Augusta University
Policy Library

Use and Disclosure of Protected Health Information

Policy Manager: Audit, Compliance, Ethics and Risk Management (ACERM)

POLICY STATEMENT
The Board of Regents of the University System of Georgia (USG) has designated itself a hybrid covered entity under the federal Health Insurance Portability and Accountability Act (HIPAA), comprised of units that perform functions subject to HIPAA requirements and units that do not (Hybrid Entity). In establishing and maintaining Hybrid Entity status, HIPAA requires the USG to designate (i) its units that provide health care services to patients and bill for such services through HIPAA-covered electronic transactions (each a "Covered Component"), and (ii) other departments at the USG providing support to Covered Components in a manner requiring the use or disclosure of protected health information ("PHI") and potentially would be considered a Business Associate of the Covered Component if separate legal entities (each a "Supporting Covered Component"). Collectively, these units are referred to as the Health Care Components (HCC). This designation is used to guide the scope and application of the USG's HIPAA compliance activities to ensure the privacy, security, and proper use and disclosure of PHI.

Pursuant to the Board of Regents of the University System of Georgia policy 7.13 *Designation of USG as a Hybrid Entity Under HIPAA*, "Any portion of USG engaged in a covered function or performing business associate activities for another component of USG engaged in a covered function, as those terms are defined by HIPAA, is hereby deemed part of the Health Care Component (HCC) of the USG Hybrid Entity. The University System Office (USO) and each USG Institution will be responsible for identifying the components, business units, colleges, or schools that are part of the HCC."

In compliance with the above policy, Augusta University (AU) has performed a review and designated specific areas of AU that are considered Health Care Components (HCC). This policy is applicable to all faculty, staff and students studying, working, or practicing in the designated health care components of Augusta University. These individuals and units shall protect the privacy of our patients and research subjects.

AFFECTED STAKEHOLDERS
Indicate all entities and persons within the Enterprise that are affected by this policy:

☒ Alumni ☒ Faculty ☒ Graduate Students ☒ Health Professional Students
☒ Staff ☒ Undergraduate Students ☒ Vendors/Contractors ☐ Visitors
☐ Other:

DEFINITIONS
These definitions apply to these terms as they are used in this policy:

Attestation is a paper or electronic document which verifies that the use or disclosure of PHI is not prohibited by 164.502(a)(5)(iii).

Office of Legal Affairs Use Only
Executive Sponsor: VP for Audit, Compliance, Ethics and Risk Management
Next Review: 5/2026

Business Associate. A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of or provides services to a covered entity. (A member of the covered entity's workforce is not a business associate. A covered healthcare provider, health plan, or healthcare clearinghouse can be a business associate of another covered entity). A business associate is liable for their own HIPAA violations.

"Billing records" shall mean patient statements, records of payment by the patient or their payer, and claims adjudication records.

Covered entity shall mean:

1) A health plan.
2) A health care clearinghouse.
3) A health care provider who transmits any health information in electronic form in connection with a covered transaction (payment, claim status, or authorizations for treatment).

"Disclosure" shall mean the release, transfer, or divulging of protected health information outside of Augusta University.

Designated Record Set. The designated record set shall include the following regardless of the medium in which they are stored:

- Medical records and billing records about individuals maintained by or for a covered health care provider.
- Enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
- Other records that are used, in whole or in part, by or for the covered entity to make decisions about individuals. This last category includes records that are used to make decisions about any individual, whether the records have been used to make a decision about the particular individual requesting access.

Records Excluded. The designated record set shall exclude records of quality assurance activities; records of peer and medical review activities; records prepared in anticipation of litigation; records of risk management and compliance activities; birth and death registries; cancer registry information; source data, such as raw data from psychological and neuropsychological tests, radiological films and images, videotapes, monitoring strips, provided that a professional interpretation or report of the source data is included in the record; research records that are not placed in the medical record; health information in Human Resources records; appointment or surgical schedules; and law enforcement investigations, unless these records are used to make decisions regarding the patient. The designated record set shall also exclude psychotherapy notes, and all records required to be kept from the patient by law, such as those records maintained subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, unless exempted from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2).

Health care components. University units that provide health care services to patients and bill for such services through HIPAA-covered electronic transactions and those units that support the provision of health care and billing services.

"Health care operations" are any of the following activities of the covered entity:

1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities.

3) Except as prohibited under § 164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable.

4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs.

5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

6) Business management and general administrative activities of the entity, including, but not limited to:
    a. Management activities relating to implementation of and compliance with the requirements of this subchapter.
    b. Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.
    c. Resolution of internal grievances.
    d. The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and

e. Consistent with the applicable requirements of § 164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

Health oversight agency means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Health records. All records identifiable to an individual patient are collected, created, or used for the provision of health care, except as excluded below. Examples include discharge summaries, progress notes, advance directives, consent forms, and medication records. Health records shall also include all health records obtained from another entity if those records are filed in the patient's record for use in health care decisions. Health records shall also include records created by business associates that meet the definition of "health records" in this policy, and that are not duplicated in the Augusta University patient record.

Hybrid entity means a single legal entity:
(1) That is a covered entity;
(2) Whose business activities include both covered and non-covered functions; and
(3) That designates health care components in accordance with paragraph § 164.105(a)(2)(iii)(D).

Limited Data Set. A limited data set is protected health information from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed.

Marketing. A communication about a product or service that encourages recipients of the communication to purchase or use the product or service. Marketing does not include communication made:

1) to provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by AU in exchange for making the communication is reasonably related to the covered entity's cost of making the communication.

2) for the following treatment and health care operations purposes, except where AU receives financial remuneration in exchange for making the communication:

a. for treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual:

b. to describe a health-related product or service (or payment for such product or service) that is provided by AU making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or

services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or

c. for case management or care coordination, contacting individuals with information about treatment alternatives and related functions to the extent these activities do not fall within the definition of treatment.

Organized Health Care Arrangement (OHCA) is an organized system of health care in which more than one covered entity participates and in which the participating covered entities hold themselves out to the public as participating in a joint arrangement and participate in certain joint activities.

Psychotherapy notes shall mean the notes recorded by a mental health professional reflecting the contents of communications during a counseling session, provided these records are kept separate from the patient's full health record. "Psychotherapy notes" shall not mean medication records, counseling start and stop times, the modalities and frequency of treatment, test results, summaries of a patient's diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date.

Payment encompasses activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for health care delivered to an individual[21] and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual.

Personal Representative is the person with legal authority to make healthcare decisions on behalf of the individual.

Protected Health Information (PHI). Health information transmitted or maintained in any form by a covered entity or its business associate that:

- Relates to the past, present, or future physical or mental health condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provisions of health care to an individual; and
- Identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual; and
- Is not an educational record (as defined the Family Educational Rights and Privacy Act, 20) U.S.C. 1232g, or excluded under 20 U.S.C. 1232g (a)(4)(B)(iv); and
- Is not an employment record.

A **"record"** is any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity.

Treatment is the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another.[20]

Use. The sharing, utilization, or analysis of protected health information by Augusta University faculty, staff and students.

TABLE OF CONTENTS

PROCESS & PROCEDURES

1.0 Uses and Disclosures of PHI Which Do Not Require Authorization 45 CFR 164.506 ("Permitted" Uses of PHI)

In general, Augusta University may use and disclose a patient's PHI without authorization for the following purposes:

1. To the individual that is the subject of the information.
2. AU may use and disclose PHI for treatment, payment, or healthcare operations activities.
3. When an opportunity to agree or object is given and there is no objection, in certain circumstances (see section 2.0 below).
4. Incident to an otherwise permitted use and disclosure.
5. For the public interest and benefit activities; and
6. Limited data sets for the purpose of research, public health, or healthcare operations

1.1 Incidental Use and Disclosure

The Privacy Rule does not require that every risk of an incidental use or disclosure of PHI be eliminated. A use or disclosure of this information that occurs as a result of, or as "incident to," an otherwise permitted use or disclosure is permitted as long as the covered entity has adopted reasonable safeguards as required by the Privacy Rule, and the information being shared was limited to the "minimum necessary," as required by the Privacy Rule.

1.2 Minimum Necessary Standard

AU's workforce members will only be allowed access to information (electronic and/or paper) reasonably needed to perform their job functions.

- The Privacy Officer, in consultation with the human resources department, system owner, the Security Officer, and other appropriate Individuals, will oversee the assignment of data classifications of any PHI that AU may create, receive, maintain, or transmit. The classification will take into account specific workforce job responsibilities, data classifications, the related need to access, modify, change, or dispose of information, and the sensitivity of the health information.
- To the extent reasonably practicable, AU will use technological controls to limit access to PHI to the amount necessary for Workforce members to perform their job functions.
- The designated IT manager is responsible for ensuring that appropriate and timely changes are made for any and all Workforce members who experience a change in responsibility in order to ensure that appropriate access to personal health information is maintained.
- Licensed practitioners who are involved in an individual's treatment may be given access to all portions of the individual's medical record.
- Especially sensitive information, such as mental health information or test results for sexually transmitted diseases, will be stored, maintained and transmitted separately from the rest of the PHI in an individual's medical record in order to limit unauthorized access.

- Supervisors are responsible for assigning appropriate access to PHI for each Workforce member under their direct supervision and submitting a signed change in responsibility form to the designated IT manager whenever a Workforce member is newly hired, changes job responsibilities, or is terminated.

2.0 Uses and Disclosures of PHI Requiring an Opportunity to Agree or Object (45 CFR 164.510)

2.1 Uses and Disclosures for Notification Purposes

- Unless the Individual has specified otherwise AU may disclose to a family member, other relative, or a close friend of the Individual, or any other person identified by the Individual or his/her Personal Representative, the PHI directly relevant to such person's involvement with the Individual's care or payment for care.
- AU may use or disclose PHI to notify or assist in the notification of (including identifying or locating), a family member, a Personal Representative of the Individual, or another person responsible for the care of the Individual, of the Individual's location, general condition, or death.
- Unless the Individual has specified otherwise or disclosure is prohibited AU may disclose to a family member, or other persons who were involved in the Individual's care or payment for health care prior to the Individual's death, PHI that is relevant to such person's involvement with the Individual. An exception applies when a restriction request or confidential communication has been made by the Individual and granted.

2.2 Uses and Disclosures to Persons Involved in the Individual's Care with the Individual Present

If the Individual is present for, or available prior to, a use or disclosure of PHI, and has the capacity to make health care decisions, AU may use or disclose the PHI if it:

- It obtains the Individual's agreement,
- It provides the Individual with the opportunity to object to the disclosure, and the Individual does not express an objection, or
- The AU Privacy Officer, or designee, reasonably infers from the circumstances, based on the exercise of professional judgment that the Individual does not object to the disclosure.

2.3 Limited Uses and Disclosures to Persons Involved in the Individual's Care When the Individual is Not Present

If the Individual is not present or not capable of agreeing or objecting (for example, in the case of an emergency), the AU Privacy Officer or, designee, may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the Individual and, if so, disclose only PHI that is directly relevant to the person's involvement with the Individual's care or payment related to the Individual's health care or needed for notification.

3. 0 Uses and Disclosures for Which Consent, an Authorization, or Opportunity to Agree or Object is Not Required (45 CFR 164-512(a))

All disclosures are subject to the minimum necessary standard and require an accounting of disclosures, unless accompanied by a valid Authorization. Prior to the disclosure the workforce member should verify the identity and authority of the person(s) making the request.

3.1 Required by law

- State and federal laws and regulations mandate certain uses or disclosures of PHI. If the law or regulation can be enforced by an official government agency, it is deemed to be required by law. This does not include private contractual agreements between parties.
- If an AU Workforce member becomes aware of any situation in which disclosure of an Individual's PHI may be required by any state or federal law or regulation, the Workforce member will immediately forward the request to AU's Legal Counsel.
- Legal counsel, the Privacy Officer, or Designee are the only people that can disclose PHI pursuant to this type of request. Workforce members should not disclose PHI, unless specifically instructed to do so by Legal Counsel or the Privacy Officer.

3.2 Judicial and Administrative Proceedings

- Any AU Workforce member who receives any Legal Process Documents (e.g., court-ordered or attorney-issued subpoenas) will immediately notify and forward these documents to AU's Legal Counsel.
- AU's Legal Counsel or Privacy Officer will review the request and determine the permissibility of the disclosure of PHI in accordance with this Policy.
- To the extent permitted by applicable state law, PHI may be released in response to a valid court order signed by a judge or an order from an administrative tribunal without additional supporting documents.
- PHI may not be released in response to an attorney-issued subpoena or discovery request unless one of the following circumstances applies:
    - The Individual provides a written and dated Authorization to release the information to the requesting party.
    - The subpoena requires the PHI to be disclosed for law enforcement or investigation purposes, and meets the requirements of including grand jury subpoenas and subpoenas issued by government attorneys on behalf of local, state, and federal enforcement agencies; or
    - Legal Process Documents not accompanied by an order of a court or administrative tribunal include the following:
        - Satisfactory Assurance from the party seeking the information that reasonable efforts have been made to ensure that the Individual who is the subject of the PHI has been given notice of the request; or
        - Satisfactory Assurance from the party seeking the information that reasonable efforts have been made to secure a qualified protective order as required by law. AU will be deemed to have received

satisfactory assurances from the entity seeking the PHI if it receives a written statement and accompanying documentation demonstrating that:
    - The party requesting PHI has made a good faith attempt to provide written notice to the Individual or, if the Individual's location is unknown, to mail a notice to the Individual's last known address;
    - The notice included sufficient information about the litigation or proceeding in which the PHI is requested to permit the Individual to raise an objection to the court or administrative tribunal and;
    - The time for the Individual to raise objections to the court or administrative tribunal has elapsed and;
    - No objections were filed; or
    - All objections filed by the Individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such a resolution.
  - AU may disclose PHI in response to lawful process without receiving satisfactory assurance if AU makes reasonable efforts to provide notice to the Individual or to seek a qualified protective order.
- Scope of Disclosure. Only the information expressly authorized by the order or requested by the subpoena or court order will be released.
- Legal Counsel, the Privacy Officer, or Designee are the only people that can disclose PHI pursuant to this type of request. Workforce members should not disclose PHI, unless specifically instructed to do so by Legal Counsel or the Privacy Officer.

3.3 Law Enforcement Purposes

Law enforcement agencies and officials may be provided with PHI only in accordance with this policy.

- Any AU Workforce member who receives any Legal Process Documents (e.g., warrant, subpoena) will immediately notify and forward these documents to AU's Legal Counsel. AU's Legal Counsel or Privacy Officer will review the request and determine the permissibility of the disclosure of PHI in accordance with this Policy. Only under exigent circumstances will any Workforce member who believes that a disclosure may be appropriate or required under this Policy will make any disclosures of PHI and only after all efforts to reach Legal Counsel and the Privacy Officer have been exercised.
- PHI may be disclosed to law enforcement agencies to make reports that are required by law, such as to report abuse.
- As a part of AU's legal responsibilities, AU may disclose PHI to law enforcement officials in response to a legal process or summons, as follows:
    - To comply with a court order or court-ordered warrant ordering disclosure to the law enforcement agency.
    - To comply with a subpoena or summons issued by a grand jury, judicial officer, or a private attorney.

  - Pursuant to an official administrative request from a law enforcement agency (for instance, the Bureau of Alcohol, Tobacco, and Firearms) provided that:
  - The PHI requested is relevant and material to a legitimate law enforcement inquiry.
  - The request is specific and limited in scope to an extent reasonably practicable in light of the purpose for which the information is sought, a
  - De-identified information could not be reasonably used.
- AU may provide PHI to law enforcement agencies and officials who are attempting to identify or locate a suspect, fugitive, material witness, or missing person. The PHI may be provided in response to requests by a properly identified law enforcement officer or in response to a public bulletin issued by a law enforcement agency.
  - Only the following information about the Individual may be provided:
    - Name and address
    - Date and place of birth
    - Social security number
    - ABO blood type and rh factor
    - Type of injury
    - Date and time of treatment
    - Date and time of death (if applicable) and
    - Description of any distinguishing physical characteristics including height, weight, gender, race, hair and eye color, facial hair, scars, and tattoos.
  - No information related to DNA or a DNA analysis, dental records, samples or analysis of body fluids or tissues, or any other information beyond the information listed above will be disclosed unless the law enforcement officer presents a warrant, subpoena, or court order meeting the requirements of Section 3, above.
- Victims of Crime. If the Individual is suspected of being the victim of an alleged crime, PHI may be disclosed upon request of a law enforcement official. The Privacy Officer, or designee, is responsible for reviewing the circumstances and determining whether disclosure will be made as follows:
  - A conscious, competent Individual will be asked for permission to disclose PHI to law enforcement officials. The Privacy Officer, or designee, will document in the Individual's Electronic Health Record or other record, the time, date, and name of the persons who witnessed the Individual's agreement or refusal which may be oral or in writing. The Privacy Officer, or designee, will, if possible, obtain a valid Authorization signed by the Individual.
  - If the Individual is not competent, the Individual's Personal Representative may agree orally or in writing to the disclosure of the Individual's PHI. The Personal Representative's agreement will be documented in the Individual's Electronic Health Record or other record. If no Personal Representative is available, the AU Privacy Officer, or designee, will try to find a family member of the Individual who may agree to contact law enforcement officials directly. In an emergency, or when no Personal Representative or family member of an Individual is available, the PHI may be disclosed by the Privacy Officer, or designee, only if the law enforcement officer signs the statement and either the Privacy Officer, or designee, or the Individual's attending physician determine that disclosure is in the Individual's best

interests. The determination will be documented in the Individual's Electronic Health Record or other record.

- AU may disclose suspicious deaths, including related PHI, to law enforcement agencies and officials, if the death is suspected of being the result of criminal conduct. The Privacy Officer, or designee, is responsible for reviewing the circumstances and determining whether disclosure will be made.
- AU may disclose evidence of suspected criminal conduct occurring on AU's premises, including related PHI, to law enforcement agencies and officers. The Privacy Officer, or designee, is responsible for reviewing the circumstances and determining whether disclosure will be made.
- If AU provides emergency health care in response to a medical emergency, other than such emergency on the premises, AU may disclose PHI to a law enforcement official if such disclosure appears necessary to alert law enforcement to:
    - The commission and nature of a crime.
    - The location of such crime or of the victim(s) of such crime; and
    - The identity, description, and location of the perpetrator of such crime.
- Legal Counsel, the Privacy Officer, or Designee are the only people that can disclose PHI pursuant to this type of request. Workforce members should not disclose PHI, unless specifically instructed to do so by Legal Counsel or the Privacy Officer.
- Before disclosing PHI to a law enforcement officer or agency, the officer or agency's identity and authority will be verified and documented. If the person is a police officer, AU's Workforce members will ask to see his or her badge and record the badge number. For persons who do not have a badge, AU's Workforce members will obtain their business card or other proof of their credentials. All requests received in writing must be on official letterhead.

3.4 Victims of Abuse, Neglect, or Domestic Violence

- If, during the course of delivering services directly to Individuals, AU's Workforce members receive reports of suspected or confirmed abuse, neglect or domestic violence (even if the report does not involve the Individual), the Workforce member will immediately notify AU's Legal Counsel.
- AU may disclose PHI about an Individual that it reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence:
- To the extent the disclosure is required by law and the disclosure complies with, and is limited to, the relevant requirements of such law.
    - If the Individual agrees to the disclosure (the agreement may be given orally as long as it is documented in the Individual's Health Profile); or
    - To the extent the disclosure is expressly authorized by statute or regulation and:
    - AU, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the Individual or other potential victims; or
    - If the Individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PHI for which disclosure is sought is not intended to be used against the Individual and that an immediate enforcement activity that depends upon the disclosure would be

materially and adversely affected by waiting until the Individual is able to agree to the disclosure.

- If AU makes a disclosure, it must promptly inform the Individual that such a report has been or will be made, unless in the documented professional opinion of a licensed professional affiliated with AU, informing the Individual would place the Individual at risk of serious harm.
- AU may elect not to treat a person as the **Personal Representative** of an Individual if AU has a reasonable belief that the Individual has been or may be subjected to domestic violence, abuse, or neglect by the Personal Representative.
- AU's Workforce member will document the following details of all abuse, neglect and/or domestic violence allegations and notify the Privacy Officer which will ensure that the information is entered into the Individual's Health Profile:
    - Information received that indicates evidence of abuse or neglect.
    - In cases of suspected or confirmed adult abuse, neglect or domestic violence, the Workforce member's efforts to encourage the Individual or the Individual's caregiver to seek safety and/or contact a local agency; and
    - Information regarding reporting to state and/or federal agencies.

3.5 Health Oversight Activities

- AU's Privacy Officer will, in consultation with Legal Counsel, make the determination of whether PHI will be disclosed for public health activities to:
    - A Public Health Authority or, at the direction of a Public Health Authority, to an official of a foreign government agency that is acting in collaboration with a domestic Public Health Authority.
    - A Public Health Authority or other appropriate 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) with respect to an FDA regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness; such purposes include:
        - To collect or report adverse events, product defects or problems (such as the use or labeling of a product),
        - or biological product deviations.
        - To track FDA-regulated products.
        - To enable product recalls, repairs, or replacement, or lookback (including locating and notifying Individuals who have received such products); or
        - To conduct post marketing surveillance.
    - A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition if AU or a Public Health Authority is authorized by law to notify such person as necessary in the conduct of an intervention or investigation.
    - An employer, about an Individual who is a member of the employer's Workforce if:

        - AU is a Health Care Provider who is also a member of the Workforce of such employer or who provides Health Care to the Individual at the request of the employer:
            - To conduct an evaluation relating to medical surveillance of the workplace; or
            - To evaluate whether the Individual has a work-related illness or injury.
    - The PHI that is disclosed consists of findings concerning a work-related illness or injury or a workplace related medical surveillance.
    - The employer needs such findings in order to comply with its obligations, under federal or state law, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and
    - AU provides written notice to the Individual that PHI relating to the medical surveillance of the workplace and work-related illnesses and injuries will be disclosed to the employer:
    - A school, about an Individual who is a student or prospective student of the school, if:
        - The PHI disclosed is limited to proof of immunization.
        - The school is required by state or other law to have such proof before admitting the Individual; and
        - AU's Privacy Officer obtains and documents the agreement to the disclosure from either the Individual (if an adult or emancipated minor) or the parent, guardian or other person in loco parentis.
        - AU will document the agreement.

3.6 Public Health Activities

AU's Privacy Officer will, in consultation with Legal Counsel, make the determination of whether PHI will be disclosed for public health activities to:

- A Public Health Authority or, at the direction of a Public Health Authority, to an official of a foreign government agency that is acting in collaboration with a domestic Public Health Authority.
- A Public Health Authority or other appropriate 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) with respect to an FDA regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness; such purposes include:
    - To collect or report adverse events, product defects or problems (such as the use or labeling of a product), or biological product deviations.
    - To track FDA-regulated products.
    - To enable product recalls, repairs, or replacement, or lookback (including locating and notifying Individuals who have received such products); or
    - To conduct post marketing surveillance.

- A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition if AU or a Public Health Authority is authorized by law to notify such person as necessary in the conduct of an intervention or investigation.
- An employer, about an Individual who is a member of the employer's Workforce if:
    - AU is a Health Care Provider who is also a member of the Workforce of such employer or who provides Health Care to the Individual at the request of the employer:
    - To conduct an evaluation relating to medical surveillance of the workplace; or
    - To evaluate whether the Individual has a work-related illness or injury.
    - The PHI that is disclosed consists of findings concerning a work-related illness or injury or a workplace related medical surveillance.
    - The employer needs such findings in order to comply with its obligations, under federal or state law, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and
    - AU provides written notice to the Individual that PHI relating to the medical surveillance of the workplace and work-related illnesses and injuries will be disclosed to the employer:

- A school, about an Individual who is a student or prospective student of the school, if:
    - The PHI disclosed is limited to proof of immunization.
    - The school is required by state or other law to have such proof before admitting the Individual; and
    - AU's Privacy Officer obtains and documents the agreement to the disclosure from either the Individual (if an adult or emancipated minor) or the parent, guardian or other person in loco parentis.
    - AU will document the agreement.

3.7 Decedents

- AU will continue to protect the PHI and ensure that the appropriate disclosures requirements are followed for a period of 50 years following the death of the individual if the records are retained for that period of time.
- AU's Privacy Officer, or designee, may disclose PHI of a decedent to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. If AU performs the duties of a coroner or medical examiner, it may use PHI for the purposes described in this paragraph.
- AU's Privacy Officer, or designee, may disclose the PHI of a decedent to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors to carry out their duties, AU may disclose the PHI prior to, and in reasonable anticipation of, the Individual's death.
- AU's Privacy Officer, or designee, may disclose PHI about a decedent to a law enforcement official for the purpose of alerting law enforcement of the death of the Individual if AU has a suspicion that such death may have resulted from criminal conduct.

- AU's Privacy Officer, or designee, may disclose to a family member or others who were involved in the Individual's care before their death, relevant PHI after their death, unless doing so is inconsistent with the Individual's previously expressed preference.
- AU's Privacy Officer, or designee, may disclose PHI about a decedent for research purposes if certain representations are obtained.

3.8 Cadaveric Organ, Eye, or Tissue Donation

Covered entities may use or disclose protected health information to facilitate the donation and transplantation of cadaveric organs, eyes, and tissue.

3.9 Research

Augusta University's use of PHI for research purposes shall be strictly limited to that information required to fulfill the stated purposes of the approved study. Disclosure of such information shall be limited to those individuals who are authorized by the approved study to have access to such information. AU is permitted to use and disclose protected health information for approved research purposes, without an individual's authorization, provided the covered entity obtains either:

1. Documentation that an alteration or waiver of individuals' authorization for the use or disclosure of protected health information about them for research purposes has been approved by an Institutional Review Board or Privacy Board;
2. Representations from the researcher that the use or disclosure of the protected health information is solely to prepare a research protocol or for similar purpose preparatory to research, that the researcher will not remove any protected health information from the covered entity, and that protected health information for which access is sought is necessary for the research; or
3. Representations from the researcher that the use or disclosure sought is solely for research on the protected health information of decedents, that the protected health information sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is sought.

A covered entity also may use or disclose, without an individuals' authorization, a **limited data set** of protected health information for research purposes.

3.10 Limited Data Set

AU may use or disclose a limited data set for research, health care operations, and public health purposes, provided the recipient enters into a data use agreement promising specified safeguards for the protected health information within the limited data set.

Data use agreements must be reviewed by the Privacy Officer or delegate if an approved standardized template is not used.

3.11 Serious Threat to Health or Safety

AU may use or disclose PHI, if AU, in good faith, believes the use or disclosure:

- If it is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and
- If it is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or
- Is necessary for law enforcement authorities to identify or apprehend an Individual:
    - Because of a statement by an Individual admitting participation in a violent crime that AU reasonably believes may have caused serious physical harm to the victim; or
    - Where it appears from all the circumstances that the Individual has escaped from a correctional institution or from lawful custody.
- A use or disclosure may not be made if the information is learned by AU:
    - In the course of treatment to affect the propensity to commit criminal conduct that is the basis for the disclosure, or counseling or therapy; or
    - Through a request by the Individual to initiate or to be referred for the treatment, counseling, or therapy.
- An AU Workforce member who believes that disclosure of PHI would avert a serious threat to health or injury should notify the AU Privacy Officer immediately.
- The AU Privacy Officer will, in consultation with Legal Counsel, determine the extent of and permissibility for disclosures of PHI for these purposes.
- AU is presumed to have acted in good faith with regard to a belief, if the belief is based upon AU's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

3.12 Essential Government Functions

An authorization is not required to use or disclose protected health information for certain essential government functions. Such functions include assuring proper execution of a military mission, conducting intelligence and national security activities that are authorized by law, providing protective services to the President, making medical suitability determinations for U.S. State Department employees, protecting the health and safety of inmates or employees in a correctional institution, and determining eligibility for or conducting enrollment in certain government benefit programs.

3.13 Worker's Compensation

- AU may disclose PHI as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.
- AU's Privacy Officer, in consultation with Legal Counsel, will determine the extent of and permissibility for disclosures of PHI for these purposes.
- Disclosure pursuant to a court ordered subpoena signed by a workers' compensation judge is permissible.

4.0 Uses and Disclosures of PHI Requiring Authorization or Attestation

AU Workforce members will obtain the individual's valid and written authorization (see 4.6 "Valid Authorization and Attestation") for any use or disclosure of protected health information that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule. The following uses and disclosures require valid authorization:

4.1 Psychotherapy Notes

AU Workforce will obtain an individual's authorization to use or disclose psychotherapy notes with the following exceptions:

- The covered entity who originated the notes may use them for treatment.
- A covered entity may use or disclose, without an individual's authorization, the psychotherapy notes, for its own training, and to defend itself in legal proceedings brought by the individual, for HHS to investigate or determine the covered entity's compliance with the Privacy Rules, to avert a serious and imminent threat to public health or safety, to a health oversight agency for lawful oversight of the originator of the psychotherapy notes, for the lawful activities of a coroner or medical examiner or as required by law.

4.2 Use of PHI for Marketing and Media Relations

Marketing is any communication about a product or service that encourages recipients to purchase or use the product or service.

Except for activities permitted by the OHCA's policies, no division or unit of Augusta University shall use health information for marketing or fundraising without the approval of the Privacy Officer. Most marketing communications involving the use of PHI about patients cannot be made without first obtaining the patient's written authorization. Patient information or lists will not be used or released for fundraising purposes without obtaining an appropriate authorization.

A patient's written authorization to use and disclose his/her PHI is not required for face-to-face communications between the patient and their health care provider, e.g., giving the patient a product sample, or advising them of a potential research study.

The Privacy Rule carves out the following health-related activities from this definition of marketing:

- Communications to describe health-related products or services, or payment for them, provided by or included in a benefit plan of the covered entity making the communication.
- Communications about participating providers in a provider or health plan network, replacement of or enhancements to a health plan, and health-related products or services available only to a health plan's enrollees that add value to, but are not part of, the benefits plan.
- Communications for treatment of the individual; and

- Communications for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or care settings to the individual.

4.3 Use & Disclosure of PHI for Media Relations

Augusta University's Public Relations Office will not disclose protected health information without authorization from the patient or their authorized representative. Inquiries regarding patients receiving care at AU shall be referred to AU's Public Relations Office.

4.4 Sale of PHI

Selling PHI is generally prohibited unless the patient signs an authorization specifically permitting the sale. This includes any disclosure of PHI where Augusta University directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI.

Sale of PHI does not include certain disclosures of PHI:

- For public health purposes
- For research purposes where the only remuneration received by Organization is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purposes
- For treatment and payment purposes
- To a business associate for activities that the business associate undertakes on AU or AU's affiliates (if such business associate executes a Business Associate Agreement with AU)
- To an Individual who is requesting access to their own PHI
- As required by law; and
- For any other HIPAA permitted purpose where the only remuneration received by Organization is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee otherwise expressly permitted by other law. The reasonable cost-based fee includes both direct and indirect costs for generating, storing, retrieving and transmitting the PHI, including labor, material and supplies.

De-identified data is not PHI and therefore is not subject to the remuneration prohibition. However, limited data sets are PHI and are subject to this provision (see the section on Limited Data Set).

4.5 Attestation for PHI Related to Reproductive Health

AU Workforce will not use or disclose protected health information for any of the following activities, without obtaining a valid attestation:

1) To conduct a criminal, civil, or administrative investigation into any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care.
2) To impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care.

3) To identify any person for any purpose described in paragraphs (a)(5)(iii)(A)(*1*) or (*2*) of 45 CFR 164.502

4.6 Valid Authorization and Attestation

A valid authorization must contain at least the following elements:

I. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.
II. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.
III. The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.
IV. A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.
V. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository.
VI. (Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.

A valid attestation is a document that meets the following requirements:

I. A description of the information requested that identifies the information in a specific fashion, including one of the following:
    a. The name of any individual(s) whose protected health information is sought, if practicable.
    b. If including the name(s) of any individual(s) whose protected health information is sought is not practicable, a description of the class of individuals whose protected health information is sought.
II. The name or other specific identification of the person(s), or class of persons, who are requested to make the use or disclosure.
III. The name or other specific identification of the person(s), or class of persons, to whom the covered entity is to make the requested use or disclosure.
IV. A clear statement that the use or disclosure is not for a purpose prohibited under § 164.502(a)(5)(iii).
V. A statement that a person may be subject to criminal penalties pursuant to 42 U.S.C. 1320d-6 if that person knowingly and in violation of HIPAA obtains individually identifiable health information relating to an individual or discloses individually identifiable health information to another person.
VI. Signature of the person requesting the protected health information, which may be an electronic signature, and date. If the attestation is signed by a representative of the person requesting the

information, a description of such a representative's authority to act for the person must also be provided.

The attestation must be written in plain language.

AU's Privacy Office must verify that attestation and authorizations meet the requirements established by this policy.

5.0 Use of PHI for Educational Purpose

5.1 Internal Use

Only the minimum necessary PHI required to achieve the learning objectives in the clinical environment may be shared within AU and AU-affiliated learners. Also, AU teachers and learners must use discretion when discussing a patient's condition during rounds, speaking quietly and avoiding conversations in public areas where patients, families and other persons are present.

5.2 External Use

Disclosure of PHI external to AU is not permitted for any reason, including for professional meetings, conferences, and lectures, etc. absent a patient's written authorization for this specific use. Patient identifiers must be removed in external educational presentations (such as in-house case presentations attended by non-affiliated physicians, visiting clinicians, non-enrolled students, etc.) rendering it acceptable for use in these settings (i.e., it is no longer PHI once de-identified).

Photographs, Video, other Patient Images (radiological, ultrasound) and Non-Textual Patient Data (physiologic tracings, slides, etc.)

Written consent from the patient is required using the official AU consent form if either of the following criteria applies:

1) The patient data is determined to be data that a patient would recognize as their own, or
2) The patient data has NOT been de-identified under HIPAA standards.

6.0 Other Requirements Relating to Uses and Disclosures of PHI

6.1 Verification of Identity and Authority

Workforce members will comply with the following procedures regarding identification and authority of Individuals, Personal Representatives, caregivers, Health Care Providers, and others (e.g., Public Official) requesting PHI.

- Prior to making a disclosure of PHI to a third party that is permitted by these procedures, an AU Workforce member will verify the recipient's identity and authority to receive the PHI.
    - If these policies and procedures require any documentation, statements, or representations from the intended recipient (such as a subpoena) as the basis for, or condition of, allowing a disclosure, AU will obtain such documentation, statements, or representations prior to making the disclosure.
    - Reliance on Documentation. If reasonable under the circumstances, AU may rely on documentation, statements, or representations that, on their face, meet the requirements for disclosure.

Types of Requestors:

- Individual Requests
    - Written Communications: AU Workforce member will verify that the communication received is signed by the Individual or if an email, contains the Individual's name in the email address.
    - Inbound Calls: Minimum requirements for Individual identification will be based on the Individual's ability to provide the following identifiers:
        - The Individual's name
        - The Individual's date of birth
        - The Individual's home address
        - The Individual's telephone number

- Individual's Personal Representative.
    - AU will accept written or verbal communication from the Individual notifying AU of the designation of a Personal Representative who has the authority under state law, by advance directive, health care proxy, or otherwise, to make health care decisions.
    - Upon notification of designation of a Personal Representative, a Workforce member of AU will document the personal representative in the patient's medical record.

- Caregiver. The minimum requirements for verifying the identity of a Caregiver approved to discuss an Individual's plan of care is based on documentation provided by the Individual.

- Health Care Provider.
    - Before AU's Workforce members may speak with a Health Care Provider regarding an Individual's PHI, the Health Care Provider or the Provider's workforce members must be able to provide the following information before PHI is shared:
        - Name of office workforce member placing telephone call (including position and title)
        - Individual's full name
        - Individual's date of birth
        - Health Care Provider's first and last name
        - Health Care Provider's office address
        - Health Care Provider's office telephone number

- Public Officials.
    - When a government agency or public official requests PHI, AU's Workforce members may rely upon the following to verify their identity, if reliance is reasonable under the circumstances:
        - For in-person requests: The official's presentation of an agency identification badge, other official credentials, or other proof of government status.
        - For written requests: The request if it is on appropriate government letterhead and identifies the identity of the requestor and their authority to receive PHI.
        - For requests made by someone acting on behalf of a government official: Evidence or documentation that establishes that the person is acting on behalf of the public official, such as a written statement on appropriate government letterhead that the person is acting under the government's authority, a contract for services, a memorandum of understanding, or a purchase order.
    - Only Legal Counsel, the Privacy Officer, and those Workforce members specifically identified and documented by AU's Privacy Officer have the authority to disclose PHI pursuant to this section.

6.2 Verification of Others Requesting PHI

If AU's receive requests from others not covered in this policy, the request will be forwarded to AU's Privacy Officer or Legal Counsel for verification of identity and authority.

6.3 Inability to Verify

If AU's Workforce members are unable to verify a requestor's identity and authority, PHI will not be disclosed. The request will be forwarded to the Privacy Officer to provide further assistance in verifying authority and identity.

6.4 Permission to Leave Messages with PHI

If the Individual has not expressly given his or her permission to leave PHI messages on an answering system, AU's Workforce members will only leave messages that include the Workforce member's name, AU's name and AU's telephone number.

- **Required Disclosures of Protected Health Information**

A covered entity is required to disclose protected health information to individuals (or their personal representatives) when they request access to, or an accounting of disclosures of their protected health information.

7.1 Department of Health and Human Services (HHS)

AU is required to disclose PHI in its possession to the Department of Health and Human Services (HHS) when HHS is undertaking a compliance investigation or review or enforcement action by:

- Providing records and compliance reports
- Cooperating with complaint investigations and compliance reviews
- Permitting access to information

8.0 Personal Representatives

8.1 Competent Adult or Emancipated Minor

A competent adult or emancipated minor who does not suffer from mental incapacity has authority to exercise his or her rights regarding the use or disclosure of PHI. A Personal Representative, who has authority under state law to make health care decisions on behalf of an Individual, may also exercise the Individual's privacy rights, on behalf of the Individual.

8.2 Exceptions

Under the following certain limited circumstances, AU may elect not to recognize the rights of a Personal Representative with respect to the privacy rights of the Individual. If AU has a reasonable belief that:

- The Individual has been or may be subjected to domestic violence, abuse, or neglect by the Personal Representative; or
- Treating such person as the Personal Representative could endanger the Individual; and
- In the documented professional opinion of a licensed professional affiliated with AU, it is not in the best interest of the Individual to treat the person as the Individual's Personal Representative, or that the provision of access by such Personal Representative to PHI, is reasonably likely to cause substantial harm to the Individual or another person.

8.3 Deceased Individuals

In the event that an Individual is deceased, a personal representative can obtain information and access to the deceased Individual's PHI so long as the request is submitted with documentation that supports the person's legal authority to act on behalf of the decedent or the estate (not restricted to persons with authority to make health care decisions), such as:

- Executor
- Administrator
- Legally authorized by a court or by state law; or
- Intestate succession

It is important to note that a power of attorney is no longer valid once the Individual is deceased and no longer represents the authority to act.

8.4 Parent as the Caregiver

When the Caregiver is the parent, the Workforce member will communicate with the parent, unless another Individual provides written evidence to the Workforce member that he or she is the Minor's legal guardian and Personal Representative.

Minor less than thirteen (13) years of age:

- If the unemancipated Minor is less than thirteen (13) years of age, then the Workforce member will speak with the Personal Representative unless the Personal Representative asks the Workforce member to speak directly with the Minor.
- If the Personal Representative withdraws their verbal consent for the Workforce member to speak with the Minor, the Workforce member will cease communication with the Minor.
- The Workforce member will verbally inform the Minor that information shared during any communication may be conveyed to the Minor's Personal Representative.
- The Workforce member will document any PHI obtained during communications with the Minor in the Minor's Electronic Health Record or other record, as appropriate.

Minor between the ages of thirteen (13) and eighteen (18), and is an unemancipated Minor:

The Workforce member will speak with the Personal Representative unless the following exceptions apply:

- When an unemancipated Minor has the authority under state law to consent to treatment without parental notification, with respect to PHI pertaining to a health care service;
- The Minor consents to such health care service and:
    - No other consent to such health care service is required by law regardless of whether the consent of another person has also been obtained; and
    - The Minor has not requested that a person be treated as the personal representative;
- The Minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting in loco parentis, and the Minor, a court, or another person authorized by law consents to such health care service; or

- A parent, guardian, or other person acting *in loco* parentis assents to an agreement of confidentiality between a health care provider and the Minor with respect to such health care service.

8.5 Consultation with Legal Counsel

Consult with Legal Counsel, as necessary, regarding state laws pertaining to a Minor's ability to consent to treatment. If the Individual is eighteen (18) years of age or older or otherwise is considered an adult under state law, the Individual will be treated as an adult.

8.6 Notification of Designation

- AU's HIM department will document the designation of a personal representative in the Individual's Electronic Health Record or other record.
- Upon receipt of a valid notification from an Individual that they no longer wish to designate a previously designated Personal Representative, the HIM department will update the Individual's Electronic Health Record or other record marking the Personal Representative's information as "inactive" or will eliminate the information from the Electronic Health Record or other record.

9.0 State Law Preemption and Exception

State laws that are contrary to the Privacy Rule are preempted by the federal requirements, which means that federal requirements will apply. Any question concerning the application of state law versus federal law should be referred to Legal Counsel for further review.

10.0 Safeguarding Protected Health Information

Augusta University healthcare components and business units that support healthcare components will safeguard all forms of protected health information by implementing appropriate administrative, technical, and physical safeguards to protect the privacy of PHI. This pertains to oral, written, and electronic PHI.

1. Appropriate measures and workforce behaviors shall be implemented to protect PHI from both intentional and unintentional use or disclosure that violates HIPAA protections. The medical center is also required to safeguard against incidental disclosures that may occur in the process of making an authorized use or disclosure.
2. Safeguards shall be implemented to address risks not already addressed in the HIPAA Security policies by implementing physical and behavioral practices.
3. Unit managers are responsible for completing self-risk assessments (as assigned by the AU Privacy Officer) of their area to determine areas of vulnerability and probabilities of inappropriate PHI disclosure.
4. Unit managers will implement appropriate safeguards that address their unit environment and functions.
5. In all circumstances, members of the workforce will use the minimum necessary information for the purpose at hand and use de-identified information whenever possible.
6. General Safeguards (examples, not an all-inclusive list):
    a. Mechanisms will be instituted to control access to the medical center unit offices and buildings
    b. Specific mechanisms will be instituted to control access to areas of buildings housing PHI, such as medical records storage locations
    c. Where possible, mechanisms will be instituted to reconfigure or separate areas (offices, workspaces, reception, hallways) open to the public to minimize PHI exposure
    d. Where possible, mechanisms will be instituted to reconfigure or separate internal units with different PHI needs to minimize unnecessary PHI exposure
    e. Where possible, move areas where PHI may be exposed away from high traffic areas (e.g., fax machines and printers away from hallways)

   f. In areas that are difficult to separate, use other mechanisms such as screen protectors, headsets, and mobile partitions, to limit PHI exposure
   g. Computer screens will be positioned so they are not directly observable by public pathways throughout buildings. This may include the use of polarized screens to limit visibility of PHI from public view
   h. Soft storage, such as disks and CDs will not be reused
   i. PHI will not be emailed except through secure channels authorized by the medical center
7. Paper Safeguards (examples, not an all-inclusive list)
   a. Where possible, all documents containing PHI will be kept in locked storage or in restricted locations
   b. Paper documents required for current use will be kept out of sight when not specifically required or currently worked on
   c. All mail will be opened, stored, and dispersed in areas away from public view.
   d. Paper documents will be properly disposed of at intervals defined by the medical center policy and disposal documented
   e. Medical records, charts and patient files will be maintained in locked storage
   f. Medical records, charts, and patient files in current use will be stored away from public view and will be kept without obvious names or labels observable by public view
   g. When PHI is to be faxed, members of the medical center workforce will contact the receiver to notify them that a fax is coming and arrange contact that notifies the sender that the fax has been received. All outgoing faxes must include a coversheet
   h. AU workforce members that handle paper PHI are required to adhere to a clean desk policy and store all PHI out of site at the end of their shift
8. Oral Safeguards (examples, not an all-inclusive list)
   a. Conversations regarding patient information should be kept to a minimum and occur in areas away from hearing distance of public or other patients
   b. Face -to-face and telephone conversations regarding PHI should use identifying information as little as possible
   c. Conversations regarding PHI should be conducted in a low voice and in private areas if possible
   d. When receiving telephone calls requesting PHI, the medical center workforce member must validate the identity of the caller before releasing information. In most cases, the request for PHI should be made in writing with a properly signed authorization, or in person with a mechanism to identify the individual requesting the PHI disclosure. In cases where the medical center workforce member may have regular communication with a business associate regarding PHI, the medical center workforce member takes responsibility for validating the identity of the business associate.
9. Healthcare components of AU will make available a complaint process for individuals to make complaints concerning safeguarding policies and procedures.
10. It is the responsibility of the AU Privacy Officer, the Chief Information Security Officer and appropriate department managers to ensure that this policy is followed.

REFERENCES & SUPPORTING DOCUMENTS

1) Uses and Disclosures for Treatment, Payment, and Healthcare Operations [45 CFR 164.506]
2) Uses and Disclosures Requiring an Opportunity to Agree or Object (45 CFR 164.510)
3) Uses and Disclosures for Which Consent, an Authorization, or Opportunity to Agree or Object is Not Required (45 CFR 164-512(a))
4) Uses and Disclosures of PHI Requiring Authorization 45 CFR 164.508
5) Uses and Disclosures Required 45 CFR 164.502(a)(2)(i)(ii)
6) Use and Disclosures of PHI Related to Reproductive Health 164.502(a)(5)(iii)

RELATED POLICIES

1) Patient Rights Under HIPAA
2) Authorizations for the Use of Protected Health Information
3) Use of Protected Health Information for Academic Purposes
4) 7.13 Designation of USG as a Hybrid Entity Under HIPAA

APPROVED BY:
Interim Executive Vice President for Academic Affairs and Provost, Augusta University
Date: 6/9/2025

President, Augusta University Date: 6/9/2025