IOWA HEALTH SYSTEM

Title: Discipline/Corrective Action for Breaches of PHI 1.HR.04

Effective Date: 08/11; Rev: 07/12

POLICY: This policy describes the manner in which IHS is protecting patient privacy and security by investigating all alleged/suspected patient privacy violations, violations of IHS security policies and procedures, and setting system-wide standards for the discipline/corrective action of its employees regarding breaches of patients' protected health information ("PHI") and violations of IHS security policies and procedures.

SCOPE: IHS system wide. All IHS and affiliate facilities including, but not limited to, hospitals, ambulatory surgery centers, home care programs, physician practices, all IHS and affiliate departments, and covered group health plans.

BACKGROUND: Iowa Health System ("IHS") is committed to ensuring compliance with all applicable privacy and security laws, regulations, standards, policies, and procedures including the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder ("HIPAA") and the HITECH Act of 2009.

PROCEDURES:

1. **Definitions**.

1.1 "Protected Health Information (PHI)" is defined as information that:

1.1.1 Is created or received by a Covered Entity or employer; and

1.1.1.1 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 payment therefor; and

1.1.1.2 Identifies the individual or could be used to identify the individual.

1.1.2 The following is a non-exclusive list of data items considered to be identifiable:

1.1.2.1 Name;

1.1.2.2 Geographic subdivision smaller than state;

1.1.2.3 All elements of date of service except year;

1.1.2.4 Telephone number(s);

1.1.2.5 Fax number(s);

1.1.2.6 E-mail addresses;

1.1.2.7 Social Security numbers;

1.1.2.8 Medical record numbers;

1.1.2.9 Health plan beneficiary numbers;

1.1.2.10 Account numbers;

1.1.2.11 Certificate/license numbers;

1.1.2.12 Vehicle identifier and serial numbers;

1.1.2.13 Device identifiers and serial numbers;

1.1.2.14 Web universal resource locators (URLs);

1.1.2.15 Internet protocol (IP) address numbers;

1.1.2.16 Biometric identifiers, including finger and voice prints;

1.1.2.17 Full face photographic images and any comparable images; and

1.1.2.18 Any other unique identifying number, characteristic or code.

1.1.3 PHI excludes the following:

1.1.3.1 Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

1.1.3.2 Student medical records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and

1.1.3.3 Employment records held by a Covered Entity in its role as employer.

1.2 "Access" means to locate and read or view the information.

1.3 "Disclosure" means to release, transfer, provide access to, or divulge in any manner the information to other employees who do not need the information to do their jobs, or outside the entity holding the information.

2. **Types of Violations**. The type of the breach of patient confidentiality, privacy violation, or security violation shall be determined according to the severity of the breach or violation, whether the breach or violation was intentional or unintentional (e.g., by reason of an error or inadvertently as a result of patient care), and whether the breach or violation indicates a pattern or practice of improper use or disclosure of confidential patient information, violation of patient privacy, or violation of IHS security policies and procedures. The degree of discipline may range from coaching to immediate termination, as determined by the investigation and the severity of the breach or violation.

Generally, the three types of breach or violation are as listed below. However, an affiliate may treat a breach or violation as a higher category of breach/violation based upon the facts of a specific breach or violation.

2.1 Carelessness or Inadvertent. Defined as an unintentional or careless access, review, or disclosure by an employee and/or disclosure of PHI without a legitimate "need to know." Examples include, but are not limited to:

2.1.1 Employee discusses confidential patient information in a public area;

2.1.2 Employee leaves a patient's medical record unattended in an accessible area;

2.1.3 Employee forgets to log off a computer terminal;

2.1.4 Employee unintentionally leaves a computer terminal unattended in an accessible area with PHI unsecured; and

2.1.5 Employee carelessness or inattention to detail relating to PHI, such as faxing to the wrong fax number or selecting the wrong physician upon registration.

2.2 Failure to Follow Policy or Access for Curiosity or Concern (no personal gain). Defined as failure to follow established privacy and security policies or an intentional access or disclosure of PHI for purposes other than patient care or other authorized reason, but unrelated to personal gain. Examples include, but are not limited to:

2.2.1 Failure to comply with established privacy and security policies such as policies prohibiting the sharing of passwords or leaving mobile devices containing PHI unattended;

2.2.2 Employee looks up birth dates or addresses of friends or relatives;

2.2.3 Employee accesses and reviews a patient's medical record out of concern or curiosity;

2.2.4 Employee routinely fails to log off computer terminal;

2.2.5 Employee routinely leaves a computer terminal unattended in an accessible area with PHI unsecured; and

2.2.6 Employee reviews a public personality's record out of curiosity.

2.3 Personal Gain or Malice. Defined as an intentional access or disclosure of PHI for personal gain or with malicious intent. Examples include, but are not limited to:

2.3.1 Employee accesses or discloses PHI for use in a personal relationship;

2.3.2 Employee gathers PHI to be sold.

3. **Discipline/Corrective Action**. Discipline/corrective action shall be administered as appropriate under an IHS affiliate's Human Resources policies and procedures. The following are guidelines for discipline/corrective action for confidentiality breaches, privacy violations and security violations. Risks to patient or employees and other serious offenses may warrant deviation from these guidelines.

3.1 Carelessness or Inadvertent.

3.1.1 *First Offense*: Depending on the facts, discipline/corrective action may include coaching, education, a verbal or written warning, suspension or termination of employment. Except in the case of termination, the employee may be required to repeat the HIPAA NetLearning module.

3.1.2 *Second and Later Offense(s) that occur within twelve (12)-month period*: Progressive discipline. Additional violations of this type (careless or inadvertent) that occur after twelve (12) months shall be treated as a First Offense.

3.2 Failure to Follow Policy or Curiosity or Concern (no personal gain).

3.2.1 *First Offense*: Depending on the facts, discipline/corrective action may include a final written warning and suspension without pay, or

termination. Except in the case of termination, the employee may be required to repeat the HIPAA NetLearning module.

3.2.2 *Second Offense*: Termination.

3.3 Personal Gain or Malice.

3.3.1 Termination.

4. **Employee Cooperation/Mitigation**. In determining the appropriate discipline or corrective action for breaches of PHI, an affiliate shall take into account the following factors:

4.1 Whether the employee took prompt and appropriate steps to mitigate the harmful effects of the breach;

4.2 Whether the employee promptly and voluntarily reported the breach; and

4.3 The extent to which the employee cooperated in the investigation of the matter.

/s/ William B. Leaver

_____

William B. Leaver
IHS President