Augusta University
Policy Library

Privacy of Health Information

Policy Manager: Audit, Compliance, Ethics, and Risk Management

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 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 protected health information ("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:

Office of Legal Affairs Use Only
Executive Sponsor: VP for Audit, Compliance, Ethics, and Risk Management
Next Review: 5/2024

DEFINITIONS

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.

Designated Record Set

Records Included. The designated record set shall include health and billing records, regardless of the medium in which they are stored.

"Health records" shall mean all records identifiable to an individual patient that 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.

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

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).

"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.

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

HIPAA. The Health Insurance Portability and Accountability Act of 1996, and the regulations issued pursuant to that law. Reference: Public Law 104-191; 45 C.F.R. 160 & 164.

Protected Health Information (PHI). Health information transmitted or maintained in any form that:

a. 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
b. 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
c. 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
d. Is not an employment record.

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

PROCESS & PROCEDURES

1.0 Use & Disclosure of PHI

1.1 Use & Disclosure of PHI With and Without Authorization – In general, Augusta University may use and disclose a patient's PHI without an authorization for the purposes of treatment, payment and health care operations. Augusta University, however, must obtain a signed authorization from the individual or the individual's personal representative for all uses and disclosures of PHI that are not otherwise permitted or required by law.

1.2 Minimum Necessary Use, Disclosure and Request for PHI – All individuals associated with Augusta University are generally expected to limit their uses and disclosures of PHI, and requests for PHI to the minimum amount of information necessary to perform their duties. This general expectation does not mean that providers should restrict exchanges of information required in order to treat patients quickly and effectively. Those divisions within Augusta University that routinely use and exchange health information will develop policies and/or procedures explaining how much information may be used disclosed or requested in situations that occur on a routine and non-routine basis. For divisions that do not routinely use and exchange health information, the responsible

manager should advise the employee(s) on how the health information may be used and disclosed, in consultation with the Privacy Officer.

1.3 De-Identification of PHI – Augusta University is permitted to allow the use or disclosure of PHI for the purpose of creating de-identified information. De-identified information is health information from which Augusta University or another entity has deleted, or blocked identifiers, so that the remaining information cannot reasonably be used to identify the person who is the subject of the information. To be fully de-identified, the following identifiers must be removed: (1) Names; (2) All geographic identifiers smaller than State, including street addresses, cities, counties, zip codes, etc.; (3) Except for the year, all dates related to the patient or subject such as birth date, date of admission or discharge, date of death, all ages over 89 unless merely specified as "age 90 or older;" (4) Phone and fax numbers; (5) E-mail addresses, personal web-sites, URLs and IP addresses; (6) Social Security numbers; (7) Medical record numbers; (8) Health plan beneficiary numbers; (9) Account numbers; (10) Certificate or license numbers; (11) Device identifiers such as serial numbers and vehicle license plate numbers; (12) Biometric identifiers such as finger and voice prints; (13) Images that can be used to identify the patient or subject, such as full-face photographs; (14) Any other unique identifying number or characteristic, except for an identifier assigned by and unique to Augusta University that will allow Augusta University alone to re-identify the patient or subject. Information may also be deemed de-identified if a person with knowledge and experience with the statistical and scientific methods for rendering information not individually identifiable determines that the risk is very small that the information to be disclosed could be used to identify the person who is the subject of the information.

Augusta University may provide either de-identified information or a limited data set in response to a requestor. Unless otherwise restricted or prohibited by other federal or state law, Augusta University can use or disclose de-identified information for research, education and other appropriate purposes, without further restriction.

1.4 Use & Disclosure of PHI via Electronic Media – Augusta University will reasonably safeguard PHI used or disclosed via electronic media from any intentional or unintentional use or disclosure. All persons provided access to Augusta University PHI have an obligation to maintain the confidentiality of patient and employee information via electronic media. Obligations regarding confidentiality continue even after termination of employment, service, association, or privileges with Augusta University. All individuals within Augusta University will exercise appropriate measures and care when storing, transporting, photocopying, disposing of, network printing, downloading, emailing, or faxing confidential information. Precautions will be taken to avoid having computer monitors, printers, fax machines, or paper records in view of unauthorized

onlookers while such data is displayed. Security measures must be in place for all electronic media devices that are portable, either issued by Augusta University or personally owned.

1.5 Use & Disclosure of PHI for Research Purposes – 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. Disclosure of information that is not essential to the stated purposes of the study is prohibited. All disclosures of protected health information for research purposes will be in accordance with state and federal law, and the guidelines and procedures of the Augusta University Human Assurance Committee (HAC).

1.6 Use & Disclosure of PHI in Psychotherapy Notes – In general, a current or former patient is entitled to reasonable access to review and examine his/her mental health records. A current patient may be denied such access if the chief medical officer or the patient's treating physician or psychologist determines that the patient's access to his/her mental health records or a disclosure of information to the patient is likely to endanger the life or physical safety of the patient or cause substantial harm to a person referenced in the records. The Augusta University treating physician or psychologist is responsible for restricting the patient's access to his/her mental health records or information and must make a notation of such determination in the patient's mental health records.

1.7 Use & Disclosure of PHI for Marketing Purposes – 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.

1.8 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 in the OHCA shall be referred to MCGHI's Public Relations Office.

1.9 Disclosure of PHI to Persons Involved in a Patient's Care – Augusta University may disclose to a family member, relative, close personal friend, or any other person or entity identified by the patient, PHI that is directly relevant to such person's involvement with

the patient's care or payment. Furthermore, Augusta University may request PHI from a patient's family member, relative, close personal friend or any other person or entity identified by the patient if such information would be required for the patient's care or payment. Augusta University faculty, staff and students should use their professional judgment in determining the identity of a patient's relative or other representative.

1.10 Patients in the Custody of Correctional Institutions or Law Enforcement – Notwithstanding any other provision in this policy, patients who are in the custody of a correctional institution or law enforcement authority are not required to be given a Notice of Privacy Practices, or an accounting of disclosures to correctional institutions and law enforcement authorities.

2.0 Notice of Privacy Practices

All Augusta University health care components shall provide their Notice of Privacy Practices to individuals regarding the use and disclosures of PHI at the time of the patient's first treatment encounter on and after the effective date of this policy. Augusta University will make a good faith effort to obtain an individual's written acknowledgement of receipt of the Notice of Privacy Practices. Augusta University will maintain a record keeping system to track the acknowledgement of receipt of the Notice of Privacy Practices.

3.0 Patient Rights Provided by HIPAA

3.1 Right to Receive a Paper Copy of the Notice of Privacy Practice – Although the Notice of Privacy Practices may be provided electronically, Augusta University will offer all of its patients a paper copy of its Notice of Privacy Practice.

3.2 Right to Request Access and Receive a Copy of PHI – Patients have the right to access, inspect and obtain a copy of PHI about them that is maintained in the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate. All requests for appointments to inspect and copy health records must be in writing. Requests must be acted upon within 30 days. An extension of 30 days is allowed if Augusta University provides the requestor with the reason for the delay and the date by which the action will be completed.

3.3 Right to Request an Amendment to Health Record – Augusta University will provide an individual the right to request an amendment to his/her PHI for as long as the information is maintained in the designated record set. Corrections and amendments to health records may be needed due to errors or omissions that have resulted from clerical errors, documentation delays, miscommunication or misunderstanding. Documentation occurring as part of the routine record completion process following patient discharge or

departure is not considered to be a correction or amendment. Patients who believe information in their health records is incomplete or incorrect may request an amendment or correction to the information. The requests must be made in writing and must be acted upon within 60 days from receipt. A one-time 30day extension is allowable if Augusta University provides a written statement of the reason for the delay. Under certain provisions, Augusta University may deny the patient's right to amend the health record. If the request is denied, the Enterprise Privacy Officer will be notified to ensure the denial process is followed. Inmates wishing to request an amendment to their health record should submit an inmate grievance through the correctional facility where they are incarcerated, since inmate health records are the property of the Georgia Department of Corrections.

3.4 Right to Request a Restriction of the Use & Disclosure of PHI – Augusta University will allow and take all necessary steps to permit individuals to request restrictions on the uses and disclosures of PHI. Augusta University, however, is not required to agree to a restriction. Upon agreeing to such a restriction, Augusta University will not violate the restriction, unless required to do so by law, or as specified within this policy.

3.5 Right to Request Confidential Communications – Augusta University will take necessary steps to accommodate reasonable requests by patients to receive confidential communication regarding their PHI. Patients have the right to request receipt of PHI by alternative means or at alternative locations. The reasonableness of a request will be determined solely on the basis of the administrative complexity of complying with the request. Requests will not be denied based on a perception of the merits of the patient's reason for making the request. Requests may be denied if the patient has not provided information as to how payment, if applicable, will be handled, or if the patient has not specified an alternative address or method of contact.

3.6 Right to Receive an Accounting of Disclosure of PHI – Augusta University patients have the right to request, in writing, an accounting of certain disclosures of their PHI. The accounting will be provided to the patient within 60 days of a written request and will include: 1) disclosures which occurred after April 14, 2003; 2) disclosures which were not authorized by the patient, subject to certain exceptions; 3) a list of protocol or other research activity for which the patient's protected health information may have been disclosed; 4) the disclosure dates; 5) a summary or listing of the information disclosed; 6) the individuals or organizations to whom the information was disclosed; 7) the individuals who disclosed the information; and 8) the purposes of the disclosures. Disclosures not required to be included in the PHI Disclosure Report include those disclosure made: 1) for treatment, payment or healthcare operations; 2) more than six years prior to the request or before the April 14, 2003 effective date; 3) as disclosures to the patient or those authorized by the patient.

4.0 Administrative Requirements

4.1 Personnel Designation – The President shall designate a privacy official who will serve as Enterprise Privacy Officer for Augusta University as well as for GHSMC and GHSMA. The Enterprise Privacy Officer's responsibilities are detailed in the Enterprise Privacy Officer's job description. Among the Enterprise Privacy Officer's primary responsibilities are:

- Overseeing the implementation of Augusta University's privacy policies and HIPAA compliance;
- Advising others as needed on health information privacy and security;
- Receiving and responding to any inquiries or complaints from governmental or licensing/accrediting bodies regarding privacy practices;
- Ruling on disputed requests for access, accountings of disclosure, and amendments;
- Managing complaints from patients regarding privacy practices;
- Complying with Breach Notification requirements, providing guidance for appropriate disciplinary action and overseeing plans for correction; and
- Developing HIPAA/HITECH training content for new hires, orientation of resident/students, annual compliance month, and plans for correction

4.2 Workforce Training – Augusta University will train all members of its workforce including employees, faculty and students, regarding the proper use and disclosure of patients' health information. Training will be appropriate for the level of staff and their duties and may include both general training and advanced training. The Division of Human Resources will be responsible for administering and documenting the training program for employees. The colleges in which a student is enrolled are responsible for ensuring that their students have been trained. All existing workforce members should be trained by the effective date of this policy, and all new workforce members must complete training in a reasonable time frame after the person joins the workforce.

4.3 Safeguards – Augusta University will reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of Augusta University's patient privacy policies and applicable federal and state law. Safeguards include administrative procedures, physical measures and technical means to protect patient's health information

4.4 Right to Make a Complaint – Any individual who believes his/her rights, granted by HIPAA privacy regulations or any other state or federal laws dealing with privacy and confidentiality, have been violated may file a written complaint regarding the alleged privacy violation. Complaints should be brought to the attention of the

Enterprise Privacy Officer. Other faculty, staff, and students who receive complaints from patients should inform the Enterprise Privacy Officer. “Copies of all written complaints, resolved or unresolved, must be forwarded to the Enterprise Privacy Officer for tracking and quality improvement purposes.”

4.5 Sanctions – Augusta University will apply appropriate sanctions against workforce members who fail to comply with Augusta University’s privacy policy. Any violation of this policy must be reported to the Enterprise Privacy Officer. The Enterprise Privacy Officer shall maintain a record of all reported violations, and the responsive actions taken.

4.6 Mitigation – To the extent practicable, Augusta University will mitigate any harmful effect that becomes known to Augusta University as a result of an improper use or disclosure of PHI.

4.7 Refrain from Intimidating or Retaliatory Acts- Augusta University will not intimidate, threaten, coerce, discriminate against or take other retaliatory action against an individual for the exercise of his/her rights to: (i) file a privacy complaint with the Secretary of the Department of Health and Human Services; (ii) testify, assist or participate in an investigation, compliance review, proceeding or hearing regarding health privacy; and (iii) oppose any act or practice made unlawful by the HIPAA privacy provisions, provided that the individual has a good faith belief that the practice opposed is unlawful and the manner of opposition is reasonable and does not involve the disclosure of PHI.

4.8 Non-Waiver of Rights as a Condition of Treatment – Augusta University may not require individuals to waive their rights of privacy, as provided through HIPAA, as a condition of the provision of treatment.

4.9 Documentation Requirements – All records created as a result of this policy, including health records, notices of privacy, internal procedures, accounting of disclosures, etc., shall be retained until at least the later of: (1) six years from the last date the record was in effect; (2) six years from the creation of the record; or, (3) any period longer than six years if required by any other applicable law, regulation or policy of Augusta University, the OHCA, or the Board of Regents. Augusta University will incorporate into its policies, procedures, guidelines and other administrative documents any changes in law and will properly document and implement any changes to policies, procedures, and guidelines as necessary by changes in law. Augusta University reserves the right to amend this policy, and all internal forms, policies and procedures related to this policy. All internal policies, procedures, notices of privacy practices and other documents created to comply with this policy shall specifically state that Augusta University reserves the right to amend these policies and documents.

5.0 Effective Date – This policy shall take effect April 14, 2003.

6.0 Business Associates

HIPAA Privacy Rules define a business associate as a person or entity that provides certain functions, activities, or services on behalf of the covered entity, involving the use or disclosure of PHI. The business associate may only use the PHI that it receives in its capacity as the business associate, as permitted by law, and its contract with Augusta University.

If an Augusta University employee knows or has reason to believe that a business associate is inappropriately using or disclosing PHI, whether the PHI was received by the individual entity or not, the employee is required to notify Augusta University's Enterprise Privacy Officer immediately regarding the suspected violation.

All agreements with business associates of Augusta University must be in writing and must contain certain mandatory provisions designed to protect the privacy and security of our patients' PHI. No Augusta University employee shall disclose PHI to a business associate without a signed business associate agreement.

The Augusta University Legal Office shall screen all contracts routed through the Division of Sponsored Program Administration to determine if the outside contractor/vendor meets the definition of a business associate and whether appropriate business associate contract language is required. The Legal Office and Materials Management shall develop screening criteria to be used by Purchasing to determine if any of their agreements need to contain language addressing health information privacy. Purchasing and the Legal Office shall provide the Enterprise Privacy Officer with copies of all business associate agreements.

REFERENCES & SUPPORTING DOCUMENTS

Augusta University Hybrid Designation
https://www.augusta.edu/services/legal/

Board of Regents of the University System of Georgia policy 7.13 *Designation of USG as a Hybrid Entity Under HIPAA*
https://www.usg.edu/policymanual/section7/C2869

HIPAA Privacy Rule
https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

HIPAA Breach Notification Rule
https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

HIPAA Security Rule
https://www.hhs.gov/hipaa/for-professionals/security/index.html

HIPAA Transactions and Code Sets Rule
https://www.hhs.gov/hipaa/for-professionals/other-administration-simplification-rules/index.html

Notice of Privacy Practices
https://www.augusta.edu/dentalmedicine/patientservices/policies/privacy.php

RELATED POLICIES
Intentionally left blank.

APPROVED BY:

Executive Vice President for Academic Affairs and Provost, Augusta University
Date: 5/21/2021

President, Augusta University Date: 5/23/2021