

Gaston County HIPAA Manual

Action	Date
Reviewed and Revised	December, 2012
Reviewed and Revised	October, 2018

See also Gaston County Information Technology HIPAA Manual for IT-related policies concerning HIPAA

PART I: ADMINISTRATIVE; GENERAL POLICY

Policy No: 1-001

Administrative Requirements for the Implementation of the HIPAA Act

Purpose:

To issue instructions to all Gaston County Departments, entities covered by an Organized HealthCare Agreement (also referred to as "OHCA") or Business Association Agreement (also referred to as BAA") as well as workforce members regarding Gaston County's obligations relating to the implementation of the Health Insurance Portability and Accountability Act (HIPAA) based upon regulations, such as those found in 45 CFR Parts 160 and 164.

Policy:

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

1. **Compliance Officer:** Gaston County must designate an individual responsible for overall compliance with HIPAA, including implementation and ongoing compliance with all Administrative Simplification issues. The Compliance Officer shall also assist the Privacy Officer and Security Officer in their duties. Unless otherwise specified, the Compliance Officer shall be the Assistant County Attorney.
2. **Privacy Official:** Gaston County must designate an individual to serve as the Privacy Official 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) and is also responsible for supervising duties and responsibilities of subsidiary privacy officers when related to HIPAA. The term "Privacy Official" shall be used interchangeably with the term "Privacy Officer." Unless otherwise specified, the Privacy Official shall be the Director of the Division of Public Health, Department of Health and Human Services.
3. **Security Officer:** Gaston County must designate an individual to serve as the Security Officer for the entire county. This individual is responsible for the development and implementation of county-wide policies and procedures relating to electronically securing Protected Health Information (PHI) and is also responsible to maintain and enhance security of the open network system and services. Unless otherwise specified, the security officer shall be the Chief Information Officer of Gaston County.

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 or Business Associate 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 directives from the County Compliance Officer, 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 or Business Associate Agreement must document the following training actions:

All Gaston County employees and other workforce members who work for a department or division covered by this policy 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 or Business Associate 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 or Business Associate 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, or use the policies as described herein. All policies must comply with federal and state law, particularly concerning laws concerning whistleblowers and 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 or Business Associate 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 or Retaliatory Acts and Waiver of Rights Prohibited: No member of Gaston County or entities of a Gaston County Organized Health Care Agreement or Business Associate 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 or Business Associate 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 or Business Associate 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 or Business Associate 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 or Business Associate 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 or Business Associate 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 or Business Associate 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 provided that 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. Final approval for such change shall be authorized by the County Manager, as described in Policy 2003-104.

Documentation Requirements: Gaston County, departments designated as covered health care components, and entities of a Gaston County Organized Health Care Agreement or Business Associate 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 healthcare component as well as entities of a Gaston County Organized Health Care Agreement or Business Associate Agreement must be submitted to the Gaston County Privacy Official to be retained permanently.

Gaston County HIPAA Committee Members

Purpose:

The purpose of this policy is to enumerate those who serve on the Gaston County HIPAA Committee. The HIPAA Compliance Committee is intended to be a cross-departmental group to discuss interdepartmental and county-wide HIPAA related issues.

Policy: The Gaston County HIPAA Committee shall meet on at least an annual basis. The purpose of this Committee is to discuss, analyze, and review broad county-wide HIPAA issues and policies. Various Departments may have individual intra-department meetings to discuss department-specific HIPAA issues and policies. The membership of the Committee is as follows:

COMMITTEE MEMBER	POSITION ON COMMITTEE
Assistant County Attorney	Compliance Officer
DHHS, Division of Public Health Director	Privacy Official
Chief Information Officer	Security Officer; Member representing IT
DHHS Director	Member, representing DHHS-Health
Chief, GEMS	Member, representing GEMS
Human Resources Director	Member, representing HR
Sheriff	Member, representing Sheriff
DHHS, Social Services Director	Member, representing DHHS-Social Svc.
Police Chief	Member, representing Police
County Manager	Ex Officio
County Attorney	Ex Officio

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.

Introduction:

Gaston County is a hybrid entity and has the following covered departments that are designated covered health care components: Community Development and Technology, Gaston County Health and Human Services, Division of Social Services.¹ The Gaston County Health and Human Services, Human Services Division has only has one section which is the Adult Services that is a covered component. All sections at the Gaston County Department of Public Health and Human Services, Division of Health, are designated as covered components with the exception of Environmental Health.

Employees of Adult Services at the Gaston County Department of Health and Human Services, Gaston Emergency Medical Services, Human Resources, Public Health, and the Office of the Sheriff shall comply with this policy, to the extent required by law. In addition to these departments which are covered health care components, other departments such as the Attorney's Office, Finance, and Information Technology having access to individually identifiable health information and will comply with this policy, to the extent required by law. This Policy is not intended to be applied to Gaston County Departments not subject to the requirements of HIPAA as a matter of regulation or law.

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. For the purposes of this Policy Manual, whenever possible and unless expressly indicated to the contrary, the requirements of an entity which is considered to be an OHCA are the same as entities which have a Business Associate Agreement ("BAA") with Gaston County.

This Manual 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. The manual is to be read in conjunction with other Gaston County Policies, including the Gaston County Personnel Policy and in particular Chapter 26, entitled Use of Informational Technology Resources as well as the Gaston County IT HIPAA Manual.

¹ Gaston County Health Department and Gaston County Department of Social Services consolidated into Gaston County Department of Health and Human Services. In this manual, any references to "Gaston County Health Department" or "Gaston County Social Services" refers to the consolidated department of Gaston County Health and Human Services.

Privacy Policy/Procedure Development and Approval Process

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

The original HIPAA policies and procedures were approved by the Gaston County Board of Commissioners in Resolution 2003-104. Such resolution authorized the Privacy Official to approve revisions and/or additions in order to maintain and better implement HIPAA compliance.

The Compliance Officer will serve as lead person for the Gaston County HIPAA Compliance Committee.

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 or Business Associate Agreement will be responsible for submitting approved policies and procedures to the Privacy Official for Gaston County.

The Gaston County Privacy Officer will incorporate any suggested changes and discuss them with the appropriate representatives from that Department. Revisions may also be discussed by members of the HIPAA Compliance Committee.

The designated employee in each covered department should submit individual policy/procedures to the Gaston County Compliance Officer 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.

PART II SECURITY AND PRIVACY OF PROTECTED HEALTH INFORMATION

Policy No: 02-001

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 or Business Associate 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.

Permitted and Required Uses and Disclosures: PHI may or shall be disclosed as follows to the individual:

- a. To carry out Treatment, Payment, and Operations (TPO) activities, within specified limits.
- b. Pursuant to and in compliance with a current and valid Authorization.
- c. In keeping with a Business Associate (BA) arrangement.
- d. As otherwise provided for in the HIPAA privacy regulations.

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.

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 such person's 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.

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.

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.

Amendment to PHI: An individual has the right to request amendment to PHI or other information in the designated record set.

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 or Business Associate 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. Unless otherwise specified by such department, all complaint processes shall be presented to the Subsidiary Privacy Officer of such department. At that time, the Subsidiary Privacy Official shall forward such complaint to the Compliance Officer and Privacy Official for additional review.

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.

HITECH Act Compliance: Gaston County, and the relevant departments and individuals, acknowledge the need to obtain compliance concerning the Health Information Technology for Economic and Clinical Health (HITECH) Act. The HITECH Act, among other things, provides standards and requirements for electronic accessing of certain types of health information, such as information accessible through a patient portal, enabling the patient to examine online information such as immunization records, prescription drug information, and to allow a patient to communicate electronically with a health care provider.

Applicability of IT Policy: The Gaston County Personnel Policy includes a section concerning information technology. Such Policy incorporated by reference to this Manual. Additionally, the Gaston County IT HIPAA Manual is incorporated herein. Such incorporated policies are available electronically to Gaston County employees.

Facsimile Transmission of Patient Health Information

Purpose: To create policies protecting PHI during facsimile

Policy: Transmitting patient information via facsimile or e-mail is 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. For the purposes of this policy, the term "facsimile" shall include all electronic methods of transmitting Patient Health Information, such as e-mail or sending documents via PDF or similar method. Additionally, the term "fax machine" or "facsimile machine", where contextually appropriate, shall also mean computer, printer, or other electronic device.

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:

Location of fax machines:

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

Use of cover page:

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

Date and time of transmission,

Gaston County Health Department's name, address, telephone, and appropriate facsimile numbers,

Authorized receiver's name,

Number of pages transmitted.

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.

Recipient confirmation

Provided if is technologically possible, 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 coversheet the information transmitted.

Misdirected transmissions

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.

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.

Receiving patient information via facsimile

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.

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

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

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 or Business Associate 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 (such as a computer database or similar program) 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 Compliance Officer.

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 on at least an annual basis to ensure that the access to PHI meets the Minimum Necessary standard.

For non-routine disclosures (other than pursuant to an authorization, such as sending disclosures to accrediting bodies, insurance carriers, research entities, funeral homes 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 Covered Entity or is from a public official or a professional for the purpose of providing services to the Covered Entity, 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 Compliance Officer.

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 provided herein. 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. A BA must be in place for all entities that create, maintain, or transmit ePHI maintained by the covered entity.

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 relating 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.

Organized Health Care Agreements

Purpose: To issue instructions to all workforce members in Gaston County regarding the content and requirements of entities of a Gaston County Organized Health Care Agreement (OHCA) relating to the OHCA's use of protected health information (PHI) concerning healthcare operations. To the extent applicable, this Policy shall also apply to entities having a Business Associate Agreement with Gaston County.

Policy: Gaston County maintains a current list of entities it has an OHCA with. Gaston County departments designated as health care components may disclose/share PHI with an entity which is part 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 Gaston County knows of an entity which signed the OHCA has violated such the agreement, Gaston County must inform the entity to cure the breach or end the violation. If such attempt is unsuccessful Gaston County must 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 or Business Associate Agreement 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 policies described herein or in the above-described notice.

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. The 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 or Business Associate Agreement 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 provided. The receipt of acknowledgment will be maintained in the designated record set. Additionally, the notice in effect 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.

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 or Business Associate Agreement 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 litigation.
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 Compliance Officer 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 it 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."

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 or Business Associate 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 or Business Associate Agreement will be responsible for receiving complaints/grievances relating to individuals' privacy rights, and rights to access their designated record set, to request restrictions in 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 Compliance Officer, 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 Compliance Officer. 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 Officer. 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 Compliance Officer and shall be given assistance in doing so, if requested.

The Privacy Official shall consult with the HIPAA Compliance Committee in investigating, reviewing and acting upon complaints/grievances. The investigator 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 investigator 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 Compliance Officer will report such finding to the workforce member's supervisor.

The Gaston County Compliance Officer 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 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 Compliance Officer. For the purposes of this Policy, the Gaston County Compliance Officer as well as the Gaston County Privacy Official may delegate such responsibilities and duties prescribed herein as deemed appropriate under the circumstances.

Use or Disclosure of PHI for Treatment, Payment or Health Care Operation

Purpose: To issue instructions to all Gaston County departments, entities of an Organized Health Care Organization or Business Associate Agreement as well as 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 health 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 as a health care component or entities of an Organized Health Care Agreement or Business Associate 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 or Business Associate Agreement 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 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.

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 or Business Associate Agreement, 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.

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 or Business Associate 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 or Business Associate Agreement, during a time period specified up to six (6) years prior to the date of the request for an accounting except for disclosures:

1. To carry out TPO as permitted under law,
2. To the individual about his/her own information,
3. For a facility directory or to persons involved in the individual's care or other notification purposes permitted under law,
4. Pursuant to the individual's authorization,
5. For national security or intelligence purposes.

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.

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. This policy is not intended to supersede the Gaston County Personnel Policy and should be read in conjunction with such policy.

Information Systems Auditing: Provided it is technologically feasible, Gaston County Information Technology Department will conduct annual 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. Such audits will be done in accordance with the most current best practices of Gaston County Information Technology.

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.

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:
 - Giving his/her access code to another person.
 - Signing on and allowing another person to use his/her code.
 - 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.

Corrective Action:

It is the responsibility of the employee's direct supervisor in conjunction with the Subsidiary Privacy Official, Compliance Officer and the Gaston County Privacy Official 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.

Suggested guidelines for corrective action to violation levels are, but not limited to, the following:

Level I Violations: Coaching or Verbal/ written warning in addition to policies and procedures retraining

Level II Violations: Written warning, EAP referral, with possible suspension in addition to policies and procedures retraining

Level III Violations: Suspension, in addition to policies and procedures retraining or Termination

These guidelines are not mandatory requirements for disciplinary actions, as numerous factors should be considered when deciding the appropriate level of discipline.

All procedural and substantive requirements found in the Gaston County Personnel Policy apply to any disciplinary action arising from this policy.

PART III: ELECTRONIC PROTECTED HEALTH INFORMATION

Note: For additional technical compliance requirements as well as relevant Information Technology Security Policies, see the Gaston County IT HIPAA Manual.

Policy No: 03-001

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 confidentiality laws and rules are a primary responsibility of Gaston County. All information systems and databases that contain PHI must be registered with or identified by with the Information Technology Department 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 shows 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 (cannot be stored on an individual workstation, i.e. hard drive or unencrypted USB drive)
Requirements	Requirements
Must be registered	Must follow PHI Privacy and Security standards
Must meet all security requirements, including for unsupported operating systems to be replaced; automatic screen locks on applicable computers; ensuring that all computers have current security patches	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, and is the Application Development/GIS Manager. 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. Such end-user requirements, such as those concerns passwords, are found in the Gaston County Personnel Policy and shall be followed. 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. Provided it is technologically possible, there shall be a procedure by Gaston County Information Technology that establishes periodic review of user access logs as well as account roles and privileges to ensure that their level of access is appropriate. Such review shall include administrators and other "super users".

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, or an ad-hoc subcommittee 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.

Security Administration

Purpose: To ensure security of Electronic Protected Health Information.

Policy: This Policy is to be read in conjunction with all Gaston County policies, including those policies pertaining to the Gaston County Information Technology department. To ensure the safeguarding of all ePHI (Electronic Protected Health Information) by following Gaston County's IT HIPAA policies as described below as well as the IT HIPAA Manual for authorization and/ or supervision, workforce member clearance and procedure for terminating workforce member upon termination. These policies will be implemented in part by employing security awareness training for all workforce members, installing commercial grade protection from malicious software/viruses, 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 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.

Additionally, there shall be a periodic review of user access logs as well as account roles and privileges to ensure that their level of access is appropriate. Such review shall include administrators and other "super users." Pursuant to Gaston County Personnel Policy, the accounts for all terminated employees shall be disabled. Such log shall also be created and reviewed for those with temporary access, such as third party vendors. All logs shall be kept for at least 90 days.

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*. All employees must also comply with the email policies as identified in the Gaston County Personnel Policy Manual.

Enforcement: Any employee found to have violated this policy may be subject to disciplinary action as described in this Manual as well as the Gaston County Personnel Policy Manual.

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.