Current Status: *Active* **PolicyStat ID:** *9778518*

Origination: *06/2014*
Last Approved: *06/2021*
Last Revised: *06/2021*
Next Review: *06/2022*
Owner: *Andrew Violet: Senior Security Analyst*
Area: *Information Technology - Security Policies*
References:
Applicability: *Des Moines University*

Information Security and Privacy Overview Policy

The Purpose, Scope, Governing Policy, and Definitions in this policy apply to all Des Moines University Information Security and Privacy Policies.

I. PURPOSE

The purpose of Des Moines University Osteopathic Medical Center Information Security and Privacy Policies is to:

a. Protect Des Moines University Osteopathic Medical Center (hereinafter "University") information and system resources.
b. Help to ensure the confidentiality, integrity, and availability of information assets.
c. Establish an information security and privacy policy management and governance structure.
d. Create awareness for personnel and other workforce personnel in making information security decisions in accordance with information security and privacy policies.
e. Help protect student, patient, and employee information from unauthorized use, disclosure, modification, or destruction.
f. Provide direction to those responsible for the design, implementation and maintenance of systems that support the University's operations.
g. Clarify management and other workforce personnel responsibilities and duties with respect to the protection of information assets and resources.
h. Support compliance with applicable legal and regulatory requirements.
i. Establish the basis for internal and external audits, reviews and assessments.

II. SCOPE

1. The University information security and privacy policies define common security and privacy requirements for all University personnel and systems that create, maintain, store, access, process or transmit information. The University information security and privacy policies apply to all University personnel, including contracted workers, consultants and others given access to the University applications, systems, and/or information.
2. The policies pertain to all University systems, applications and information in all forms in all locations where University business processes are performed.

3. The policies also apply to information resources owned by others, such as contractors of the University and entities in the private sector, in cases where University has a legal, contractual or fiduciary duty to protect said resources while in University custody. In the event of a conflict, the more restrictive measures apply.
4. The policies covers the University network system which is comprised of various hardware, software, communication equipment and other devices designed to assist the University in the creation, receipt, storage, processing, and transmission of information. This definition includes equipment connected to any University domain or VLAN, either hardwired or wireless, and includes all stand-alone equipment that is deployed by the University at its office locations or at remote locales. The policies will be reviewed annually.
5. The policies will be communicated to all personnel who have any type of access to business information assets.

III. POLICY

A. Governing Policy Statement

The University possesses information that is sensitive and valuable (for example, personal health information, personally identifiable information, financial data, building plans, and research information) as well as information that is required for business processes. Some information is protected by federal and state laws and/or contractual obligations that prohibit its unauthorized use or disclosure. Access to this information by unauthorized individuals could cause irreparable harm to the University or members of the University community, and could also subject the University to fines or other government sanctions. Additionally, if University information were tampered with or made unavailable, it could impair its ability to do business.

The University therefore requires all employees, contracted workers, and students to protect information, and the supporting information assets (such as computing devices and storage media) as specified within the associated information security and privacy policies and supporting procedures. All employees are required to know and follow all these policies.

B. Definitions

Common terms and acronyms that may be used throughout the University information security and privacy policies include:

1. Breach: The unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. The term "breach" does not include—
    a. any unintentional acquisition, access, or use of protected health information by an employee or individual acting under the authority of a covered entity or business associate if—
        - such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the covered entity or business associate; and
        - such information is not further acquired, accessed, used, or disclosed by any person; or
    b. any inadvertent disclosure from an individual who is otherwise authorized to access protected health information at a facility operated by a covered entity or business associate to another similarly

situated individual at same facility; and

c. any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person.

2. Education Records:

   a. The term means those records that are:

      - Directly related to a student; and
      - Maintained by an educational agency or institution or by a party acting for the agency or institution.

   b. The term does not include:

      - Records that are kept in the sole possession of the maker, are used only as a personal memory aid, and are not accessible or revealed to any other person except a temporary substitute for the maker of the record.
      - Records of the law enforcement unit of an educational agency or institution.
      - The following:
        - Records relating to an individual who is employed by an educational agency or institution, that:
          - Are made and maintained in the normal course of business;
          - Relate exclusively to the individual in that individual's capacity as an employee; and
          - Are not available for use for any other purpose.
        - Records relating to an individual in attendance at the University who is employed as a result of his or her status as a student are education records and not excepted under paragraph 2. b. of this definition.
      - Records on a student who is 18 years of age or older, or is attending an institution of postsecondary education, that are:
        - Made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his or her professional capacity or assisting in a paraprofessional capacity;
        - Made, maintained, or used only in connection with treatment of the student; and
        - Disclosed only to individuals providing the treatment. For the purpose of this definition, "treatment" does not include remedial educational activities or activities that are part of the program of instruction at the agency or institution;
      - Records created or received by an educational agency or institution after an individual is no longer a student in attendance and that are not directly related to the individual's attendance as a student.
      - Grades on peer-graded papers before they are collected and recorded by a teacher.

3. Directory Information for Education Records

   a. The Family Educational Rights and Privacy Act (FERPA) defines Directory Information as information contained in the education records of a student that would not generally be considered harmful or an invasion of privacy if disclosed. The following student information is available for release to the

public:

i. Name, local address, telephone number

ii. DMU email address

iii. Major field(s) of study

iv. Year in program(s)

v. Dates of attendance

vi. Enrollment status

vii. Degrees and awards received

viii. Participation in officially recognized activities

b. Further information regarding FERPA and disclosure of information is available at: www.dmu.edu/registrar/ferpa

c. Information that has been properly de-identified or that is shared under the "Directory Information" exception, is not protected by FERPA and is not subject to FERPA's use and re-disclosure limitations.

4. Electronic Protected Health Information (EPHI): Protected health information (PHI) in any type of electronic form.

5. Health Information Technology (HIT): The term 'health information technology' means hardware, software, integrated technologies or related licenses, intellectual property, upgrades, or packaged solutions sold as services that are designed for or support the use by health care entities or patients for the electronic creation, maintenance, access, or exchange of health information.

6. Individual Notice: Notice provided to an individual, with respect to a breach, that is provided promptly and in the following form:

a. Written notification by first-class mail to the individual (or the next of kin of the individual if the individual is deceased) at the last known address of the individual or the next of kin, respectively, or, if specified as a preference by the individual, by electronic mail. The notification may be provided in one or more mailings as information is available.

b. In the case in which there is insufficient, or out-of-date contact information (including a phone number, email address, or any other form of appropriate communication) that precludes direct written (or, if specified by the individual, electronic) notification to the individual, a substitute form of notice shall be provided, including, in the case that there are 10 or more individuals for which there is insufficient or out-of-date contact information, a conspicuous posting for a period determined by the Secretary on the home page of the Web site of the covered entity involved or notice in major print or broadcast media, including major media in geographic areas where the individuals affected by the breach likely reside. Such a notice in media or web posting will include a toll-free phone number where an individual can learn whether or not the individual's unsecured protected health information is possibly included in the breach.

c. In any case determined to require urgency because of possible imminent misuse of unsecured protected health information, in addition to notice described in (A), notice may be provided to individuals by telephone or other means, as appropriate.

7. Individually identifiable health information (IIHI): This has the same meaning as protected health information (PHI).

8. Protected Health Information (PHI): Protected health information (PHI) means individually identifiable health information described as follows:
    a. That is:
        - Transmitted by electronic media;
        - Maintained in electronic media; or
        - Transmitted or maintained in any other form or medium.
    b. PHI excludes individually identifiable health information in:
        - Education records covered by the Family Educational Rights and Privacy Act (see definition of Education Records).
        - Records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice.
        - Employment records held by a covered entity in its role as employer
        - Regarding a person who has been deceased for more than 50 years.
    c. PHI is information that 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, employer, or health care clearinghouse; and
        - 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
            - With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
    d. The following are the 18 explicitly identified PHI items:
        - Names
        - Geographic subdivisions smaller than a state
        - All elements of dates directly related to the individual (Dates of birth, marriage, death, etc.)
        - Telephone numbers
        - Facsimile numbers
        - Driver's license numbers
        - Electronic mail addresses
        - Social security numbers
        - Medical record numbers

- Health plan beneficiary numbers
- Account numbers, certificate/license numbers
- Vehicle identifiers and serial numbers
- Device identifiers and serial numbers
- Web Universal Resource Locator's (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers
- Full face photographic images and any comparable images
- Genetic data

9. Additionally, any information that can be linked to a specific individual will also be considered to be PHI.
10. Information security: the preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.
11. Data Steward: This is the position or department that is ultimately responsible for ensuring specified types of information is appropriately safeguarded.
12. Media Notice: Notice provided to prominent media outlets serving a state or jurisdiction, following the discovery of a breach, if the unsecured protected health information of more than 500 residents of the State or jurisdiction is, or is reasonably believed to have been, accessed, acquired, or disclosed during the breach.
13. Personally Identifiable Information (PII): Any piece of information, or combination of information items, that can be associated with one individual. PII items are typically considered to be those explicitly specified with any one of a number of data protection and privacy laws.
    a. For the purpose of meeting security breach notification requirements, PII is defined as a person's first name or first initial and last name in combination with one or more of the following data elements:
        i. Social security number
        ii. State-issued driver's license number
        iii. State-issued identification card number
        iv. Financial account number in combination with a security code, access code or password that would permit access to the account
        v. Medical and/or health insurance information
    b. For the purpose of maintaining the confidentiality of records, PII is also defined as:
        i. Person's ID number in combination with a security code, access code or password that would permit access to the student's education records or other confidential information.
        ii. A list of personal characteristics that would make the person's identity easily traceable (for example, a combination of gender, birth date, and zip code).
14. Personal Information: This is information that can be linked to a specific individual, group of individuals, or reveal activities or other types of characteristics of an individual or group. Many types of personal information are not explicitly protected by any law or regulation. PII is a subset of personal information.
15. Qualified Electronic Health Record: The term 'qualified electronic health record' means an electronic record of health-related information on an individual that—

a. includes patient demographic and clinical health information, such as medical history and problem lists; and

b. has the capacity—

- to provide clinical decision support;
- to support physician order entry;
- to capture and query information relevant to health care quality; and
- to exchange electronic health information with, and integrate such information from other sources.

C. Applicable Laws/Regulations/Legal Requirements

1. The University must follow all HIPAA and HITECH requirements in addition to all other applicable laws, mandates, regulations and legal requirements.
2. The University will identify and document all legal requirements by following the *Legal: Regulatory, Contractual & Standards Compliance Procedure.*

D. Policy Exceptions

1. Exceptions to the information security and privacy policies may be granted in unusual and unique circumstances when it is not possible to be in compliance with a specific policy.
2. Exceptions will be coordinated with appropriate Management, Compliance, Human Resources personnel.
3. The Information Security Officer must document within the written approval the mitigating controls that must be followed for the exception, along with the reasonable time period for which the exception is granted.

Approved By:

Angela Franklin, Ph.D., President

Attachments

No Attachments

Approval Signatures

Approver	Date
Angela Franklin: President	06/2021
Carolyn Weaver: Chief Information Officer	06/2021

Approver	Date
Keith Grey: Associate Chief Information Officer	06/2021
Andrew Violet: Senior Security Analyst	06/2021

Applicability

Des Moines University