gaston County IT HIPAA Manual Structure and Naming Convention**
4. **Gaston County IT HIPAA Security Matrix**
5. **IT HIPAA Policies**

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.

A recap of Title II was from Wikipedia titled, "Health Insurance Portability and Accountability Act" dated 7 October 2009 at 19:03. Access to this information is allowed under Wikipedia's "Creative Commons Attribution-ShareAlike License."

Title II: Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform

Title II of HIPAA defines numerous offenses relating to health care and sets civil and criminal penalties for them. It also creates several programs to control fraud and abuse within the health care system. However, the most significant provisions of Title II are its Administrative Simplification rules. Title II requires the Department of Health and Human Services (HHS) to draft rules aimed at increasing the efficiency of the health care system by creating standards for the use and dissemination of health care information.

These rules apply to "covered entities" as defined by HIPAA and the HHS. Covered entities include health plans, health care clearinghouses, such as billing services and community health information systems, and health care providers that transmit health care data in a way that is regulated by HIPAA.

Per the requirements of Title II, the HHS has promulgated five rules regarding Administrative Simplification:

1. Privacy Rule
2. Transactions and Code Sets Rule
3. **Security Rule**
4. Unique Identifiers Rule
5. Enforcement Rule.

The Security Rule is the focus of Electronic Protected Health Information (ePHI). It provides a matrix for IT compliance, which is the basis of the Gaston County IT HIPAA Manual.

Security Rule Guidelines

The Final Rule on Security Standards was issued on February 20, 2003. It took effect on April 21, 2003 with a compliance date of April 21, 2005 for most covered entities and April 21, 2006 for "small plans". The Security Rule complements the Privacy Rule. While the Privacy Rule pertains to all Protected Health Information (PHI) including paper and electronic, *the Security Rule deals specifically with Electronic Protected Health Information (ePHI)*.

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.

Required or Addressable:
In the document produced by the Department of Health & Human Services titled, "HIPAA Security Series: #6 Security Standards: Implementation for the Small Provider," dated December 10, 2007, explains "Required or Addressable":

"Many of the standards contain implementation specifications. An implementation specification is a more detailed description of the method or approach covered entities can use to meet a particular standard. ***Implementation specifications are either required or addressable***. Regardless of whether a standard includes one or more implementation specifications, covered entities must comply with each standard. Where there is no implementation specification for a particular standard, such as the "Workstation Use" and "Person or Entity Authentication" standards, compliance with the standard itself is required.
• 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."***

New Enforcement Legislation
The Health Information Technology for Economic and Clinical Health (HITECH) Act is effective as of February 17th, 2010. The HITECH Act permits state attorney general's offices to

pursue civil charges on behalf of victims, in addition to fines for HIPAA violators of up to $1.5 million per year.
From the Office of the Civil Rights on 02/22/10
http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html:

Civil Money Penalties. OCR may impose a penalty on a covered entity for a failure to comply with a requirement of the Privacy Rule. Penalties will vary significantly depending on factors such as the date of the violation, whether the covered entity knew or should have known of the failure to comply, or whether the covered entity's failure to comply was due to willful neglect. Penalties may not exceed a calendar year cap for multiple violations of the same requirement.

	Penalty Amount	Calendar Year Cap
For violations occurring prior to 2/18/2009	Up to $100 per violation	$25,000
For violations occurring on or after 2/18/2009	$100 to $50,000 or more per violation	$1,500,000

A penalty will not be imposed for violations in certain circumstances, such as if:

- the failure to comply was not due to willful neglect, and was corrected during a 30-day period after the entity knew or should have known the failure to comply had occurred (unless the period is extended at the discretion of OCR); or
- the Department of Justice has imposed a criminal penalty for the failure to comply (see below).

In addition, OCR may choose to reduce a penalty if the failure to comply was due to reasonable cause and the penalty would be excessive given the nature and extent of the noncompliance.
Before OCR imposes a penalty, it will notify the covered entity and provide the covered entity with an opportunity to provide written evidence of those circumstances that would reduce or bar a penalty. This evidence must be submitted to OCR within 30 days of receipt of the notice. In addition, if OCR states that it intends to impose a penalty, a covered entity has the right to request an administrative hearing to appeal the proposed penalty.
Criminal Penalties. A person who knowingly obtains or discloses individually identifiable health information in violation of the Privacy Rule may face a criminal penalty of up to $50,000 and up to one-year imprisonment. The criminal penalties increase to $100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses, and to $250,000 and up to 10 years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use identifiable health information for commercial advantage, personal gain or malicious harm. The Department of Justice is responsible for criminal prosecutions under the Privacy 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 <u>one</u> 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 Manual Structure.

1. This HIPAA Manual will be designed to note the type of Security Safeguard – Administrative, Physical, or Technical.
2. The Standard of each Security Safeguard.
3. The specific HIPAA section reference number.
4. Dates of last updates.

For example:

Administrative Safeguards	
	Security Management Process - Section: § 164.308(a)(1) • Risk Analysis *comment regarding this issue*

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 01-030	R
• Sanction Policy Defined, Gaston County HIPAA Manual, Policy 01-140	R
• Information System Activity Review Defined, Gaston County HIPAA Manual, Policy 02-010	R
Assigned Security Responsibility - Section: § 164.308(a)(2)	
• Assign Security Responsibility Defined, Gaston County HIPAA Manual, Policy 01- 020, 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.	R

• 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.	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 HIPAA Manual, Policy 02-040	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. (Dean Hoyle)	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 01-050	R

Physical Safeguards	Required or Addressable
Facility Access Controls - Section: § 164.310(a)(1) • Contingency Operations Defined Gaston County Disaster Recovery Plan. Dean Hoyle maintains a list of these as part of an extensive DR 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.	R
• Media Re-use Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 310-4-20.	R
• Accountability Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 310-4-30.	A
• Data Backup and Storage Existing Data Backup Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 310-4-40.	A

Access Control - Section: § 164.312(a)(1)	
• Unique User Identification Defined, Gaston County HIPAA Manual, Policy 02-030 (Rewrite)	R
• Emergency Access Procedure Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 312-1-20.	R
• Automatic Logoff Defined, Gaston County HIPAA Manual, Policy 02-030	A
• Encryption and Decryption Defined, Gaston County HIPAA Manual, Policy 02-030	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	A

Defined, Gaston County IT HIPAA Manual, Policy # ITSP - 312-3-10.	
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 02-030 • Other Arrangements	R R
Requirements for Group Health Plans - Section: § 164.314(b)(1) • Implementation Specifications Defined, Gaston County HIPAA Manual, Policy 02-030	R

Policies, Procedures and Documentation Requirements	
Policies and Procedures - Section: § 164.316(a) • Creation and Maintenance Defined, Gaston County HIPAA Manual, Policy 01-010	R

Documentation - Section: § 164.316(b)(1) • Time Limit Defined, Gaston County HIPAA Manual, Policy 01-020 • Availability Defined, Gaston County HIPAA Manual, Policy 01-020 • Updates Defined, Gaston County HIPAA Manual, Policy 01-010	 R R R

Gaston County IT HIPAA Manual Policies

ITSP-308-3-10 - Authorization and/or Supervision
ITSP-308-3-20 – Workforce Clearance Procedure
ITSP-308-3-30 – Termination Procedures
ITSP-308-4-10 - Isolating Health Care Clearing House Functions
ITSP-308-4-20 – Access Authorization
ITSP-308-4-30 - Access Establishment and Modifications
ITSP-308-5-10 – Security Reminders
ITSP-308-5-20 – Protection from Malicious Software
ITSP-308-5-30 - Log-in Monitoring
ITSP-308-6-10 – Response and Reporting
ITSP-308-7-10 - Data Backup Plan
ITSP-308-7-20 - Disaster Recovery Plan
ITSP-308-7-30 - Emergency Mode Operation Plan
ITSP-308-7-40 -Testing and Revision Procedures
ITSP-308-8-10 – Evaluation
ITSP-310-1-20 - Facility Security Plan
ITSP-310-1-30 - Access Control and Validation Process
ITSP-310-1-40 - Maintenance Records
ITSP-310-2-10 - Define Workstation Use
ITSP-310-3-10 - Define Workstation Security
ITSP-310-4-10 - Device and Media Controls – Disposal
ITSP-310-4-20 - Device and Media Controls - Media Re-use
ITSP-310-4-30 - Device and Media Controls – Accountability
ITSP-310-4-40 - Data Backup and Storage Existing Data Backup
ITSP-312-1-20 - Emergency Access Procedures
ITSP-312-2-10 - Audit Control
ITSP-312-3-10 - Mechanism to Authenticate
ITSP-312-4-10 - Person or Entity Authentication
ITSP-312-5-00 - Integrity Controls & Encryption

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 (e.g. "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)

2. 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.

4. Scope

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

5. Policy
   5.1 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.
   5.2 This list must be documented.
   5.3 Review Cycle - The list should be reviewed and updated annually.

6. Revision History
   4.1 - 09/14/2010

Policy: # ITSP – 308-3-20
IT Security Policy – Workforce Clearance Procedure
HIPAA: Workforce Security - Section: § 164.308(a)(3)

2. 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.

4. Scope

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

5. Policy
   5.1 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.
   5.2 Review Cycle - The specific groups and methods should be reviewed and updated annually.

6. Revision History
   6.1 – 09/10/2010

Policy: # ITSP – 308-3-30
IT Security Policy – Termination Procedures
HIPAA: Workforce Security - Section: § 164.308(a)(3)

2. 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).

4. Scope

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

5. Policy
   5.1 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.
   5.2 Termination of Physical Access – When any member of the workforce has been terminated, physical access, whether key card, ID card, etc. must be discontinued.
   5.3 Authorization to Terminate Access – authorization for termination is initiated by authorized personnel, whether a supervisor of ePHI, Human Resources, or Gaston County IT.
   5.4 Timing of Termination of Access – Termination to the ePHI is required in a timely manner.

6. Revision History
   6.1 – 09/10/2010

Policy: # ITSP – 308-4-10
IT Security Policy – Isolating Health Care Clearinghouse Functions
HIPAA: Information Access Management - Section: § 164.308(a)(4)

4. 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.

5. Scope

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

6. Policy
   6.1 Server Identification – Create and maintain a list of servers containing ePHI data.
   6.2 Access Identification – Create and maintain a list of third party entities, including vendors, who access these systems.
   6.3 Third Party Process – Create and maintain a list of the process each third party entity uses to access the Gaston County ePHI.
   6.4 Isolation Identification – document methods to isolate the ePHI internally.
   6.5 Review Cycle - The specific lists and methods should be reviewed and updated annually.

4. Revision History
   4.1 – 09/10/2010

Policy: # ITSP – 308-4-20
IT Security Policy – Access Authorization
HIPAA: Information Access Management - Section: § 164.308(a)(4)

2. 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.

4. Scope

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

5. Policy
   5.1 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.
   5.2 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.
   5.3 Employees must receive HIPAA and security awareness training prior to obtaining access to ePHI.

6. Revision History
   6.1 – 09/10/2010

Policy: # ITSP – 308-4-30
IT Security Policy – Access Establishment and Modification
HIPAA: Information Access Management - Section: § 164.308(a)(4)

2. Purpose

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

4. Scope

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

5. Policy
   5.1 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.
   5.2 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.
   5.3 Review Cycle - The access should be reviewed and updated annually.

6. Revision History
   6.1 – 09/10/2010

Policy: # ITSP – 308-5-10
IT Security Policy – Security Reminders
HIPAA: Security Awareness and Training - Section: § 164.308(a)(5)

2. 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.

4. Scope

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

5. Policy
   5.1 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 Gaston County IT, Human Resources or both. Training may be instructor led, on-line or in book form.

5.2 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.

5.3 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 History

4.1 – 12/09/2010

Policy: # ITSP – 308-5-20

IT Security Policy – Protection from Malicious Software

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

2. 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, etc.

4. Scope

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

5. Policy

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

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

4. Revision History

4.1 – 12/09/2010

Policy: # ITSP – 308-5-30

IT Security Policy –Log-in Monitoring

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

4. Purpose

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

5. Scope

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

6. Policy
   6.1 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.
   6.2 Discrepancy Reporting – Information Technology shall create a report based on failed login attempts.
   6.3 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.
   6.4 Review and Document – Review the Discrepancy Report on a timely basis.
   6.5 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 stated in 4.2 of this policy.
   6.6 Retention Cycle - The logs must be retained for seven years from the date of creation as defined by HIPAA.

4. Revision History
   4.1 – 12/09/2010

Policy: # ITSP – 308-6-10
IT Security Policy – Response and Reporting
HIPAA: Security Incident Procedures - Section: § 164.308(a)(7)

4. 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.

5. Scope

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

6. Policy
   6.1 Members of the IT Department, Managers, and 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 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.

6.2 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 (e.g. SecureWorks).

4. Revision History

4.1 – 12/09/2010

Policy: # ITSP – 308-7-10

IT Security Policy – Data Backup Plan

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

4. 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).

5. Scope

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

6. Policy

6.1 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.

6.2 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.

6.3 Retrievable State – Backups must be able to restore data as retrievable exact copies.

6.4 Backup Storage – Backups must be stored in a secure environment.

6.5 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 it the new solution

does not support access to the backup format or media type, third-party services, such as Ontrack Recovery, can be used for this conversion on an as-needed basis.

6.6 Retention Cycle - ePHI backups must be able to be retrievable for seven years.

4. Revision History

4.1 – 12/09/2010

Policy: # ITSP – 308-7-20

IT Security Policy – Disaster Recovery Plan

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

4. 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.

5. 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.

6. Policy

6.1 Departments in conjunction with Information Technology shall create a list of the ePHI that must be backed up.

6.2 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.

6.3 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.

6.4 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.

6.5 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 History

4.1 – 12/09/2010

Policy: # ITSP – 308-7-30

IT Security Policy –Emergency Mode Operation Plan

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

4. 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.

5. Scope

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

6. Policy

6.1 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.

6.2 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.

6.3 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.

6.4 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.

6.5 Contact List – the Emergency Mode Operation Plan must include a list of personnel with contact information needed for the restoration process.

4. Revision History

4.1 – 12/09/2010

Policy: # ITSP – 308-7-40
IT Security Policy –Testing and Revision Procedures
HIPAA: Contingency Plan - Section: § 164.308(a)(7)

4. 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.

5. 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.

6. Policy
   - 6.1 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.
   - 6.2 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.
   - 6.3 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.
   - 6.4 Test Cycle - The simulation testing must occur at least once every two years.
   - 6.5 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
   - 4.1 – 12/09/2010

Policy: # ITSP – 308-8-10
IT Security Policy – Evaluation
HIPAA: Evaluation - Section: § 164.308(a)(8)

4. Purpose

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

5. Scope

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

6. Policy
   6.1 Frequency of HIPAA Compliance Evaluation – an internal review of HIPAA Compliance should occur every two years.

4. Revision History
   4.1 – 12/09/2010

Policy: # ITSP – 310-1-20
IT Security Policy – Facility Security Plan
HIPAA: Facility Access Controls - Section: § 164.310(a)(1)

4. Purpose

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

5. Scope

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

6. Policy
   6.1 Systems and electronic media containing ePHI are to be located in physically secure locations.
   6.2 Secure locations must have physical access controls, such as Card Key, door locks, etc.
   6.3 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, door lock, etc.

4. Revision History
   4.1 – 12/09/2010

Policy: # ITSP – 310-1-30

IT Security Policy – Access Control and Validation Process

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

4. 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.

5. Scope

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

6. Policy

6.1 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.

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

4. Revision History

4.1 – 12/09/2010

Policy: # ITSP – 310-1-40

IT Security Policy – Maintenance Records

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

4. 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).

5. Scope

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

6. Policy

3.4 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.

3.5 Log Content – the information logged must include at least the location, date, time, name of person, vendor company name (if any).

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

5. Revision History

4.2 – 12/09/2010

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 History

4.1 – 12/09/2010

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 identification 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 History
   4.1 – 12/09/2010

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 formats. 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 Memory Stick – 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 History

4.1 – 12/09/2010

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 History

4.1 – 12/09/2010

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 therefore.

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 History
   4.1 – 12/09/2010

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 History
   4.1 – 12/09/2010

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 History
   4.1 – 12/09/2010

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 History
   4.1 – 12/09/2010

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 History
   4.1 – 12/09/2010

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 History
   4.1 – 12/09/2010

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 History

4.1 – 12/09/2010