ANNE ARUNDEL HEALTH SYSTEM
CONFIDENTIALITY AGREEMENT

By acknowledging this policy, I understand that as a workforce member/contractor/vendor of Anne Arundel Health System ("AAHS"), or an individual who has been given specific authorization by AAHS to participate in certain confidential patient care or other activities, I have a responsibility to safeguard patient privacy, Protected Health Information ("PHI"), as well as other AAHS confidential business information by assuring that access, use, and disclosure of the information is made by myself or others ONLY when the "Need to Know" exists. I understand, acknowledge, and agree that my, as well as my coworkers' and other individuals' access to PHI is permitted ONLY when I or they "need to know" the information, and that all other access to PHI is STRICTLY PROHIBITED by state and federal law.

"Need to know" is defined as OBTAINING, USING OR COMMUNICATING PHI or other AAHS employee or any other information which **is** REQUIRED for me to perform my specific job duties or as defined by the scope of my activities at AAHS. This pertains to PHI in the form of patient medical and personal information which is communicated orally or is accessed either by computer or in paper form, or in which **is** used in preparing patient services such as dietary support, pharmacy support, or diagnostic support in the form of laboratory, radiology or other procedures. I may only obtain, use or communicate PHI on the specific patient to whom I am providing care or support services.

PHI means individually identifiable health information which is a subset of health information, including demographic information collected from an individual and is created or received by a health care provider, health plan, or healthcare clearing house; and that which relates to the past present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual; or which there is a reasonable basis to believe the information can be used to identify the individual.

I hereby agree not to OBTAIN, USE OR COMMUNICATE ANY PHI or other information about patients, employees or any other aspect of AAHS business which is not REQUIRED for me to perform my job or the scope of my activities at AAHS. I realize that to do so is a serious offense and that improper access, use, or communication of patient PHI or AAHS information results in harm to patients, employees and AAHS as a whole. I am aware that an offense of this nature will result in disciplinary action up to and including possible termination of my employment and/or contractual relationship with AAHS.

I hereby agree to:

1. I will only obtain, use or communicate a patient's Protected Health Information (PHI), employee information, or other AAHS information on a 'Need To Know" basis.

2. I will not openly discuss, nor be careless with, a patient's Protected Health Information (PHI), employee information, or other AAHS information in a manner that my conversation may be overheard, or file viewed, by someone who does not "Need To Know" the information.

3. **I** will not disclose my computer password or any other personal code or password which has been given to me by AAHS, and understand, acknowledge and agree that to do so is considered a breach of the confidentiality of the information which the password protects.

4. I will log off **OR** lock the computer EACH and every time I leave the computer for any reason.

5. I will not use my computer password to access confidential personal employee and/or family member information.

6. I will report any suspected or potential breaches of confidentiality to the Corporate Compliance Officer, and/or Privacy Officer.

7. I will follow all Health System policies including those that pertain to Confidentiality of Medical Records and Information (ERR3.1.05), Use and Disclosure of Protected Health Information (MR7.1.01), Faxing of Medical Information (MR7.1.04), the Corporate Compliance Plan (ADM1.1.64), and Computing and Electronic Communications Usage (HR8.3.20)

8. I have received and will abide by the Confidentiality Policy (HR8.2.05) and Breach of PHI & Sanctions (ADM1.1.75)

HR8.2.05 - Confidentiality

HUMAN RESOURCES 018660, approved by VP Human Resources on 9/2008

Scope

Hospital/Medical Center

Policy Statement

The Medical Center will safeguard confidential information concerning patients, employees, AAMC business, and other matters. Unauthorized disclosure of confidential information is prohibited and may result in corrective action.

Definitions

none

Procedures

A. Application

This policy applies to AAMC employees and others who have access to confidential Medical Center information.

B. Definition

Confidential information includes, but is not limited to, information concerning:

-personal health information of Medical Center patients.

-current or former employees.

-job applicants.

-volunteers.

-members of the medical staff.

-board members or other officials.

-AAMC business, finances, or operations.

This definition includes information from all sources, including computer data.

C. Restrictions

C.1. Medical Center employees may not obtain, use, communicate, transfer and/or provide confidential information unless authorized by the appropriate department head.

C.2. Employees who violate this policy may be disciplined, up to and including dismissal. Unauthorized disclosure of legally protected information may result in civil liability or criminalprosecution.

C.3. Patient personal health information may be given to another employee only when necessary to provide services to the patient. (Refer to **MR7.1.01** - "**Use and disclosure of protected health information**" - Use and Disclosure of Protected Health Information) for additional information.

C.4. Employees are not to provide information about patients, physicians, board members, employees, or Medical Center business to representatives of the press without authorizationfrom the Public Relations Department or the appropriate department head.

C.5. Employees may not represent themselves as spokespersons for the Medical Center.

C.6. Employees may not access patient personal health information in any manner (i.e., computer, patient chart, etc.), unless required to do so to provide care.

D. Confidentiality Pledge

All employees will sign an AAMC confidentiality pledge as a condition of employment. The pledge outlines employee responsibilities concerning patient personal health information which can be accessed by the computer or in paper form, and protection of computer system data.

E. Reporting Violations

Employees who learn of a breach of confidentiality must report the incident to the appropriate supervisor.

References

none

Cross References

MR7.1.01 - "**Use and disclosure of protected health information"** - "Use and Disclosure of Protected Health Information"

Policy File Attachments

Confidentiality_Pledge.doc

128915 bytes

ADM1.1.75 - Breach of protected health information (phi) and sanctions

HIM-MEDICAL RECORDS 018715, approved by Chief Information Officer on 6/2009
OPS on 4/2009, HPRC on 5/2009

Scope

Anne Arundel Health System (AAHS), Inc., subsidiaries and affiliates.

Policy Statement

AAHS and its Workforce are entrusted with patients' protected health information (PHI). PHI is highly confidential and the utmost efforts and care must be taken to protect the privacy and security of all health information, both paper and electronic. The policy is intended to provide a framework for appropriate access, use, and disclosure of PHI by workforce and those granted access to medical records for job intended purposes. Any breach in health information security and/or privacy by members of the Workforce, as defined below, is subject to investigation and corrective action as set forth by this policy.

Definitions

1. "Privacy Breach" - A Privacy breach occurs when a member of the Workforce accesses, reviews, uses, discusses, and/or discloses a patient's PHI in violation of AAHS policies and procedures relating to privacy, or for purposes other than:

1.1. Treatment of the patient

1.2. Payment for treatment or services rendered

1.3. Health care operations as defined by the Privacy Rule (HIPAA)

1.4. As otherwise permitted or required under federal and/or state laws, rules or regulations.

2. "Protected Health Information (PHI)" - Any information, identifiable to an individual including: (a) demographic information, whether or not recorded in any form or medium that relates directly or indirectly to the past, present or future physical or mental condition of an individual; (b) information regarding the provision of health care to an individual; or (c) information regarding the past, present or future payment for the provision of health care to an individual.

3. "Security Breach" – A Security breach occurs when a member of the Workforce:

3.1. Releases or transmits PHI in an unauthorized manner.

3.2. Attempts to access or successfully accesses, uses, discloses, modifies or destroys PHI in violation of AAHS security policies and procedures relating to appropriate use of medical records, computer and/or any other information systems equipment or document containing PHI.

3.3. Shares sign-on code and/or password information with another person or uses another person's sign-on code and/or password to access PHI.

3.4. Interferes with system operations in an AAHS information system in such a way as to corrupt or destroy data.

4. "Workforce" – Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for AAHS, is under the direct control or supervision of AAHS, whether or not they are paid by AAHS.

Procedures

1. Access/Use/Disclosure of PHI

1.1. Workforce members will only access Protected Health Information, use, discuss and/or disclose a patient's Protected Health Information for the following purposes:

1.1.1. Treatment of the patient

1.1.2. Payment for treatment or services rendered

1.1.3. Health care operations as defined by the privacy rule

1.1.4. As otherwise permitted or required under federal and state laws, rules and regulations.

2. Sign-on code and Password

2.1. A Workforce member's sign-on code and password are the equivalent of his or her legal signature.

2.2. Workforce members will not disclose their sign-on code or password to anyone nor attempt to learn or use another person's sign-on code or password.

2.3. Workforce members will be accountable for all work done or PHI accessed under their sign-on code.

2.4. If a Workforce member believes the confidentiality of his/her sign-on code has been compromised, the Workforce member is responsible for immediately contacting the Help Desk to change his/her password.

2.5. Sign-on codes and passwords will be issued only after the Workforce member's supervisor has completed, signed and submitted an access request through the Help Desk.

2.6. The Workforce member is to sign a Confidentiality Pledge during the new-hire orientation or as part of the hiring process.

3. Monitoring access

3.1. A Workforce member's access to electronic health information will be logged in audit trails.

3.2. Audit trails of access to electronic health information will be periodically and randomly monitored to ensure compliance with this policy. 4. Reporting Breaches

4.1 All Workforce members have an obligation to immediately report privacy and security breaches that they suspect or of which they have direct knowledge to 4PTS, the Privacy Officer, and/or, the Corporate Compliance Officer, and/or the Information Security Officer (when security implications exist).

4.1.1 AAHS will not take any adverse or other action against any Workforce member who reports an actual or suspected privacy or security breach as long as the report is made in good faith and the Workforce member him- or herself was not actively, intentionally or willfully involved in the breach. However, knowingly making a false report will result in sanctions.

4.1.2 No AAHS Workforce member shall intimidate, threaten, coerce, discriminate against or take other retaliatory action against any individual who files a complaint or reports a possible breach, or who cooperates in the investigation or disciplinary action arising from a complaint or report.

4.1.3 If reported via 4PTS, enough information must be included in order to follow-up with an investigation; such as, but not limited to: (a) the location of the incident (unit), or (b) identification of an employee with whom the matter may be discussed, along with a description of what occurred.

<u>5. Levels of information security and privacy breaches:</u>

5.1 Level I: Carelessness: A violation of PHI security and privacy by unintentional means or carelessness.

<u>Examples include, but are not limited to:</u>

5.1.1. Discussing patient information in a public area.

5.1.2. Leaving a copy of a patient's health information in a public area.

5.1.3. Forgetting to log-off the computer when leaving the immediate area surrounding the computer.

5.1.4. Sending unencrypted PHI over the internet.

5.1.5. Failing to install security passwords on a PDA which contains a patient's PHI. 5.2. Level II: Curiosity or Concern (No Personal Gain): An intentional violation of PHI security and privacy for reasons unrelated to personal gain.

Examples include, but are not limited to:

5.2.1. Looking up the birth date, address, or health information of a friend or relative.

5.2.2. Reviewing anyone's medical record out of curiosity or concern.

5.2.3. More than one attempt to sign-on to a system which the Workforce member is not authorized to access. (One attempt is assumed to be accidental).

5.2.4. Sharing a password with another person so he/she can sign-on to system. 5.3. Level III: Personal Gain or Malice: A violation of information security and privacy policy for personal gain or with malicious, willful or wanton intent.

Examples include, but are not limited to:

5.3.1. Corrupting patient information.

5.3.2. Compiling a mailing list for sale or personal use.

5.3.3. Use of a patient's identifying information to gain access to the patient's financial information and/or records for personal gain.

5.3.4. Reviewing a patient record to use the information in a personal relationship.

5.3.5. Obtaining AAHS records for the purposes of treatment of the patient and then releasing the AAHS records to an attorney or law enforcement officer or agency for legal purposes.

5.3.6. Accessing PHI with the intent to sell information (i.e. to the Media).

6. Investigations

6.1. AAHS Workforce members are expected to comply and cooperate with AAHS's investigation and corrective actions for violations of privacy and/or security laws, regulations and policies.

6.2. The Privacy Officer or Information Security Officer (as appropriate) shall coordinate a thorough and confidential investigation of all alleged breaches commensurate with the level of the breach. The investigation process may involve, but not be limited to, interviewing the Workforce member accused of the breach, interviewing other individuals, computer access audit trails, and reviewing documentation.

6.2.1. Investigations of a breach involving Workforce will be conducted in coordination with Human Resources, and/or the Privacy Officer, and/or the Information Security Officer as necessary and appropriate.

6.2.2. The Corporate Compliance Officer should be made aware of all breach-related investigations until all related issues are closed.

7. Actions/Sanctions

7.1. Appropriate sanctions will be assessed for each confirmed violation. Assessed sanctions are based on the Human Resources Discipline Policy (**HR8.3.01** - "**Discipline**") and will be enforced according to the severity of the violation, the prior history of the Workforce member and the discretion of the Workforce member's immediate supervisor, as follows:

7.1.1. Incidents of Level I: CarelessnessIncidents confirmed as carelessness will fall under Group I disciplinary action.

7.1.2. Incidents of Level II: Curiosity or Concern (no personal gain) Incidents confirmed as curiosity or concern will fall under Group II disciplinary action.

7.1.3. Incidents of Level III: Personal Gain or Malice

Confirmed violations of this type will fall under Group III or Group IV depending on severity and will be referred to Human Resources along with The HIPAA Steering Committee for collaboration of corrective action pursuant to the Human Resources Discipline Policy (**HR8.3.01** - "**Discipline"**).

7.2. Appropriate actions / sanctions for each confirmed violations by Hospitalists will be applied according to the severity of the violation, the prior history of the Hospitalist and in accordance with the Medical Staff Bylaws, rules, regulations, and policies (articles 7.3 - 7.6).

7.3. Violators of patient's confidentiality and privacy under the Health Insurance Portability and Accountability Act (HIPAA) may be subject to federal fines and penalties and may be reported to regulatory, accreditation, law enforcement, and licensure organizations for misuse or misappropriation of health information.

7.4. If the investigation of an alleged breach concludes that a system, procedure or policy of AAHS needs to be addressed, the owner of the related AAHS policy will be notified by either Human Resources, The Privacy Officer, the Corporate Compliance Officer, Information Security Officer, or other appropriate person, to facilitate any necessary revisions or changes.

7.5. Sanctions do not apply when a member of the Workforce in good faith, discloses PHI to a health oversight agency, public health authority or other entity authorized by law to oversee health care conduct or conditions, health care accreditation organization or attorney for purposes of reporting unlawful conduct, violations of professional or clinical standards or care, services, or conditions at AAHS that potentially endangers one or more patients, workers, or the public.

8. Documentation

8.1. The Privacy, Information Security Officer, and/or Corporate Compliance Officer (as appropriate), will maintain documentation relating to investigations that occur under this policy for a period of six (6) years.

8.2. Any documentation of an action taken in accordance with this section 3.7 of this policy shall be placed in the Workforce member's employment file.

For questions and/or assistance, please call the AAHS Privacy Officer at 443.481.4130.

References

1996 Health Insurance Portability and Accountability Act (HIPAA) Public Law 104-191: Privacy Rule 164.524.

Security and Electronic Signature Standards; Proposed Rule, 45 CFR Part 142, Section 142.308(a)(iii).

Standards for Privacy of Individually Identifiable Health Information, 45 CFR, Part 164, Subpart E, Section 164.530 (e).

Maryland Code Health General Article § 4-301. Definitions; § 4-304. Copies of records: changes in records.

Cross References

HR8.3.01 - "**Discipline"** – "Discipline Policy"

Medical Staff Bylaws