Health Information Privacy and Security (HIPAA)

Effective: April 14, 2003
Updated/Revised: February 12, 2009
Contact: Thielen Student Health Center

Contents

Introduction

Iowa State University (ISU) is committed to protecting the privacy and security of personal health information concerning our employees and students. This policy is designed to assure ISU's compliance with all applicable federal and state laws and regulations that require an individual's personal health information to be kept confidential and private. It is the result of a comprehensive review performed by the HIPAA Compliance Task Force.

Applicable Laws and Regulations

Personal health information is required to be kept confidential and private under a number of federal and state laws and regulations. For example,

- Iowa Code Chapter 22.7(2) addresses the confidentiality of public hospital, medical and professional counselor records;
- Iowa Code Chapter 228 addresses the disclosure of mental health and psychological information;
- The Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232(g) and 34 CFR Part 99 address the confidentiality of student education records; and
- The Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. 1320(d) and 45 CFR Parts 160 and 164 address the confidentiality of patient health information and records.

Although the development of this policy has been motivated by HIPAA and its accompanying regulations, Iowa State University health care providers have always had policies and procedures that addressed the confidentiality of personal health information. Since there are numerous state and federal laws and regulations that apply to the confidentiality and privacy of personal health information, this policy intends to bring together in one comprehensive policy the commitment ISU has for compliance with those federal and state laws and regulations. This is true whether the personal health information is protected by HIPAA, FERPA, other state or federal laws and regulations, or a combination of federal and state laws and regulations.
top

Policy Statement

It is the policy of ISU to comply with all federal and state laws and regulations that require personal health information of our employees and/or students to be kept confidential and private.

Hybrid Entity

Since the primary mission of ISU is education, and only part of our activities include covered functions under the final HIPAA Privacy Rule, ISU has determined that it is a hybrid entity for purposes of HIPAA. The ISU hybrid entity will have two parts. First is the Health Care Provider component that contains the departments that provide health-related services. The second is the Health Plan component that includes certain health plans within the ISU Benefits Office that are self-insured, are determined to be covered by the HIPAA regulations, and must therefore comply with HIPAA.

The ISU Health Care Provider component includes the following units:

- Thielen Student Health Center;
- Thielen Student Health Center Pharmacy;
- ISU Student Counseling Service;
- Cyclone Sports Medicine/Physical Therapy; and
- ISU Athletic Training.

The ISU Health Plan component includes:

- The self-insured ISU Plan including the Indemnity, PPO and HMO plans;
- The Basic and Comprehensive Dental plans; and
- The Medical Reimbursement Flexible Spending Account program.

There are also administrative support units within ISU that provide assistance to our designated Health Care Provider component and designated Health Plan component. These support units are part of the ISU hybrid entity and include:

- Information Technology Services;
- Accounts Receivable;
- Internal Audit;
- University Counsel; and
- Risk Management.

In the process of developing this policy, all departments within ISU were reviewed by the HIPAA Task Force to determine whether or not they should be included within the ISU hybrid entity. Although the following departments occasionally would come in contact with or maintain personal health information about an employee or student in departmental records, it was determined that these departments are not to be designated as part of the ISU hybrid entity:

- Dean of Students;
- Student Accessibility Services (SAS);
- Employee Assistance Program (EAP);
- Facilities, Planning and Management;
- Family and Marriage Therapy Clinic;
- Kinesiology;
- University Human Resources;
- Lied Fitness Center;
- Occupational Medicine;
- Department of Public Safety;
- Procurement Services;

- Student Financial Aid;
- Student Health Insurance;
- Treasurer; and
- Workers' Compensation Program.

top

Office for Responsible Research

Special attention to the Office for Responsible Research was given by the HIPAA Task Force. Although it does not provide covered functions under HIPAA, it has the important responsibility of educating researchers about the impact of HIPAA on human subjects research.

ISU does conduct some research that involves personal health information of the research subjects. Research that involves human subjects is reviewed and approved by the Institutional Research Board (IRB) at ISU.

In the context of human subject research, personal health information of our employees and students is protected by the federal "common rule" under which the ISU IRB must operate. The Office for Responsible Research and the IRB at ISU are not designated as part of our hybrid entity. The Office for Responsible Research will be responsible for educating researchers conducting human subjects research to comply with HIPAA regulations involving privacy and security of the personal health information of the human subjects that are the focus of their research. This generally requires that an appropriate authorization be obtained from the subject of the research unless the IRB has determined that a waiver of the authorization requirement is appropriate.

The Office for Responsible Research and the IRB will provide education to researchers about the appropriate elements of an authorization for use in human subject research. They also can provide researchers with information about how to seek personal health information from health care providers by using that authorization, a limited data set agreement or, if the data sought is preparatory to their research, obtaining de-identified information. However, the ultimate determination of when disclosure will be made in these circumstances, and the final review and approval of disclosure pursuant to an authorization, will be made by the health care provider that possesses the personal health information of the research subject.

Health Information Privacy Officer

The Health Information Privacy Officer at ISU is responsible for development and implementation of policies, procedures and educational programs that will assure compliance with the various federal and state laws and regulations that require personal health information to be kept confidential and private. This person will provide leadership to the overall management of ISU's health information privacy compliance and will chair the ISU Health Information Privacy Compliance Committee.

The Health Information Privacy Officer shall have the responsibility and authority to:

- Develop and implement the ISU Policy and Procedures concerning the privacy and security of personal health information of ISU employees and students as determined by the ISU Health Information Privacy Compliance Committee.
- Provide oversight of privacy practices within the ISU designated health care provider components.
- Receive and investigate complaints concerning the use and disclosure of personal health information by the ISU designated health care provider components.
- Develop and implement an organization-wide training program in collaboration with the ISU designated health care provider components.

- Review, update and improve, where necessary, the policies and practices of the ISU designated health care components as they relate to the privacy of personal health information of our employees and students.

The Health Information Privacy Officer for ISU is the Director of the Thielen Student Health Center.

The Health Information Privacy Officer will be assisted by a Health Information Privacy Compliance Committee, as described in Section 7. In addition, the director of each ISU health care provider shall designate an employee to be the contact person for health information privacy within the department. That person will act as the liaison for the department to the Health Information Privacy Officer. The ISU Office of University Counsel will provide legal advice to the Health Information Privacy Officer.

top

Health Information Security Officer

ISU has determined that the responsibility for the security of health information on campus should be placed with the Information Technology Services department since most of the personal health information that must be kept secure will exist electronically.

The Health Information Security Officer is responsible for development and implementation of policies, procedures and educational programs that will assure that each designated health care provider and the ISU Benefits Office have in place appropriate administrative, technical and physical safeguards to protect the privacy of the personal health information of our employees and students. In addition, the director of each ISU health care provider and the ISU Benefits Office shall designate an employee to be the contact person for health information security within the department. That person will act as the liaison for the department to the Health Information Security Officer.

The Health Information Security Officer will be a permanent member of the Health Information Privacy Compliance Committee. The Health Information Security Officer for ISU is the person from Information Technology Services who is responsible for information technology involving medical records at the Thielen Student Health Center.

Health Information Privacy Compliance Committee

To assist in assuring that the personal health information of our employees and students is kept confidential and private, a permanent committee, the Health Information Privacy Compliance Committee, is formed. The chair of this committee shall be the Health Information Privacy Officer. Other members of the committee shall include:

- The Health Information Security Officer.
- A person from each ISU health care provider who has the responsibility within the designated health care component for privacy policy and procedures or security policy and procedures. This person shall be designated by the director of the respective health care provider.
- A person designated by the ISU Benefits Office.
- A person designated by the Office for Responsible Research.
- A person designated by the ISU Office of University Counsel.

The persons designated to be liaisons to the Health Information Security Officer will not be members of the Health Information Compliance Committee but could be invited to provide advice to the Committee on any security related issue.

The responsibility of this committee is to provide advice and support to the Health Information Privacy Officer and assist in developing, monitoring, implementing, and revising ISU's policy and procedures requiring confidentiality and privacy of the personal health information of our employees

and students. The Committee is delegated the authority to develop the specific details of ISU policy and procedure to assure compliance with health information privacy laws and regulations.

Notice of Privacy Practices

ISU shall have two specific Notices of Privacy Practices. One will apply to the designated health care providers within our hybrid entity, and the other will apply to our health plans within the ISU Benefits Office (see Resources below).

It is the responsibility of the Health Information Privacy Officer and the Health Information Privacy Compliance Committee to monitor and review the privacy practices and procedures described in the Notice of Privacy Practices, make revisions as necessary, and communicate any revised notice to our employees and students, as required by various federal and state laws and regulations.

top

Resources

Links

- Employee Benefits
- Code of Federal Regulations (CFR)
- Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232(g)
- FERPA, U.S. Department of Education
- Health Information Privacy Compliance Committee
- Health Insurance Portability and Accountability Act (HIPAA)
- Institutional Review Board (IRB)
- Iowa Code
- Office for Responsible Research
- Student Records
- Thielen Student Health Center
- University Counsel
- Notice of Privacy Practices for ISU Healthcare Providers [PDF]