Augusta University
Policy Library

Sanctions for Privacy and Cybersecurity Violations Policy

Policy Manager: Office of Audit, Compliance, Ethics & Risk Management

POLICY STATEMENT
Augusta University will apply sanctions for members of its workforce who fail to comply with its privacy and cybersecurity policies, procedures, or practices. This policy supports compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, and Breach Notification Rules, located at 45 CFR Subparts C, D, and E.

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). References to AU in this policy refers to AU HCC.

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

See *Policy Regarding Protected Health Information*.

PROCESS & PROCEDURES
In accordance with any disciplinary action and/or sanctions policy in force through Human Resources or Administration, appropriate sanctions will be applied against workforce members who fail to comply with the Privacy and Cybersecurity policies, procedures, or practices of AU. For individuals subject to its authority, AU may impose disciplinary action in accordance with the rules set forth in the Code of Conduct, applicable Medical Staff Bylaws, as well as any other existing and applicable policies or guidance documents.

Office of Legal Affairs Use Only
Executive Sponsor: VP for Audit, Compliance, Ethics and Risk Management
Next Review: 5/2030

The sanctions shall vary depending on the severity of the violation, whether the violation was intentional or unintentional, whether the violation indicates a pattern or practice of improper access, use or disclosure of protected health information (PHI), and similar factors. Relevant laws, regulations, organizational policies and procedures, and prior applied sanctions will be considered. The sanctions imposed may include but are not limited to:

- Counseling and Education or equivalent from the supervisor and/or the AU Privacy Officer about policy and/or regulatory non-compliance
- Warning or equivalent verbal or written communication that warns the workforce member that the performance or conduct is unacceptable and violates AU policies
- Suspension or equivalent administrative leave with/without pay (Manager shall review such action with Employee Relations, Human Resources or Vice President of Human Resources prior to communicating with the workforce member)
- Discharge or equivalent – a workforce member, contractor, or business associate may be terminated from employment or contract. (Manager shall review such action with Employee Relations, Human Resources or Vice President of Human Resources prior to communicating with the workforce member)
- Notification to law enforcement officials and regulatory, accreditation and licensure organizations

For business associates, vendors, and independent contractors, the AU Privacy Officer will work with the applicable AU department to recommend sanctions and implement any corrective action.

Violations are categorized according to the nature of the privacy or security incident. Categorization helps standardize corrective action determinations and assists with trending reports to improve operations regarding patient privacy, security, and accessibility to PHI.

Categories of Privacy Incidents

The following categories define the significance and impact of the privacy incident or violation to help guide its corrective action and remediation steps:

Category	Type of Violation	Description
1	Accidental or Inadvertent Violation	This is an unintentional violation of privacy or cybersecurity policy/procedure that may be caused by carelessness, lack of knowledge, lack of training, or other human errors. *Examples of this type of incident include but are not limited to directing PHI via mail, e-mail, or fax to a wrong party or incorrectly identifying a patient record.*

2	Failure to Follow Established Policies and Procedures	This is a violation due to reckless disregard, poor job performance or lack of performance improvement. *Examples of this type of incident include but are not limited to: release of PHI without proper patient authorization; repeat victim of phishing incidents, leaving detailed PHI on an answering machine; failure to report privacy violations; improper disposal of PHI; failure to properly sign off from or lock computer when leaving a work station; failure to properly safeguard password; providing credentials to co-workers, failure to safeguard portable device from loss or theft; or transmission of PHI using an unsecured method.* This Category also includes a repeated Category 1 violation.
3	Deliberate or Purposeful Violation Without Harmful Intent	This is an intentional violation due to curiosity or desire to gain information, for personal use or convenience, or poor professional judgement. *Examples of this type of incident include but are not limited to accessing the information of friends, family members, co-workers, high-profile people, celebrities, accessing, using or disclosing PHI without a legitimate need to do so, such as checking the results of a coworker's pregnancy test.* This Category also includes a repeat of a Category 2 violation.
4	Willful and Malicious Violation with Harmful Intent	This is an intentional violation causing patient or organizational harm. *Examples of this type of incident include but are not limited to disclosing PHI to an unauthorized individual or entity for improper or illegal purposes (i.e., identity theft); or improperly disclosing PHI to the media or on social media with the intent to cause harm.* This Category also includes a repeat of a Category 3 violation.

Factors of consideration

The following factors also assist to define the significance and impact of the privacy incident:

- Violation of sensitive information such as HIV-related, psychiatric, substance abuse, and genetic data
- High volume of people or data affected
- High exposure for the organization
- Large organizational expense incurred, such as breach notifications
- Hampering the investigation, lack of truthfulness
- Negative influence on others
- History of performance issues and/or violations

Considerations to Mitigate Sanctions
Consideration to include:

- Violator's knowledge of privacy practices (i.e., inadequate training, training barriers, or limited English proficiency)
- Culture of surrounding environment (i.e., investigation determines inappropriate practices in business unit)
- Violation occurred as a result of attempting to help a patient
- Victim(s) suffered no financial, reputational, or other personal harm
- Violator voluntarily admitted the violation in a timely manner and cooperated with the investigation
- Violator showed remorse
- Action was taken under pressure from an individual in a position of authority

Following completion of the investigation, the AU Privacy Officer will collaborate with the involved workforce member's director/supervisor to discuss findings, corrective action plans and recommended sanctions. Any employee discipline will first be referred to the appropriate Human Resources personnel and Office of Legal Affairs when appropriate.

To assure consistency and accountability for all involved parties, the AU Privacy Officer will document and maintain records to support the collaborative efforts of enforced sanctions. Documentation shall include but is not limited to the: workforce member name, violation, date of violation, supporting evidence/investigation summary, and authorized sanction.

When applicable, the AU Privacy Officer will refer all violations of state and federal law to appropriate external agencies for further investigation and/or prosecution, but will notify AU Senior Leadership, including AU General Counsel, prior to doing so. Under HIPAA penalties for misuse or misappropriation of PHI includes both civil monetary penalties and criminal penalties.

REFERENCES & SUPPORTING DOCUMENTS

HIPAA Security Rule – 45 CFR Part C
HIPAA Breach Notification Rule - 45 CFR Part D

RELATED POLICIES
Privacy of Health Information

APPROVED BY:
Interim Executive Vice President for Academic Affairs and Provost, Augusta University
Date: 3/14/2025

President, Augusta University Date: 3/25/2025