Privacy and Confidentiality of Individually Identifiable Health Care Information under HIPAA

Policy 911

1 Purpose

1.1 Appalachian recognizes the applicability of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH Act), and its regulations to certain sectors of the University. This policy addresses the University’s obligations to comply with HIPAA and its accompanying privacy regulations, which require the University's health care components to protect against unauthorized use or disclosure of individually identifiable health information (specifically "protected health information" or "PHI"). Protected health information under HIPAA excludes individually identifiable health information in education records, including student health records covered by the Family Educational Rights and Privacy Act (FERPA) as amended, 20 USC 1232g and records described at 20 USC 1232g(a)(4)(B)(iv). Records protected by FERPA will be protected and disclosed as mandated by FERPA and University policy including the Policy Statement on the Family Educational Rights and Privacy Act.

1.2 As an entity containing subdivisions and components that act as health care providers and create, receive, maintain and transmit ePHI, the University is a Hybrid Entity with designated Covered Health Care Components. This Policy identifies the Health Care Components subject to HIPAA's privacy, security, breach notification and enforcement provisions.

2 Scope

2.2 This policy applies to all Covered Health Care Components and all employees and students subject to HIPAA requirements.

3 Definition

3.1 Authorization

Written authorization from the patient or Legally Authorized Representative to use or disclose protected health information is required, except for the following purposes:

1. treatment payment or health care operations;
2. when a waiver of an authorization is approved by the HIPAA Privacy Officer or designee;
3. judicial and administrative proceedings;
4. limited law enforcement proceedings;
5. investigations of abuse or neglect;
6. identification of a deceased person or the cause of death;
7. activities related to national defense.

3.2 Business Associate

A person or entity that is not a part of the University's workforce, but who performs certain functions, activities, or services for the University's covered health care components involving the use and/or disclosure of PHI.

3.3 Covered Entity

A health plan; a health care clearinghouse; and/or a health care provider who transmits protected health information in an electronic format in connection with a HIPAA covered transaction.

3.4 Covered Health Care Components

Those units that are health care providers that engage in HIPAA transactions and functional units that provide support services to covered entities.

3.5 Covered Transactions

The transmission of information between two parties to carry out financial or administrative activities related to health care. The following non-exhaustive list includes types of transmissions that are considered covered transmissions:

1. Health care claims for reimbursement purposes.
2. Health care payment and remittance data.
3. Coordination of benefits information.
4. Health care claim status.
5. Health plan enrollment and disenrollment information.
6. Eligibility for health plan benefit information.
7. Referral certification and treatment authorization information.
8. Health care claims attachments.
9. Other transactions that the Secretary of the U.S. Department of Health and Human Services may prescribe by regulation.

3.6 De-identified PHI

Health information that cannot be identified to the individual patient. For PHI to be considered de-identified, the following identifiers of the individual or of relatives, employers, or household members of the individual, must be removed:

1. Names;
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census:
    1. The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and
    2. The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000;
3. All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers;
5. Vehicle identifiers and serial numbers, including license plate numbers;
6. Fax numbers;
7. Medical device identifiers and serial numbers;
8. Email addresses;
9. Web Universal Resource Locators (URLs);
10. Social security numbers;
11. Internet Protocol (IP) addresses;
12. Medical record numbers;
13. Biometric identifiers, including finger and voice prints;
14. Health plan beneficiary numbers;
15. Full-face photographs and any comparable images;
16. Account numbers;
17. Certificate/license numbers; and
18. Any other unique identifying number, characteristic, or code.

3.7 Information Technology (IT) Standards

Documented principles that establish requirements and processes that provide a reliable basis for shared expectations on how the University will comply with Information Technology related University policies, as well as federal and state laws and regulations.

4 Policy Statements

4.1 HIPAA Oversight Program

4.1.1 The Chancellor shall vest one individual as the HIPAA Privacy Officer and one individual as the HIPAA Security Officer with the authority to oversee and manage the HIPAA Oversight Program. The HIPAA Privacy Officer and Security Officer, or designees, will co-chair a HIPAA Oversight Committee (HIPAA-OC), with membership appointed by the Chancellor to oversee the overall development, implementation, and operationalization of the University HIPAA compliance program. The HIPAA-OC will be responsible for:

1. Collaborative development and maintenance of a University HIPAA Policy.
2. Prioritization, Coordination, and Oversight of tasks and project work related to HIPAA compliance needs or gaps.
3. Oversight of the formal designation of University units as covered entities.
4. Review and advise executive leadership on proposals to establish new covered entities.
5. Review any third party applications that may interface with protected health information in the context of HIPAA or like data

types (e.g. research health information, protected health information not involved in billed services).
6. Annual review of HIPAA gap and risk assessment to identify issues and resource needs.
7. Selection and engagement with consultant groups as needed for periodic review and assessment of HIPAA compliant status.

The HIPAA-OC will provide an annual compliance status report to the Chancellor, Provost, Chief Information Officer, General Counsel and Chief Audit Officer.

4.2 HIPAA Oversight Program Requirements

4.2.1 Notice of Privacy Practices. The University's covered health care components shall provide to each patient, no later than the date of the first service delivery, a Notice of Privacy Practices containing a description of (a) the uses and disclosures of PHI that may be made by a covered health care component of the University, (b) the covered component's duties with regard to PHI, and (c) the rights afforded to patients. The Notice of Privacy Practices must be posted by each covered component and made available to patients on request.

4.2.2 Generally Permitted Uses and Disclosures of PHI (other than for treatment, payment and health care operations):

1. De-identified PHI. De-identified PHI may be used or disclosed without consent or authorization as long as no means of re-identification is disclosed. Release of de-identified PHI by a covered health care component of the University must receive the prior approval of the University's HIPAA Privacy Officer.
2. Marketing. The use or disclosure of PHI for marketing purposes (communication intended to encourage the purchase or use of products or services) requires an authorization, except for face-to-face communications with the individual patient by the covered health care component (a) to describe health related products or services that are provided by or included in a plan of benefits; (b) for treatment of the patient; or (c) for case management or care coordination or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to that individual.
3. Business Associates. PHI may be used and disclosed to a business associate of a covered health care component provided the business associate has signed and is in compliance with a Business Associate Agreement in a form approved by the University's HIPAA Privacy Officer.
4. Research. Use or disclosure of PHI for University research purposes generally requires the permission of the patient(s). Such permission must be in the form of an authorization as defined above. Use or disclosure is permitted without authorization if the University's HIPAA Privacy Officer or designee grants a waiver or partial waiver of the authorization.

4.2.3 Consent or Authorization Not Required under HIPAA. The disclosures without consent or authorization that are permitted by HIPAA are set forth below. To the extent that North Carolina law is more stringent or provides greater privacy protection, North Carolina law will apply.

1. Disclosures required by law. PHI may be disclosed to the extent required by applicable law.
2. Public Health Activities. PHI may be used and disclosed to a public health authority that is authorized by law to collect or receive such information for preventing or controlling disease, injury, or disability, including public health issues, vital records, child or adult abuse or neglect, adverse food or drug events, and investigations of work-related illnesses or injuries as required by law.
3. Victims of Abuse, Neglect or Domestic Violence. PHI may be used or disclosed to a government authority that is investigating a report of abuse, neglect, or domestic violence to the extent disclosure is required or permitted by applicable law.
4. Health Oversight Activities. With certain exceptions, PHI may be used or disclosed to a health oversight agency for oversight activities authorized by law, including audits, civil, administrative or criminal investigations or proceedings, inspections, licensure, or disciplinary actions.
5. Judicial and Administrative Proceedings. PHI may be disclosed in the course of a judicial or administrative proceeding in response to a valid court order issued by a court of competent jurisdiction.
6. Law enforcement purposes. PHI may be disclosed for law enforcement purposes under court order when approved by the Office of General Counsel.
7. Decedents. PHI regarding decedents may be disclosed to coroners, medical examiners, and funeral directors if necessary to carry out their duties.
8. Serious Threats to Health or Safety. PHI may be used or disclosed under certain circumstances if a covered health care component believes in good faith that the use or disclosure is necessary to protect a person or the public from serious harm.
9. Specialized Government functions. PHI may be used or disclosed for specialized government functions such as military and veterans' activities, security and intelligence activities, protective services for officials, medical suitability, and correctional institutions and other law enforcement custodial situations.
10. Workers Compensation. PHI may be used or disclosed to the extent required to comply with workers' compensation laws and similar programs.

4.2.4 Revocation of Authorization. Under any circumstances other than those listed above, written authorization will be obtained before use or disclosure of patients’ PHI. This authorization may be subsequently revoked by the patient in writing. Upon receipt

of such revocation, a covered health care component of the University will not disclose the patient's PHI, except for disclosures which were in process prior to the receipt of the revocation.

4.2.5 To use or disclose PHI for any purpose other than treatment, payment, or health care operations, a covered component must obtain a signed and dated specific Authorization (on a form approved by the University's HIPAA Privacy Officer) from the patient or authorized representative, unless authorization is waived or not required under HIPAA.

4.2.6 Any release of information for purposes other than treatment, payment, or health care operations without a signed authorization must be reviewed and approved by the Privacy Officer, or designee, except (1) where the release is to the individual patient, (2) where delay in seeking such approval would impair response to a health or safety emergency, or (3) where such release is permitted by rules of the covered health care component.

4.2.7 HIPAA Security Procedures and Training. All units subject to HIPAA requirements must comply with HIPAA Security Procedures which include training requirements, sanction procedures if training requirements are not followed, and a process to monitor and periodically evaluate the training program to ensure it is kept current with new technologies and campus policies. At minimum, all employees and students subject to HIPAA requirements must complete campuswide security training and HIPAA training upon hire or start of work within the covered entity, and annually.

4.3 Minimum Necessary Standard

4.3.1 Covered health care components must limit uses and disclosures of PHI to the minimum necessary to accomplish the intended purpose of the use or disclosure except (1) disclosures to or requests by a health care provider for treatment purposes; (2) disclosures to the individual patient; (3) uses and disclosures 4.4

4.4 Patients Rights

4.4.1 Right to Receive a Notice of Privacy Practices. No later than the date of the first delivery of health care services, a patient has the right to receive a Notice of Privacy Practices containing a description of (a) the uses and disclosures of PHI that may be made by a covered health care component of the University, (b) the covered component's duties with regard to PHI, and (c) the rights afforded to patients. The Notice of Privacy Practices is provided by the applicable covered health care component.

4.4.2 Right to Access PHI. A patient has a right to inspect and receive a copy of their PHI that is used to make decisions about the patient for as long as the University maintains the information, except for information specifically exempted from disclosure to the patient by HIPAA. A patient must make a request for such access to the applicable covered health care component.

4.4.3 Right to Request an Amendment of PHI. A patient has a right to request an amendment of PHI contained in designated records sets. A covered health care component is not required to grant the request for amendment and may deny the request under specified circumstances.

4.4.4 Right to an Accounting of Disclosures. A patient has the general right to receive an accounting of disclosures of PHI in the six years prior to the request. A patient must make a request for a list of disclosures to the applicable covered health care component.

4.4.5 Right to Request Restrictions on release of PHI.

> 4.4.5.1 A patient has a right to request restrictions on the uses and disclosures of PHI to carry out treatment, payment, or health care operations, and restriction on disclosures made to an individual's family, friends, or relatives. The covered health care component is not required to agree to the requested restriction. However, if the covered health care component does agree, it must abide by the restriction except in emergencies and in situations where use or disclosure is permitted by HIPAA without authorization.
>
> 4.4.5.2 An agreed upon restriction may be terminated by the patient or by the covered health care component provided that the termination is effective only for PHI created or received after the date of termination.
>
> 4.4.5.3 Restrictions that are agreed to and terminations of agreed upon restrictions must be documented in writing and retained by the covered health care component for a period of six years from the date of the creation of the termination or restriction or from the date it was last in effect, whichever is later.

4.4.6 Right to Receive Confidential Communication. A patient has the right to request how and where to be contacted to receive PHI. This request must be made in writing, and it must state the address at which the PHI is to be received and explain whether the request will interfere with the patient's chosen method of payment. The covered health care component will accommodate all reasonable requests. Requests may be made by contacting the University's Privacy Officer.

4.4.7 Right to File a Complaint. If a patient is concerned that a covered health care component of the University has violated any of the patient's privacy rights, or if a patient disagrees with a decision that is made about access to their PHI, the patient may contact the University's Privacy Officer. The patient may also file a written complaint to the Director, Office for Civil Rights of the

U.S. Department of Health and Human Services. There will be no intimidation, threat, coercion, discrimination or retaliation against any individual for filing a complaint or for exercising any of the above-listed rights.

4.5 Physical and Electronic Security

4.5.1 Physical and Electronic Security of PHI. HIPAA requires physical and electronic security to maintain the privacy of PHI in all forms, including oral, written, and electronic. Covered health care components shall ensure the physical and electronic security of all PHI.

4.6 Breaches of Privacy and Security

4.6.1 Breaches of privacy of PHI are to be reported immediately to the University's Privacy Officer. Breaches of security are to be reported according to procedures set forth by ITS Office of Information Security.

4.6.2 Covered health care components must mitigate, to the extent practicable, any known harmful effects of the use or disclosure of PHI in violation of this policy or the requirements of HIPAA.

4.6.3 Any University employee or contractor who is in violation of this policy is subject to disciplinary action up to and including discharge in accordance with applicable University policies and procedures. Individuals may also be subject to civil and criminal penalties under HIPAA.

4.7 Exceptions

4.7.1 Exceptions to this policy must be approved by the Chief Information Officer and the Office of General Counsel.

5 Additional References

HIPAA Privacy Regulations

6 Contacts

6.1 Administrative

Chief Information Security Officer | 828-262-6278
Office of the Chief Information Officer | 828-262-6278 | Office of the Chief Information Officer

6.2 Other University Contact

Office of General Counsel | 828-262-2751