# Table of Contents

**Introduction** ................................................................................................................................. 4

**Definitions** ........................................................................................................................................ 5

**Access, Use, and Disclosure** ........................................................................................................... 12
- Minimum Necessary .......................................................................................................................... 12
- Limited Data Sets ............................................................................................................................. 12
- De-Identified PHI .............................................................................................................................. 13
- Protecting Verbal and Written PHI ................................................................................................. 14
- Disclosure Verification ....................................................................................................................... 15
- Disclosure Consent, and Authorization ............................................................................................ 15
- Disclosure for Healthcare Operations .............................................................................................. 18
- Disclosure for Healthcare Treatment ................................................................................................. 18
- Disclosure as Required by Law ......................................................................................................... 19
- Disclosure for Public Health and Safety .......................................................................................... 20
- Disclosure to Others ......................................................................................................................... 21
- Disclosure about Deceased Patients ............................................................................................... 22
- Disclosure for Employees ............................................................................................................... 23
- Disclosure for Specialized Government Functions ......................................................................... 23
- Disclosures for Research .................................................................................................................. 23
- Disclosure to Business Associates .................................................................................................. 24
- Disclosure for Marketing .................................................................................................................. 25
- Disclosure for Fundraising .............................................................................................................. 26
- Disclosure in Meetings ..................................................................................................................... 26
- Psychotherapy Notes ........................................................................................................................ 27
- Use of Email ...................................................................................................................................... 27
- Use of Fax Machines ........................................................................................................................ 28
- Public Areas ..................................................................................................................................... 28
- No Sale ............................................................................................................................................ 29
- Disclosure Tracking .......................................................................................................................... 29
- Privacy Breach .................................................................................................................................. 30

**Patient Rights** ................................................................................................................................ 34
Introduction

Idaho State University (ISU) is committed to protecting the privacy, security, integrity, confidentiality, and availability of personal health information (PHI) it is entrusted with. This manual was created to assist ISU in complying with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the HITECH Act.

ISU is a hybrid entity, in accordance with ISU’s HIPAA Privacy Policy, ISUPP 10010. Only the healthcare components (covered functions) of ISU must comply with this manual. All references to ISU in this manual shall be construed to mean only the healthcare components of ISU.

This manual sets forth the administrative, technical, and physical safeguards that shall reasonably protect PHI from access, use, and disclosure that violate the law.

ISU reserves the right to revise this manual at any time. When changes are made, ISU shall promptly notify and educate the workforce members on the changes. Workforce members are responsible for understanding and complying with this manual. Violations will not be tolerated and may subject the workforce member to disciplinary action, up to and including termination.
Definitions

The terms and acronyms used in this manual have the following definitions and meanings. However, in the event any definition differs from the definition provided by the HIPAA rules and regulations, the definition set forth by HIPAA shall govern. These are general definitions and not intended to be a complete glossary of all terms:

**Accounting of Disclosures:** A written record of certain disclosures of PHI that may be required to be maintained and provided to a requesting individual under certain prescribed circumstances.

**Authorization:** A written document completed and signed by an appropriate individual that generally allows use and/or disclosure of PHI for purposes other than treatment, payment, or healthcare operations.

**Breach:** The unauthorized acquisition, access, use, or disclosure of PHI in a manner not permitted by HIPAA, which compromises the security or privacy of PHI.

**Business Associate:** A person, entity, company, or organization that is not a member of ISU’s workforce and yet performs a function or activity on behalf of ISU that involves the use or disclosure of PHI.

**Business Associate Agreement (BAA):** A contract between ISU and a business associate, or between a business associate and its business associate subcontractor that establishes the permitted and required uses and disclosures of PHI by the business associate.

**Common Rule:** The Federal Policy for Protection of Human Subjects described in 45 CFR Part 46, Subpart A. The Common Rule provides protections for individuals and establishes the role of institutional review boards in achieving those protections.

**Consent:** A document signed and dated by the patient or guardian/representative that a covered entity obtains prior to using or disclosing PHI to carry out treatment, payment, or healthcare operations.

**Covered Entity:** A health plan, healthcare clearinghouse, or healthcare provider that is covered by HIPAA.

**Covered Functions:** Those functions of an entity the performance of which makes the entity a health plan, healthcare provider, or healthcare clearinghouse (that is, the function makes the entity a “covered entity” subject to HIPAA.)

**Data Breach:** a use or disclosure of unsecured PHI as described in 45 C.F.R. § 164.400 et seq.

**De-identified Information:** Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. De-identified information is not subject to the HIPAA Privacy Rule.

**Department of Health and Human Services:** The U.S. Department of Health and Human Services, of which the Office of Civil Rights is a part, and is charged with the development, implementation, and enforcement of the Privacy Rule.
Designated Record Set:
1. A group of records maintained by or for a covered entity that includes:
   a. Medical records and billing records used by a covered entity to make decisions about an individual;
   b. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
   c. Use, in whole or in part, by or for the plan to make decisions about individuals.
2. For purposes of this definition, the term record means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity. It includes patient information originated by another healthcare provider and used by the covered entity to make decisions about the patient, tracings, photographs, videotapes, digital and other images that may be recorded to document care of the patient.

Disclosure: The release, transfer, provision of access to, or divulging in any other manner, information outside the entity holding the information.

Employer: As defined by the Internal Revenue Code, 26 U.S.C. 3401(d): “For purposes of this chapter, the term “employer” means the person for whom an individual performs or performed any service, of whatever nature, as the employee of such person, except that:
1. if the person for whom the individual performs or performed the services does not have control of the payment of the wages for such services, the term “employer” (except for purposes of subsection (a)) means the person having control of the payment of such wages, and
2. in the case of a person paying wages on behalf of a nonresident alien individual, foreign partnership, or foreign corporation, not engaged in trade or business within the United States, the term “employer” (except for purposes of subsection (a)) means such person.”

Electronic PHI (ePHI): Any PHI that is maintained or transmitted in electronic media and may be accessed, transmitted, or received electronically.

Fundraising: The solicitation of funds to benefit the healthcare component of the ISU hybrid entity. Permissible fundraising activities include appeals for money, sponsorship of events, etc. Fundraising does not include royalties or remittances for the sale of products of third parties (except auctions, rummage sales, etc.).

Healthcare: Care, services, or supplies related to the health of an individual. Healthcare includes, but is not limited to, the following:
1. Preventative, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
2. Sale or dispensing of a drug, device, equipment or other item in accordance with a prescription.

Healthcare Clearinghouse: A public or private entity including a billing service, re-pricing company, community health management information system or community health information system, and “value-added” networks and switches that does either of the following functions:
1. Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction;
2. Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

**Healthcare Operations:** Any of the following activities of the covered entity to the extent that the activities are related to covered functions:

1. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing healthcare costs, protocol development, case management and care coordination, contacting of healthcare providers and patients with information about treatment alternatives; and related functions that do not include treatment;
2. Reviewing the competence or qualifications of healthcare professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of healthcare learn under supervision to practice or improve their skills as healthcare providers, training of non-healthcare professionals, accreditation, certification, licensing, or credentialing activities;
3. Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for healthcare (including stop-loss insurance and excess of loss insurance), provided that the requirements of 45 CFR § 164.514(g) are met, if applicable;
4. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
5. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
6. Business management and general administrative activities of the entity; including, but not limited to:
   a. Management activities relating to implementation of and compliance with the requirements of the HIPAA Privacy Regulations;
   b. Customer service, including the provision of data analyses for policyholders, plan sponsors, or other customers, provided that PHI is not disclosed to such policyholder; plan sponsor, or customer;
   c. Resolution of internal grievances;
   d. The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and
   e. Consistent with the applicable requirements of § 164.514, creating de-identified health
information or a limited data set, and fundraising for the benefit of the covered entity.

**Healthcare Provider:** An entity that provides healthcare, service, or supplies related to the health of an individual.

**Health Information:** Any information, whether oral or recorded in any form or medium, that:
1. is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and
2. 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.

**Health Oversight Agency:** An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the healthcare system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

**Health Plan:** An individual or group plan that provides, or pays the cost of, medical care as defined at 45 C.F.R. § 160.103.


**HIPAA Privacy Regulations:** The HIPAA Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164.

**HIPAA Privacy Rule:** The HIPAA Privacy Regulations.

**HITECH Act:** The Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009.

**Human Subjects Committee:** ISU’s IRB and Privacy Board for HIPAA and research related issues. (See HSC Website at http://www.isu.edu/research/hsc.shtml.)

**Individual:** The person, generally the patient, who is the subject of the PHI.

**Individually Identifiable Health Information:** Information that is a subset of health information, including demographic information collected from an individual, and:
1. Is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and
2. 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
   a. That identifies the individual; or
b. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

**Information System:** An interconnected set of information resources under the same direct management control that shares common functionality, including hardware, software, information, data, applications, and communications.

**Institutional Review Board (IRB):** Any board committee, or other group formally designated by an institution to review, to approve the initiation of, and to conduct periodic review of, biomedical research involving human subjects. The primary purpose of such review is to assure the protection of the rights and welfare of the human subjects.

**Law Enforcement Official:** An officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

1. Investigate or conduct an official inquiry into a potential violation of law; or
2. Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

**Limited Data Set:** Protected health information that excludes direct identifiers of individuals (patients), or of their relatives, employers or household members. A limited data set is subject to the HIPAA Privacy Rule and requires a Data Use Agreement prior to release of the data set for internal and external uses and disclosures. The elements of the LDS are set forth at 45 C.F.R. § 164.514.

**Marketing:**

1. To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service, unless the communication is made:
   a. To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits.
   b. For treat of the individual; or
   c. For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.
2. An arrangement between a covered entity and any other entity whereby the covered entity discloses PHI to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.

**Minimum Necessary:** Only the minimum necessary PHI may be used or disclosed to achieve the intended purpose of the use or disclosure.
**Notice of Privacy Practices:** A document required by HIPAA that provides the patient with information about his or her rights under the Privacy Rule and how ISU uses the PHI.

**Office of Civil Rights (OCR):** A sub-agency of the U.S. Department of Health and Human Services authorized to investigate potential violations and enforce HIPAA’s requirements. References to HHS in this or any other policy should be interpreted to include references to OCR.

**Payment:** The activities undertaken by a healthcare provider or health plan to obtain or provide reimbursement for the provision of health care.

**Person:** Those who may file a privacy complaint including the patient, individual, patient’s personal representative, employee, business associate, group, or organization.

**Personal Representative:** The person who has authority under law to act on behalf of a patient.

**Privacy Rule:** The regulation issued by the U.S. Department of Health and Human Services entitled Standards for Privacy of Individually Identifiable Health Information.

**Protected Health Information:** Individually identifiable health information that is maintained in any medium or transmitted or maintained in any other form. PHI excludes individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act (FERPA), and records held by a covered entity in its role as an employer.

**Psychotherapy Notes:** Notes recorded (in any medium) by a healthcare provider who is a mental health professional that:

1. Document or analyze the contents of conversation during a private counseling session or a group, joint or family counseling session, and
2. Are separated from the rest of the individual’s medical record.

Psychotherapy notes exclude medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date. Psychotherapy notes are used only by the therapist who wrote them, maintained separately from the medical record and not normally involved in the documentation necessary for health care treatment, payment or health care operations.

**Re-identified Information:** Health information previously de-identified may be re-identified using a code, key or other record identifier. This re-identified information is PHI and is subject to the HIPAA Privacy Rule.

**Research:** A systematic investigation, including research development, testing, and evaluation designed to develop or contribute to generalizable knowledge.

**Risk Analysis:** The process of identifying, prioritizing, and estimating ISU’s exposure to risk to identify threats and vulnerability.

**Security:** The administrative, physical, and technical safeguards in an information system.
**Security Rule:** The federal privacy regulations promulgated under the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

**Treatment:** The provision, coordination, or management of health care and related services by one or more healthcare providers, including the coordination or management of health care by a healthcare provider with a third party, consultation between healthcare providers relating to a patient, or the referral of a patient for health care from one healthcare provider to another.

**Use:** With respect to individually identifiable health information, means the sharing, employment, application, utilization, examination, or analysis or such information within an entity that maintains such information.

**Workforce Members:** Employees, authorized volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes, for example, full-time, part-time, regularly scheduled contract workers, and members of the Board of Trustees.
Access, Use, and Disclosure

**Minimum Necessary**
ISU shall ensure that access to information is provided on a need-to-know basis. Workforce members and business associates will be given access to PHI or PHI will be disclosed to them only when there is a legitimate business need for access to the information. No workforce member or business associate shall access or attempt to access PHI unless he or she has been given access rights and has a legitimate business reason for doing so, such as carrying out job duties, functions, and responsibilities.

ISU shall implement procedures and use technological tools wherever possible, to restrict access to PHI based on the specific roles of the workforce members and business associates. Access and use shall be limited to the “minimum necessary” to achieve the intended purpose of the use of the PHI.

ISU shall review non-routine requests for access to information. A decision for each request will be made on an individual basis to determine whether the PHI requested is the minimum necessary.

ISU shall not apply the minimum necessary standard to:

1) any request for information from the patient;
2) disclosures required by the Secretary of the U.S. Department of Health and Human Services when determining whether ISU is compliant with HIPAA;
3) any disclosures required by federal, state, or local laws, rules, and regulations.

ISU shall review requests for information from another healthcare agency, health plan, or clearinghouse, and ensure it provides only the minimum necessary PHI required to achieve the purpose of the particular use or disclosure if the request is accompanied by an appropriate authorization for release of medical information.

**Limited Data Sets**
A limited data set is PHI that excludes the following identifiers of the patient, or the patient’s relatives, employer, or household members:

1) names;
2) address, except city, state, and zip code;
3) phone numbers;
4) fax numbers;
5) email addresses;
6) social security numbers;
7) medical record numbers;
8) health plan numbers;
9) certificate or license numbers;
10) vehicle identifiers, including license plate numbers;
11) device identifiers and serial numbers;
12) URLs;
13) IP addresses;
14) biometric identifiers;
15) photographic images of the face and comparable images.
ISU may use or disclose a limited data set if a Data Use Agreement is signed with the recipient for the purpose of research, public health, or healthcare operations. The Data Use Agreement must:

1) establish the permitted uses and disclosures;
2) not allow the recipient to use or further disclose the information in a manner that would violate this manual or HIPAA regulations except as required by law;
3) establish who can use or receive the limited data set;
4) provide that the recipient will use appropriate safeguards to prevent use or disclosure other than as allowed by the Data Use Agreement;
5) provide that the recipient shall report any use or disclosure in violation of the Data Use Agreement;
6) ensure that any authorized person that the recipient provides the limited data set to agrees to the same restrictions and conditions that apply to the recipient;
7) provide that the recipient shall not attempt to identify the information or contact the person.

If the recipient breaches the Data Use Agreement, ISU shall take reasonable measures to cure the breach or end the violation. If ISU cannot, it shall discontinue disclosing PHI to the recipient and report the issue to the Secretary of the U.S. Department of Health and Human Services.

**De-Identified PHI**

Information that does not identify an individual, and information that ISU has no reasonable basis to believe can be used to identify an individual is not PHI. It is considered de-identified.

ISU may use de-identified information to report demographic information, quality of service initiatives, cost efficiencies, and other uses directly related to its work.

Before information can be used, the HIPAA Compliance Officer shall confirm that it is de-identified. The following identifiers must be removed and the HIPAA Compliance Officer must verify that the information, used alone or in combination with other information, cannot identify the individual who is the subject of the information:

1) name;
2) street address;
3) city;
4) county;
5) zip code (and equivalent geocodes, except the first three digits if, according to the current publicly available data from the Census Bureau shows that the geographic unit formed by combining all zip codes with the same first three digits contains more than 20,000 people, and the first three digits for all such geographic units containing 20,000 or fewer people is changed to 000);
6) all dates except year (this includes birth date, admission date, discharge date, date of death), and all ages over eighty-nine (89), all elements of the date (including year) that is indicative of such age, except that ages may be aggregated into one category of age ninety (90) or older;
7) phone numbers;
8) fax numbers;
9) email addresses;
10) social security numbers;
11) medical record numbers;
12) health plan numbers;
13) account numbers;
14) certificate or license numbers;
15) vehicle identifiers, such as license plate numbers;
16) device identifiers, such as serial numbers;
17) URLs;
18) IP addresses;
19) biometric identifiers;
20) photographs of the face and any comparable images;
21) any other unique identifying number, characteristic, or code.

The HIPAA Compliance Officer shall ensure that a mechanism exists that will allow the information to be re-identified by ISU, as long as the code is not derived from or related to information about the patient and is not otherwise capable of identifying the patient. ISU shall not use or disclose the mechanism for re-identification. If information is re-identified, the HIPAA Compliance Officer shall oversee the process.

**Protecting Verbal and Written PHI**

ISU shall protect printed or hard copies of PHI by:

1) ensuring that incoming PHI is delivered to the correct department and person to limit access to PHI;
2) limiting the number of photocopies made of PHI;
3) ensuring that workforce members have a “clean desk” practice so that PHI is turned face down on desks or concealed in another manner, and not open on computer screens when away from the desk;
4) ensuring that unauthorized personnel cannot view PHI on the workforce member’s desk or computer;
5) storing hard copies of PHI in a secure, locked area with access limited to designated personnel;
6) destroying PHI when it is no longer required to be retained by shredding it or placing it in designated, locked containers for shredding;
7) viewing the hard copy record in the secure locked area;
8) having workforce members sign out hard copy records if they must be moved from the secure, locked area;
9) ensuring that hard copy records do not leave the building without the express written approval of the HIPAA Compliance Officer;
10) returning hard copy records to the secure, locked area when the need for the record is completed, but always by the end of each work day.

ISU shall ensure that printers, scanners, copiers, and fax machines are not easily accessible to unauthorized persons. Documents containing PHI shall be promptly removed from a printer, scanner, copier, or fax machine and placed in a secure location. Workforce members shall only access such documents if they have the authority to do so.

ISU shall protect verbal PHI in face-to-face conversations by:

1) conducting meetings in a room with a closed door;
2) keeping voices down;
3) only including workforce members who have a need to know;
4) limiting the PHI discussed to the minimum amount necessary to accomplish the purpose of the
meeting. If it is not possible to meet in a room with a closed door, the workforce members shall speak in the most private area possible with lowered voice to minimize any inadvertent disclosure.

ISU shall protect verbal PHI while on the telephone by:
1) keeping voices down;
2) requesting that unauthorized persons step away from the area, if possible;
3) using a phone that is located in as private an area as possible, or moving to as private an area as possible before continuing a conversation;
4) limiting the PHI discussed to the minimum amount necessary to accomplish the purpose for the conversation.

Disclosure Verification
If ISU does not know the individual or organization requesting disclosure of patient PHI, ISU shall take reasonable steps to verify the identity and authority of the individual or organization.

If the request is made in person, reasonable steps may include a request to see identification. If the request is made by telephone, reasonable steps may include verification of identity through information that would only be known by the requestor (last four digits of the social security number, date of birth, telephone number, maiden name, spouse’s name).

Disclosure Consent, and Authorization
ISU shall not use or disclose PHI that was received or created outside the process of providing treatment, payment, or healthcare operations, without an authorization signed by the patient.

Authorization is not required to disclose PHI:
1) when required by law;
2) as part of health oversight activities;
3) to identify a deceased person;
4) when a waiver is granted for the purposes of a research project;
5) to the Secretary of the U.S. Department of Health and Human Services.

An authorization is not valid if:
1) the expiration date has passed or the expiration event is known by the covered entity to have occurred;
2) the authorization has not been filled out completely;
3) the authorization has been revoked;
4) material information in the authorization is known to be false or incorrect.

ISU shall not condition treatment on the provision of an authorization except for:
1) research-related treatment may be conditioned on the provision of an authorization;
2) provision of health care that is solely for the purpose of creating PHI for disclosure to a third party (fitness-for-duty exams, life insurance physicals).

ISU shall allow a patient to revoke an authorization at any time in writing. However, this does not apply to the extent that ISU has already acted in reliance on such authorization.
ISU shall retain any signed authorization and related documents for six (6) years from the date the authorization was signed. ISU shall provide the patient with a copy of the authorization.

An authorization must:
1) be written in plain language;
2) contain a description of the information to be used or disclosed that identifies the information in a specific and meaningful manner;
3) have the name or other specific identification of the person(s) or class of persons authorized to make the requested use or disclosure;
4) have the name or other specific identification of the person(s) or class of persons to whom ISU may make the requested use or disclosure;
5) include an expiration date or expiration event that relates to the patient or the purpose of the use or disclosure;
6) include a statement of the patient’s right to revoke the authorization in writing and any exceptions to the right to revoke, and a description of how the patient may revoke the authorization;
7) have a statement that information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and may no longer be protected;
8) include the signature of the patient and the date it was signed;
9) if signed by a personal representative, have a description of the personal representative’s authority to act on behalf of the patient.

When ISU requests a patient authorization for its purposes or for the use or disclosure by others, the following shall be included:
1) a statement that ISU shall not condition treatment on the patient’s provision of the authorization;
2) a description of each purpose of the requested use or disclosure;
3) a statement that the patient has the right to inspect or copy the PHI to be used or disclosed and may refuse to sign the authorization;
4) a statement that disclosure by ISU of the information will result in direct or indirect remuneration to ISU from a third party;
5) a statement that the patient has the right to refuse to sign the authorization.

ISU shall give patients the opportunity to request a restriction on the use or disclosure of PHI. Such request shall be in writing to the HIPAA Compliance Officer. However, ISU does not have to agree to the request, but will determine on a case-by-case basis.

ISU shall accept every request for disclosure restriction if the disclosure is for payment or operations purposes and the PHI only relates to a service for which payment was made before services were provided.

ISU shall make every attempt to honor the patient’s request. If the restriction is accepted, ISU shall mark the relevant portions of the patient’s records to prevent improper use or disclosure and shall notify any business associate who may use or disclose the PHI of the restriction. ISU shall not use or disclose the PHI unless the patient terminates the restriction, or if the PHI must be disclosed to another provider in order to provide emergency treatment to the patient. ISU shall notify such provider of the restriction.
The patient may terminate the restriction verbally or in writing. If terminated verbally, the termination shall be appropriately documented in the patient file.

ISU may terminate the restriction and notify the patient. However, such termination shall only apply to PHI created or received after the patient is notified. ISU may:

1) terminate the restriction in person and have the patient or personal representative sign and date a notification of termination of the restriction;
2) terminate the restriction by sending the notification by certified mail, return receipt requested. The restriction shall not be terminated until ISU receives confirmation that the person served received the notification.
3) terminate the restriction by telephone. The call shall be documented and an email or letter shall be sent as well to confirm the conversation in writing. The termination shall be effective the date the person was informed by telephone.
4) terminate the restriction by encrypted email to a verified email account. The email shall be documented. The termination shall be effective the date of the email.

ISU shall not agree to a restriction on use or disclosure:
1) when required by an investigation to determine ISU’s compliance;
2) for facility directories;
3) that does not require authorization or the opportunity to object.

If ISU creates PHI for the purpose of research that includes treatment of patients, ISU shall obtain an authorization for the use or disclosure of such information. The authorization will include:

1) a description of the extent to which PHI will be used or disclosed to carry out treatment, payment, or healthcare operations;
2) a description of PHI that will not be used or disclosed for purposes permitted by law if ISU does not limit its right to make a use or disclosure that is required by law or permitted by law to mitigate a serious and imminent threat to public health or safety;
3) a reference to any patient consent and the Notice of Privacy Practices, as applicable. An authorization under this paragraph can be in the same document as a consent to participate in research, a consent to use or disclose PHI to carry out treatment, payment or healthcare operations, or a Notice of Privacy Practices.

As a general rule, ISU shall not combine authorizations for use or disclose PHI with a consent to carry out treatment or payment, or with an informed consent to participate in research. However, a compound authorization may be used when:

1) an authorization created for research that includes treatment of the patient can be combined with a consent for use or disclosure, another research consent, or a Notice of Privacy Practices;
2) an authorization for use or disclosure of psychotherapy notes is combined with another authorization for a use or disclosure of psychotherapy notes;
3) an authorization for other than a disclosure of psychotherapy notes can be combined with another authorization except when treatment is conditioned on the provision of one of the authorizations;
4) an authorization for a research study can be combined with any other type of written permission for the same or another research study, with an authorization for the creation or maintenance of a research database or repository, or with a consent to participate in research.
Any compound authorization must show each authorization visually and organizationally separate from other content in the document, and must be separately signed and dated.

**Disclosure for Healthcare Operations**

ISU may use or disclose PHI without an authorization for the purpose of healthcare operations, unless required by law.

Information that is accessed, used, and disclosed for healthcare operations is subject to the “minimum necessary” disclosure rule. Only those workforce members who have been given authority are allowed to access, use, or disclose the minimum necessary PHI to carry out their duties for healthcare operations.

Auditors, third party management companies, attorneys, accountants, and other third parties may assist ISU in carrying out its healthcare operations. All such third parties shall have a business associate contract in place before they can access, use, or disclose PHI.

PHI may be disclosed for the healthcare operations purposes of other providers and health plans if:

1. the other provider or health plan is covered by HIPAA privacy regulations;
2. the other provider or health plan has a current or prior relationship with the patient; and
3. the information is being requested for purposes related to assessment or evaluation of care and competence, health care fraud, abuse detection, or compliance.

Disclosures of PHI made for healthcare operations are not required to be recorded in a patient’s file or a disclosure log. The disclosure log may be either in the electronic health record or on paper.

**Disclosure for Healthcare Treatment**

ISU may access, use, or disclose PHI without written consent or authorization for the purpose of treatment.

ISU’s workforce members may request and be given access to the complete health records of any patient currently being treated or who was previously treated.

Outside physicians, hospitals, labs, pharmacies, nursing homes, and similar third-party providers may be given access to all PHI of a patient, including the complete record if requested. If a patient requests and is granted a restriction on disclosure to a specific provider, ISU shall not release any PHI to that provider unless it is an emergency.

ISU may share PHI with treatment providers to arrange for appointments, referrals, diagnostic tests, consultations, management and coordination of care, determinations of suitability for services, and other purposes directly related to a patient’s treatment.

If ISU receives a request for PHI from a health care provider that is unknown to ISU, the provider’s identity shall be verified and documented. ISU may:

1. call the requestor at an official phone number;
2. ask that the requestor fax the request on official letterhead of the provider;
3. contact the patient directly to confirm that the provider is involved in the patient’s treatment.
Disclosures for treatment do not have to be recorded on a disclosure log. However, a note shall be made in the patient’s record, either in the electronic health record or on paper, regarding by whom and to whom the information was disclosed, how the provider is involved in the patient’s treatment, and the date of disclosure.

**Disclosure as Required by Law**

ISU shall follow all federal, state, and local laws, rules and regulations that mandate certain uses or disclosures of PHI. If the law, rule, or regulation can be enforced by an official government agency, it shall be deemed as “required by law”.

If federal or state law requires a use or disclosure for judicial or administrative purposes, such as responding to a subpoena or court order, ISU, through its Office of General Counsel, shall verify the validity of the order and that office shall only release the information expressly authorized by the court order or as requested by the subpoena.

ISU shall comply when federal or state law requires a use or disclosure for law enforcement purposes. Law enforcement agencies and officials may be provided with PHI for the purpose of making reports that are required by law, including to report a suspicious injury or suspected abuse or neglect.

If law enforcement agencies and officials are attempting to identify or locate a suspect, fugitive, material witness, or missing person, the following information may be provided:

1. name;
2. address;
3. date and place of birth;
4. blood type and rh factor;
5. type of injury;
6. date and time of treatment;
7. date and time of death (if applicable);
8. description of distinguishing physical characteristics such as height, weight, gender, race, hair color, eye color, facial hair, scars, and tattoos.

Any other PHI, such as DNA, dental records, samples of body fluids or tissues can only be disclosed with a valid court order, such as a warrant or subpoena.

ISU shall disclose PHI to law enforcement if the patient is suspected of being the victim of an alleged crime as follows.

1. a conscious, competent patient must give consent in order for ISU to disclose to law enforcement, by signing an authorization form if possible. If not possible, ISU shall document the date, time, and name of the person(s) who witnessed the authorization or refusal of authorization;
2. if the patient is unconscious or incompetent, the legally authorized representative may agree to disclosure of PHI by signing an authorization form;
3. if no legally authorized representative is available, ISU shall attempt to find a family member who can contact law enforcement officials directly;
4. in an emergency situation or if no authorized representative or family member is available, ISU may disclose the PHI only if the patient’s attending physician determines that disclosure is in the patient’s best interest and documents the decision.
ISU shall disclose PHI to law enforcement officials in the case of a death suspected of being the result of criminal conduct. The HIPAA Compliance Officer shall review the circumstances and determine the extent of PHI to be disclosed, if any, and document the resulting determination.

ISU shall disclose PHI to law enforcement officials if there is evidence of suspected criminal activity on ISU premises. The HIPAA Compliance Officer shall review the circumstances and determine the extent of PHI to be disclosed, if any, and document the resulting determination.

ISU shall report to law enforcement officials information to help identify or apprehend an individual if the person admitted to participating in a violent crime that is reasonably believed to have caused serious physical harm to a victim, or if it appears that the person has escaped from lawful custody or a correctional institution. The PHI disclosed shall be limited to the statement made by the person and the information described above for suspects, fugitives, material witnesses, or missing persons.

ISU shall verify the identity of the law enforcement official requesting the information, and document the manner of verification. For example, the workforce member may ask to see a badge and record the badge number, or ask that the request be in writing on official letterhead.

If disclosure is required by law, ISU will log the disclosure in accordance with the accounting of disclosures.

**Disclosure for Public Health and Safety**

ISU may disclose PHI if in the professional opinion of a workforce member who is a licensed professional, an adult patient appears to be the victim of abuse, neglect, or domestic violence if:

1. the disclosure is required by law;
2. the disclosure is permitted by law and such disclosure is necessary to prevent serious harm to the patient or a third-party victim; or
3. the patient has agreed to the disclosure, and such consent is documented in writing with a signature from the patient or in the patient’s file.

The patient shall be promptly informed of the disclosure, either verbally or in writing unless the workforce member who is a licensed professional believes that informing the patient will place the patient at serious risk of harm and so documents this belief, or if the patient cannot be informed and the patient’s personal representative may be the person responsible for the abuse, neglect or injury, such that informing the personal representative would not be in the patient’s best interest. Any disclosure made shall be logged appropriately.

ISU may disclose PHI to a public health authority that is authorized by law to collect or receive PHI for the purpose of preventing or controlling disease, injury, or disability, including but not limited to:

1. reporting of disease;
2. reporting of injury;
3. reporting a vital event such as birth or death;
4. conducting public health surveillance;
5. conducting public health investigations;
6. conducting public health interventions.

ISU may disclose PHI to those responsible for an FDA-regulated product or activity if related to the quality, safety, or effectiveness of the FDA-regulated product or activity, such as:
1) collecting or reporting adverse events;  
2) collecting or reporting product defects or problems;  
3) collecting or reporting biological product deviations;  
4) tracking FDA-regulated products;  
5) enabling product recalls, repairs, replacement, look-back activities;  
6) notifying individuals who have received a product that has been recalled, withdrawn, or is the subject of a look-back activity; or  
7) conducting post-marketing surveillance.

ISU may disclose PHI to a person who may have been exposed to a communicable disease, or is at risk of contracting or spreading such disease. Except in the event of an emergency, ISU shall notify the appropriate public health authority to make such notification.

**Disclosure to Others**

ISU recognizes that an adult patient who is competent may exercise his or her rights regarding the access, use, and disclosure of PHI. These rights include the right to:

1) receive a Notice of Privacy Practices;  
2) inspect and obtain copies of PHI;  
3) amend the record;  
4) obtain an accounting of disclosures of PHI;  
5) request restrictions on the use or disclosure of PHI;  
6) receive confidential communications from ISU.

A competent adult patient may also grant these rights to another person through a valid durable power of attorney for healthcare. Other persons who may exercise these rights include:

1) a court-appointed guardian, conservator, or administrator;  
2) a spouse or other relative if authorized by state law to make treatment decisions on behalf of the patient; or  
3) the executor or administrator of a deceased patient’s estate.

If the patient is a minor, who is under the age of 18, the following persons may exercise the patient’s privacy rights:

1) the minor on his or her own behalf if allowed under state law;  
2) a court-appointed guardian, conservator, or administrator;  
3) parents;  
4) other persons authorized by state law to make treatment decisions for a minor patient;  
5) the executor or administrator of a deceased minor patient’s estate.

Parents and guardians are generally involved in obtaining treatment for a minor, and can consent to treatment and assume responsibility for payment. A non-custodial parent may be allowed to review PHI, but usually does not have the right to exercise a minor’s privacy rights. If the non-custodial parent is responsible for payment, that parent also has access to payment records. A stepparent usually does not have the right to access PHI unless given such rights by a court. A stepparent may be given access to the part of the PHI directly relevant to the care provided by the stepparent if actively involved in the minor’s health care treatment.
When a minor obtains treatment without parent or guardian involvement, and is emancipated under state law, parents and guardians can access PHI only if state law does not prohibit disclosure of the PHI and the treating practitioner determines it is appropriate to release the PHI; the minor’s parent or guardian will be billed for the treatment if the minor has been advised and does not object to the parent or guardian being billed. If the minor does not agree and other payment arrangements are not made, the minor may elect to reject treatment to avoid having a bill sent to a parent or guardian.

If ISU does not know the person making a request to exercise privacy rights on behalf of a patient, the person’s identity and authority must be verified and documented. If the request is made verbally, such request shall be documented in the patient’s file. Otherwise, acceptable means of verification include:

1) a driver’s license;
2) birth certificate;
3) passport;
4) social security card;
5) marriage certificate;
6) guardianship papers;
7) power of attorney documents;
8) a photo identification accompanying another type of verification; and
9) any other verification deemed reasonable by the HIPAA Compliance Officer.

ISU recognizes that PHI may be shared with other relatives, close personal friends, or others the patient identifies. When a patient is accompanied by a person unknown to the treating practitioner, the treating practitioner shall not discuss or disclose any PHI until and unless the patient gives consent. Such consent must be documented in the patient file. If the patient cannot consent, the treating practitioner must make a professional determination as to whether a disclosure is reasonable and in the patient’s best interests, such as a person picking up medical supplies or a prescription. ISU shall verify and document the person’s identity and authority.

ISU may disclose PHI to notify or assist in the location and notification of a family member, personal representative, or other person responsible for the patient’s care. PHI shall be limited to the patient’s location, general condition, or death. The disclosure shall be appropriately logged.

**Disclosure about Deceased Patients**

The PHI of a deceased patient is subject to the same privacy protection as the PHI of living patients until the patient has been deceased for fifty (50) years. After fifty (50) years, it is no longer considered PHI.

An executor or the administrator of the patient’s estate has the right to exercise the same privacy rights that the patient would have, which includes the right to inspect and obtain copies of the health record, request amendments, and obtain an accounting of any disclosures.

If allowed by state law, the deceased patient’s PHI may be released as follows:

1) to a medical examiner or coroner for the purpose of identifying the deceased, determining the cause of death, or other duties as authorized by law;
2) to funeral directors as necessary to carry out their duties;
3) to organ donation agencies for the purpose of facilitating organ, eye, or tissue donation and transplantation, if the deceased patient or the deceased patient’s personal representative authorizes the disclosure, or as otherwise required or authorized by law;
4) to an authorized official or agency for the purpose of carrying out public health activities, health oversight, law enforcement, research, or other purposes for which an authorization is not required if the disclosure complies with this manual.

ISU shall log all disclosures for other than treatment, payment, health care operations or as authorized by the patient’s personal representative.

Disclosure for Employees
ISU shall not disclose an employee’s health information to his or her employer unless it receives a written authorization signed by the patient allowing disclosure, or the employee is being evaluated for workplace related injuries or conditions.

ISU may disclose limited PHI without the patient’s written authorization if:
1) ISU provided the patient with an evaluation related to medical surveillance of the workplace as required by OSHA or other state or federal agencies;
2) ISU made a determination of whether the patient suffered a work-related illness or injury;
3) the employer provides written certification stating that the PHI is necessary to comply with its obligations regarding occupational and workplace safety;
4) the patient has received written notice that any findings will be disclosed to the employer. ISU shall obtain and verify the employment relationship and the requestor’s identity and authority to obtain the PHI on behalf of the employer.

Disclosures to employers shall be logged appropriately.

Disclosure for Specialized Government Functions
ISU may access, use, and disclose PHI of patients:
1) who are armed forces personnel if deemed necessary by appropriate military command authorities to assure proper execution of a military mission as published in a notice in the Federal Register;
2) to authorized federal officials for provision of protective services to the President or other authorized persons (18 USC 3056), or foreign heads of state, or those authorized by 22 USC 2709(a)(3), or for investigations authorized by (18 USC 871 and 879).

Disclosures for Research
ISU generally will only access, use, or disclose PHI that is created for the purposes of research with prior authorization by the patient. However, authorization is not necessary if:
1) other documentation is obtained showing alteration to or waiver of authorization has been approved by an Institutional Review Board (IRB);
2) the researcher represents that access, use, and disclosure is sought to review PHI as necessary to prepare a research protocol, and no PHI shall be removed from the covered entity during review;
3) the patient is deceased and the researcher represents that access, use, or disclosure is solely for research on the PHI of the decedent, and the research provides documentation of the death of the patient.

If access, use, or disclosure is provided based on documentation of alteration or approval of a waiver, the IRB shall provide:
1) a statement identifying the IRB and the date of approval;
2) a statement that the IRB determined that the waiver satisfies its criteria;
3) a brief description of the PHI that the IRB deems necessary for access or use; and
4) a statement that the waiver was reviewed and approved by the IRB review procedures.

ISU shall ensure that:
1) the use or disclosure of PHI involves no more than minimal risk to the patient;
2) the waiver won’t adversely affect the patient’s privacy rights or the patient’s welfare;
3) the research could not be reasonably conducted without alteration or waiver;
4) the research could not be reasonably conducted without the PHI;
5) the privacy risk to the patient’s PHI is reasonable in relation to the anticipated benefits the patient may receive, if any, and the importance of the knowledge reasonably expected to result from the research;
6) an adequate plan exists to protected the PHI from improper use and disclosure;
7) an adequate plan exists to appropriately destroy the PHI when it is no longer needed, unless retention is required by law; and
8) there is written assurance that the PHI will not be reused or disclosed to anyone else unless required by law, for authorized oversight of the research, or for other research for which access, use, or disclosure would be permitted by ISU.

The IRB shall follow the requirements of the Common Rule. The proposed research shall be reviewed at meetings where a majority of the members are present, including at least one member not affiliated with ISU or the entity conducting or sponsoring the research, and a person affiliated with such entities. The alteration or waiver of authorization must be approved by a majority of the IRB members present at the meeting.

The IRB may use a documented expedited review procedure if the research involves no more than minimal risk to the patient’s privacy.

**Disclosure to Business Associates**

ISU shall only allow access, use, or disclosure of PHI to a business associate if a Business Associate Agreement (BAA) has been executed between ISU and the business associate. The BAA shall require the business associate to appropriately safeguard the information, and ISU must receive satisfactory assurances that the business associate can comply.

ISU does not require a BAA for disclosures made to another healthcare provider if it concerns treatment of a patient.

If ISU becomes aware that the business associate has violated the BAA, ISU shall immediately notify the business associate and cure the violation pursuant to the terms of the BAA. If the violation cannot be cured, ISU shall determine if it can feasibly terminate the BAA pursuant to the termination procedures in the BAA. If it cannot, ISU shall report the violation to the Secretary of the U.S. Department of Health and Human Services.

The BAA shall establish the permitted and required uses and disclosures of PHI by the business associate. The business associate shall not be allowed to further disclose the PHI in a manner that would violate ISU’s privacy and security procedures.
The BAA shall allow the business associate to use and disclose PHI in order to manage and administer its obligations and carry out its legal responsibilities. A business associate may be allowed to provide data aggregation services related to ISU’s healthcare operations.

The BAA shall specifically provide that the business associate will:

1) not use or further disclose PHI other than as permitted by the agreement or as required by law;
2) use appropriate safeguards to prevent use or disclosure of the PHI other than as provided by the BAA;
3) report use or disclosure of PHI that violates the BAA;
4) ensure its agents and subcontractors who have access to the PHI will be held to the same restrictions and conditions that apply to the business associate in the BAA;
5) make PHI available to the patient in the same manner as ISU makes PHI available to the patient;
6) allow a patient to request amendment to the PHI and incorporate any amendment in accordance with ISU procedure;
7) keep an accounting of disclosures in accordance with ISU procedure;
8) make its internal practices, books, and records relating to use and disclosure of PHI available to the Secretary of the U.S. Department of Health and Human Services for the purpose of determining ISU’s compliance with HIPAA;
9) implement the protections as required by the Security Rule;
10) immediately notify ISU if there has been a breach involving PHI;
11) return or destroy all PHI upon termination of the BAA unless required to keep the PHI by law, in which case, certify that the PHI shall no longer be used.

**Disclosure for Marketing**

ISU shall not use or disclose PHI for marketing purposes without prior written authorization from the patient, unless it is a marketing communication that is a function of the healthcare operation. A marketing communication is one in which the communication:

1) takes place face-to-face with the person;
2) concerns products or services that have nominal value, such as giving out a pen;
3) concerns ISU’s or a third party’s health-related products and services as long as ISU is not receiving remuneration for the communication.

If ISU does receive remuneration for communicating a treatment option to a patient, ISU shall ensure that its Notice of Privacy Practices states it may communicate such options and ISU is receiving payment in exchange for communicating such options. The Notice of Privacy Practices shall let patients know how to opt out of such communications, and opting out shall not be burdensome for the patient either financially or otherwise.

If ISU uses or discloses PHI to target communication to a certain patient based on health status or communication, ISU shall make a prior determination that the product or service being marketed could be beneficial to the health of the patient being targeted. The communication must explain why the patient was targeted and how the product or service relates to the patient’s health. If the patient opts out of receiving future marketing communications, ISU shall ensure that the patient no longer receives such communications.

ISU may disclose PHI to a business associate for marketing communications only if the function of the business associate is to assist ISU with conducting such marketing communications.
ISU shall never sell, nor allow anyone else to sell, any patient PHI.

**Disclosure for Fundraising**

Fundraising communications are a solicitation for funds, either verbally or in writing. It does not include an acknowledgement or thank you note for a donation, or an update of fundraising activities that does not include a request for additional donations.

Non-PHI sources of information, including a purchased mailing list, alumni or employee information, direct contact by a potential donor, are not subject to this manual. Only fundraising activities that are conducted by a department of ISU or on behalf of ISU must comply.

ISU shall obtain patient authorization prior to using PHI for fundraising activities. The PHI that may be used includes:

1) patient demographics such as name, address, phone number, email address, age, gender, date of birth;
2) dates of service;
3) covered entity that provided service, but not a specific diagnosis or the nature of services or treatment the patient received;
4) the name of the treating professional;
5) information about the outcome of the treatment, which may only be used to screen or exclude patients from receiving fundraising communications; and
6) health insurance status.

Any communication that involves a solicitation must contain language describing how the patient may opt out of future communications. Such language shall be clear and conspicuous and not impose an undue burden on the patient. If the patient opts out, it is a revocation of any prior authorization for use or disclosure of PHI for fundraising communications. ISU may allow patients to affirmatively opt back in to receiving communications if the patient later changes his or her mind.

ISU may offer educational campaigns or awareness campaigns in collaboration with a third party. ISU shall not share PHI with the third party or allow the third party to use ISU’s patient list to send fundraising solicitations. However, at the event, the third party may ask patients to provide contact information to the third party. No fundraising shall occur at the event.

ISU shall not condition treatment or payment on the patient’s choice with respect to receiving fundraising communications.

**Disclosure in Meetings**

ISU shall restrict the use or disclosure of PHI in meetings or similar settings such that PHI is not provided unnecessarily to unauthorized individuals.

In a meeting where PHI is discussed, it should only be attended by workforce members who are specifically invited who have a specific business purpose for attending. These meeting shall be conducted in a secure area so that no unauthorized person can overhear or view PHI.

If a meeting includes third parties who are not authorized to have access to PHI, such meeting shall take place in a fully enclosed room so that the third party cannot hear or view PHI being handled by workforce members in the immediate vicinity.
If PHI is written on a whiteboard or blackboard, it must be erased so it is unidentifiable before the attendees leave the room.

If PHI is distributed during the course of a meeting and is not required by the workforce members for healthcare operations purposes, the PHI must be collected and destroyed at the completion of the meeting.

**Psychotherapy Notes**

ISU shall obtain a patient authorization for the release of psychotherapy notes. However, the covered entity can rely on a patient’s consent for use or disclosure for:

1) the provider, individual originator of the psychotherapy notes, to provide treatment;
2) use in supervised training programs;
3) defending a legal action or other proceeding brought by the individual.

ISU shall not obtain patient authorization to disclose psychotherapy notes when required by law, as part of health oversight activities, to identify a deceased person, or when a waiver is granted for a research project.

The following types of highly confidential information are generally protected by federal and/or state statute and may not be photocopied, emailed, mailed, or faxed without specific patient authorization or as required by law:

1) psychotherapy records of treatment by a psychiatrist, licensed psychologist, or psychiatric clinical nurse specialist;
2) professional services of a licensed psychologist;
3) social work counseling or therapy;
4) domestic violence victim counseling;
5) sexual assault counseling;
6) records about sexually-transmitted diseases;
7) HIV test results;
8) alcohol and drug abuse records that are protected by federal confidentiality rules (42 CFR part 2).

**Use of Email**

Workforce members shall refrain from including patient PHI in electronic email messages. If PHI must be transmitted by email, distribution shall be restricted to those with a need to know, and email shall be encrypted. Only the minimum amount necessary shall be transmitted via encrypted email. Unencrypted email messages are not secure and not private.

Workforce members shall only communicate with a patient by email if the patient has given affirmative consent to be contacted in this manner. The workforce member shall verify the accuracy of the email address before sending any encrypted email containing PHI to avoid inadvertently sending the email to the wrong person or entity.

All email sent that contains PHI shall include a confidentiality statement in the body of the email.

ISU cannot guarantee that email will be private. Any person who uses email expressly waives his or her right to privacy in any email they create, send, receive, or save and consents to review of such email. The HIPAA Compliance Officer or designee may access, monitor, and review email as necessary,
although it is not ISU’s intent to regularly monitor the content of email, but may do so to support audits, security, investigations, maintenance, and operations. In no event shall email be accessed, monitored, or reviewed out of personal curiosity, or at the request of those not authorized to make such request. If ISU is involved in litigation, all email pertaining to that litigation shall not be deleted until the General Counsel releases the litigation hold.

**Use of Fax Machines**

ISU shall promptly remove any documents that are delivered via fax and ensure that it is given to the appropriate recipient or filed in a secure, locked area.

If a workforce member is sending a fax that includes PHI, the workforce member shall:

1. ensure that only the minimum necessary to meet the requestor’s needs is transmitted;
2. not transmit highly confidential information;
3. verify that he or she is faxing to the correct number to eliminate inadvertent errors in dialing;
4. maintain the verification sheet that shows the transmission was successful in the patient’s record;
5. use a cover sheet that includes the name of the recipient, fax number, phone number, date, number of pages transmitted, and a confidentiality statement;
6. pre-program and test destination numbers for frequent recipients, and ask the frequent recipients to immediately notify ISU of a change to the fax number.

If a workforce member becomes aware that the fax was sent to the wrong person or entity, a fax shall be sent to the recipient asking that the material be returned or destroyed, and the HIPAA Compliance Officer shall be notified.

**Public Areas**

ISU shall ensure that equipment, including telephones, workstations, fax machines, copy machines, and printers, are not located in public areas such that PHI may be overheard or viewed by unauthorized individuals.

ISU shall ensure that the display screens for PCs and workstations that are used for PHI are positioned in such a way that they cannot be easily viewed by an unauthorized person walking by, waiting in the reception area or a related public area, or through a window.

Fax machines and printers used for PHI shall be located in a secure area such that printouts cannot be easily viewed by an unauthorized person walking by, waiting in the reception area or a related public area, or through a window.

Workforce members who use a portable device shall remain cognizant of their position when viewing PHI.

Workforce members shall make every effort to conceal paper charts, medical records, faxes, or other documentation containing PHI, and shall appropriately file them away when not in use, or secure them when the workforce member steps away. Electronic records shall be closed when no longer needed or when the workforce member steps away.

Filing cabinets containing PHI shall be located in a locked room and shall themselves be locked when PHI access is not necessary.
Faxes and computer printouts shall be collected as soon as possible and appropriately filed.

All activities involving PHI shall take place in areas that are physically secure and protected against unauthorized access, interference, and damage.

**No Sale**

ISU shall not sell patient PHI unless it receives written authorization from the patient. The sale of PHI is a disclosure where ISU directly or indirectly receives payment from the entity that receives the PHI.

Sale of PHI, even if ISU receives payment, does not include a disclosure made:

1) for public health purposes;
2) for research purposes if the payment is strictly remuneration to cover the cost to prepare and transmit the PHI;
3) for treatment and payment purposes;
4) for sale, transfer, merger, or consolidation of all or part of the covered entity and for related due diligence purposes;
5) to a business associate for activities the business associate undertakes on behalf of ISU if the payment is strictly for performance of contracted services;
6) to the patient;
7) as required by law;
8) for any other purpose if the payment is strictly to cover the cost to prepare and transmit the PHI.

**Disclosure Tracking**

ISU recognizes that a patient has the right to receive an accounting of disclosures of PHI made by ISU in the six (6) years prior to the date on which the accounting is requested. ISU shall act on a patient’s request no later than sixty (60) days after receipt of a request. If ISU is unable to provide the accounting within this time, it may be extended by no more than thirty (30) days provided that ISU provides the patient with a written statement of the reasons for the delay and the date by which ISU shall respond. No other extension is allowed.

An accounting of disclosures shall include:

1) the date of the disclosure;
2) the name of the entity or person who received the PHI and the address of such entity or person, if known;
3) a brief description of the PHI disclosed;
4) a brief statement of the reason for the disclosure to reasonably inform the patient of the basis for the disclosure.

If ISU has made multiple disclosures of PHI to the same person or entity for a single purpose or pursuant to a single authorization for use or disclosure, the accounting of disclosures may provide:

1) the information required for the first disclosure during the accounting period;
2) the frequency, periodicity, or number of disclosures made during the accounting period;
3) the date of the last disclosure during the accounting period.

ISU shall provide the first account to a patient in any twelve (12) month period without charge. ISU may charge a reasonable, cost-based fee for each subsequent request by the same patient within that twelve
(12) month period. ISU will inform the patient in advance of the fee to give the patient the opportunity to withdraw or modify the request to avoid or reduce the fee.

If ISU determines that it must exclude PHI from an accounting of disclosures for any reason stated in this manual, it will provide a timely written explanation to the patient in plain language. It shall state:

1) the basis for the exclusion;
2) a description of how the patient may complain to the HIPAA Compliance Officer or to the Secretary of the U.S. Department of Health and Human Services for failure to comply with the patient’s request.

An accounting of disclosures does not apply to disclosures:

1) to carry out treatment, payment, and healthcare operations;
2) to a patient or to the patient’s personal representative;
3) for the facility’s directory;
4) to persons involved in the patient’s care or for other notification purposes;
5) for national security or intelligence purposes;
6) to a correctional institution;
7) to law enforcement officials;
8) that involve de-identified information.

ISU shall temporarily suspend a patient’s right to receive an accounting of disclosures to a health oversight agency or law enforcement official for the time specified by such agency or official, if the agency or official provides ISU with a written or verbal statement that such accounting would reasonably likely impede the agency’s activities, and specifying a time for which the suspension is required. If the statement is verbal, ISU shall document the statement and the identity of the agency or official making the statement; temporarily suspend the patient’s right to an accounting of disclosures, and limit the temporary suspension to no longer than thirty (30) days from the date of the statement unless a written statement is received during that time extending the suspension.

A patient may request an accounting of disclosures for a period of time that is less than six (6) years from the date of the request.

ISU shall use a Protected Health Information Disclosure Log to document all disclosures of patient PHI, which shall be used when a patient requests an accounting of disclosures of his or her PHI. The log shall include the patient’s name, date of service, date of request, description of PHI released, number of pages released, the reason for disclosure, the recipient of the PHI. The log may be in the electronic health record or on paper.

Only those workforce members who are specifically authorized to release PHI may do so. The PHI shall be disclosed in a secure manner.

**Privacy Breach**

An unauthorized, acquisition, access, use, or disclosure of unsecured (unencrypted, unshredded, or not rendered unusable or unreadable to unauthorized persons) PHI in a manner that compromises the privacy or security of the PHI is presumed to be a breach of PHI unless it is demonstrated that there is a low probability that the PHI has been compromised. The HIPAA Compliance Officer shall make the determination of the probability of compromise.
There is no breach if there is:

1) unintentional acquisition, access, or use of PHI by a workforce member or business associate if the acquisition, access, or use was made in good faith and would otherwise be in the scope of the workforce member’s or business associate’s scope of authority unless there is further inappropriate use or disclosure;
2) inadvertent disclosure by an authorized workforce member to another person who is authorized to access the PHI provided there is no further inappropriate use or disclosure;
3) disclosure to an unauthorized person if ISU has a good faith belief that the unauthorized person would not reasonably be able to retain the information.

If a workforce member discovers or suspects there has been a breach of unsecured PHI, he or she shall report the matter immediately to the HIPAA Compliance Officer. If a workforce member is uncertain of whether or not a situation constitutes a breach, he or she shall contact the HIPAA Compliance Officer immediately. Examples include:

1) noticing PHI in a location other than where it is normally stored;
2) noticing a computer running in a strange manner;
3) someone trying to log into his or her computer;
4) his or her computer has a virus;
5) lost or missing equipment;
6) the appearance of unauthorized equipment.

The HIPAA Compliance Officer shall investigate any report and determine whether the situation constitutes a breach, and whether ISU has reporting obligations. The HIPAA Compliance Officer shall consider:

1) the type of information that is inappropriately used or disclosed;
2) the characteristics of the recipient of the information;
3) whether PHI was acquired or viewed;
4) the ability to mitigate the inappropriate disclosure;
5) other relevant factors that arise in the course of investigation.

If the HIPAA Compliance Officer determines there has been a breach, he or she shall notify the affected patients as soon as possible, but no later than sixty (60) days after the initial discovery of the breach. Notice shall include:

1) a brief description of the breach;
2) the date of the breach, if known, and the date of discovery of the breach;
3) a description of the PHI that was compromised;
4) information on steps the patient can take to protect him or herself from potential harm as a result of the breach;
5) a brief description of the actions taken by ISU to investigate the breach, mitigate the harm, and protect against any further breaches;
6) contact information for patients to ask questions or learn additional information, which must include a toll-free telephone number, email address, a website, or a postal address.

The notice must be sent by first-class mail, or if the patient has agreed to electronic notice and such notice has not been withdrawn, the notice may be sent by electronic mail.
If ISU has insufficient or out-of-date contact information, ISU shall attempt to identify a substitute form of notice to reach the patient. If there is insufficient or out-of-date contact information, substitute notice may be provided by telephone or an alternative form of written notice, such as a conspicuous posting for a period of ninety (90) days on the covered entity’s website, or a conspicuous notice in a major print or broadcast media in geographic areas where the patients affected by the breach likely reside. The notification must include a toll-free number that remains active for at least ninety (90) days, so the patient can learn whether his or her PHI was included in the breach.

If the substitute notice takes place by telephone, the designated person giving notice should limit disclosure of PHI until he or she can confirm with reasonable certainty that the person on the phone is the affected patient.

If the situation is urgent because of the potential for misuse of the PHI, the HIPAA Compliance Officer may provide information by telephone or other means in addition to written notice.

If a breach involves more than 500 residents of a state or jurisdiction, the HIPAA Compliance Officer shall notify prominent media outlets in the state or jurisdiction. The notification must be given without unreasonably delay, and in all cases, be given within sixty (60) days after discovery of the breach involving more than 500 residents of a state.

If a breach involves more than 500 patients, the HIPAA Compliance Officer shall provide notice to the Secretary of the U.S. Department of Health and Human Services at the same time as notice is provided to the affected patients and in the manner specified on the U.S. Department of Health and Human Services website.

If the breach involves fewer than 500 patients, the HIPAA Compliance Officer shall maintain a log or other documentation of the breach and not later than sixty (60) days after the end of the calendar year, provide the required notification to the Secretary of the U.S. Department of Health and Human Services for breaches occurring during the preceding calendar year, in the manner specified by the Secretary of the U.S. Health and Human Services.

If a law enforcement official states that a notification, notice, or posting otherwise required by law would impede a criminal investigation or cause damage to national security, ISU shall:

1) delay such notification, notice, or posting for the time period specified by the law enforcement official in writing;

2) delay such notification, notice, or posting temporarily, and for no longer than thirty (30) days from the date the law enforcement official gives verbal notice, unless the law enforcement official provides a written statement during those thirty (30) days to delay for a longer period of time.

ISU shall evaluate any applicable state law requirements if there is a breach that includes electronic PHI. The HIPAA Compliance Officer will evaluate whether the potential breach includes a breach of PHI that may require notification under applicable state laws.

ISU’s IT Security shall monitor signs that may signal security incidents or breaches of electronic PHI have occurred or are occurring, including:

1) network intrusion detection sensor alerts when a buffer overflow attempt occurs against an FTP server;
2) antivirus software alerts when it detects that a host is infected with a worm;
3) the server crashes;
4) workforce members complain of slow access to the hosted software;
5) a system administrator sees a filename with unusual characters;
6) a workforce member receives a threatening email message;
7) the software host records an auditing configuration change in its log;
8) the application logs multiple failed login attempts from an unfamiliar remote system;
9) the network administrator notices an unusual deviation from typical network traffic flows;
10) unusual port scans of a group of targeted hosts;
11) web server log entries showing usage of a web vulnerability scanner;
12) announcement of a new exploit that targets a vulnerability of ISU’s mail server;
13) a threat that a group will attack the system.
Patient Rights

Notice of Privacy Practices
ISU recognizes that individuals have a right to adequate notice of ISU’s uses and disclosures of PHI, their rights with respect to their PHI, and ISU’s legal obligations in safeguarding PHI.

A written copy of the Notice of Privacy Practices (Notice) shall be given to all patients, their parent (if a minor), legal guardian, and/or personal representative, the first time the patient receives treatment or services. ISU will not be required to provide a written copy of the Notice at subsequent visits or delivery of services.

A copy of the Notice shall be written in plain language and posted prominently in the waiting room or admissions area of each covered entity, where it can easily be read. The Notice shall also be posted on the website of each covered entity.

A printed copy of the Notice shall be made available to any person, whether or not a patient, upon request. A copy of the Notice may be provided electronically if the person agrees to email delivery.

The first time a patient receives treatment or services, the patient or the patient’s authorized representative shall sign a receipt acknowledging that the Notice was provided. If a signature cannot be obtained, the covered entity shall document that a good faith attempt was made to obtain a signature on the acknowledgement. The patient shall receive a copy of the signed Notice, and the original or documentation that attempt was made to obtain a signature, shall be filed in the patient’s medical record.

In the case of an emergency, ISU shall not be required to provide the Notice or obtain a signed acknowledgement until after the emergency has been resolved.

If ISU makes any change to the Notice, it shall contain all the required elements that accurately reflect the law. The effective date of the new Notice shall be printed on the Notice, and shall not be retroactive. A revised copy of the Notice shall be posted prominently, and written copies shall be provided to anyone who requests it. If the changes are significant, a written copy must be provided at the patient’s first treatment or service after the effective date, and a patient or patient representative signature shall be obtained to document that ISU has provided a copy of the new Notice. Subsequent visits will not require that a written copy be given, unless it is requested.

ISU shall retain copies of the Notice(s) for six (6) years from the date of creation or revision.

Designated Record Set
PHI, confidential information, and records, including records from other providers, whether in paper or electronic format, that are used to make decisions about the patient served are considered part of the designated record set. The patient or personal representative has the right to inspect and obtain a copy of the designated record set. Administrative records, which includes investigative records, are not part of the designated record set.
If ISU receives a request for a copy of the complete record, the HIPAA Compliance Officer shall review the contents of the record prior to releasing a copy, and shall remove any components that ISU is authorized to restrict access to.

**General Requirements**

ISU shall, in general, disclose a patient’s PHI to any person, entity or company:

1) after verification that the disclosure is authorized by treatment, payment, or healthcare operations as defined in the privacy regulations;
2) who is a bona fide business associate;
3) when the discloser is the patient;
4) if a valid authorization has been received.

ISU shall release information received or created outside the process of providing treatment, payment, or healthcare operations only with direct authorization from the patient and consistent with the terms of the authorization.

Prior written consent to use or disclose PHI is not required:

1) if ISU has an indirect treatment relationship with the patient;
2) in an emergency;
3) if use or disclosure is required by law;
4) if the patient’s consent to receive treatment is clearly inferred by the circumstances.

**Designating a Personal Representative**

ISU shall treat a person as the personal representative of a patient if, under applicable law, such person has the authority to act on behalf of the patient who is an adult or an emancipated minor, to make decisions related to health care.

ISU shall treat a person as the personal representative of a patient if, under applicable law, such person is acting in loco parentis and has authority to act on behalf of an unemancipated minor in making decisions related to health care. However, ISU shall not treat a person as the personal representative of an unemancipated minor if the minor has the authority to act:

1) by consenting to the healthcare service and no other consent is required by law and the minor has not requested that such person be treated as the personal representative;
2) and lawfully obtain such healthcare services without consent of a person acting in loco parentis and the minor, a court, or another person authorized by law consents to such healthcare service;
3) and a person acting in loco parentis assents to an agreement of confidentiality by the healthcare provider and the minor with respect to such healthcare service.

**Right to Request Alternate/Confidential Communication**

ISU shall permit patients to request and receive confidential communications of PHI by alternative means or at alternative locations. Such request shall be immediately forwarded to the HIPAA Compliance Officer. The request shall be made in writing, and ISU shall verify and document the identity and authority of the person to make the request.

Reasonable requests must:

1) specify how payment will be handled if the request includes a change in the method of billing;
2) provide an alternate address with adequate details describing the alternative means of communications to be used;
3) include a method for the requestor to pay the extra cost of alternative communication (overnight service).

If the request is reasonable, ISU shall accommodate the request and the HIPAA Compliance Officer shall document the patient file. If it is unreasonable, the HIPAA Compliance Officer may deny the request and document why the request was determined to be unreasonable. In making the determination, the HIPAA Compliance Officer may consult with workforce members to determine if the circumstances support agreeing to the communication or if it would have a negative impact on the patient’s care, payment for care, or administration of benefits.

**Request for Access, Inspection, and Copies**

ISU recognizes that a patient has a right to access, inspect, and obtain a copy of PHI about the patient in a designated record set for as long as the PHI is maintained in the designated record set. The request must be in writing, and ISU shall act on the request no later than thirty (30) days after receipt of the request. If the request is accepted, ISU shall inform the patient and provide the requested records. If the request is denied, ISU shall provide a written denial. If ISU is unable to take action within thirty (30) days, ISU may extend the time by no more than thirty (30) days if it provides the patient with a written statement of the reason for the extension and the date by which ISU shall complete its action. No other extension of time is allowed.

ISU shall provide access to the PHI in the form or format requested by the patient if it is readily available in such form or format. If not, it shall be provided in a readable hard copy form or other form or format as agreed between ISU and the patient.

ISU may provide a summary or explanation of the PHI requested instead of providing access to all PHI if the patient agrees in advance to the summary and to any fees that may be imposed. A reasonable cost-based fee may be required, and must consist only of:
1) cost of copying (supplies, labor);
2) postage if the patient has requested it be mailed;
3) time to prepare the explanation or summary, if the patient has agreed to receive an explanation or summary.

ISU shall arrange with the patient a convenient time and place to inspect or obtain a copy of the PHI, or shall mail the PHI at the patient’s request. If PHI is requested in electronic form, ISU shall provide the patient with the PHI in the format requested by the patient if it is able to do so, or in a readable electronic format that the patient agrees to.

If the patient requests that ISU transmit the PHI to a third party, ISU shall provide the PHI to such third party if the patient’s request is in writing and signed by the patient, and clearly identifies the third party and where to send the PHI.

ISU will document the designated record sets subject to access and the person(s) or office(s) responsible for receiving and processing requests for access. All documentation, including the written request and any denials, shall be retained for six (6) years from the date of document creation or the date it was last in effect, whichever is last.
The right to access, inspect, or copy records does not include:

1) psychotherapy notes;
2) information compiled in reasonable anticipation of, or for actual use in a civil, criminal, or administrative action or proceeding;
3) disclosure prohibited by applicable law; or
4) disclosure that would jeopardize the safety of the patient or others.

The right also does not include PHI maintained by ISU that is:

1) subject to the Clinical Laboratory Improvements Amendments of 1988 (42 USC 263a) if access is prohibited by law;
2) exempt from the Clinical Laboratory Improvement Amendments of 1988 (42 CFR 293.3(a)(2));
3) obtained under confidentiality from a party other than a healthcare provider;
4) requested by a parent regarding a minor patient if the treating physician believes it is in the minor’s best interest to maintain privacy;
5) in a designated record set that includes the patient’s clinical records, payment and insurance records, and any other health information maintained and used by ISU to make decisions about the patient, except information used or created for quality assurance activities, to obtain legal advice, or for other internal operations of ISU.

ISU shall, upon written request, provide the patient with access to or a copy of the medical record in whole or in part, if it meets an exception above. If the patient requests specific information that is not contained in the designated record set but the department knows where the information is located, the patient will be given information as to where to direct the request for access.

ISU may deny patient access without giving the patient an opportunity for review if:

1) the PHI is exempted above;
2) the patient is an inmate and the correctional institution has directed ISU not to provide a copy because it would jeopardize the health, safety, security, custody, or rehabilitation of the patient or other inmates, an official or employee or other person responsible for the inmate;
3) the PHI was created or obtained in the course of research, while the research is in progress, and the patient agreed to the denial of access when consenting to participate in the research and was informed that the right of access would be reinstated once the research was completed;
4) the PHI is contained in records subject to the Privacy Act (5 USC 552a) if the denial of access meets the requirements of the law;
5) PHI was obtained from someone other than a healthcare provider under confidentiality and obtaining copies would be reasonably likely to reveal the source of the information;
6) the record includes the patient’s clinical records, payment and insurance records, and any other health information maintained and used by ISU to make decisions about the patient, but not including information used or created to conduct quality assurance activities, obtain legal advice, or other internal operations of ISU.

ISU may deny access if the patient is given the right to have the denial reviewed if:

1) a licensed healthcare professional has determined that access is reasonably likely to endanger the life or physical safety of the patient or another person;
2) the PHI refers to another person that is not a healthcare provider, and a licensed healthcare professional has determined that access is reasonably likely to cause substantial harm to the person;
3) the request is made by the patient’s personal representative and a licensed healthcare
professional has determined that access by the personal representative is reasonably likely to cause substantial harm to the patient or another person.

If allowed, the denial shall be promptly reviewed by a licensed healthcare professional designated by ISU. Such licensed healthcare professional must not be directly involved in the denial of access, and shall, within a reasonable period of time, determine whether or not to deny the requested access. The covered entity shall promptly provide written notice to the requestor of the determination, and take necessary action to carry out the reviewing professional's determination. The determination shall be made in plain language and include:

1) the basis for the denial;
2) a statement of the patient's review rights and how to exercise the review rights;
3) a method to complain to ISU, including the name and telephone number of the HIPAA Compliance Officer, or to the Secretary of the U.S. Department of Health and Human Services for failure to comply with the request.

If the denial is in part, ISU shall give the patient access to the portion that can be accessed.

Request for Amendment and Error Correction
ISU recognizes that a patient has the right to have PHI or a record in a designated record set amended for as long as the PHI is maintained in the designated record set.

ISU may deny a patient’s request for amendment if it determines the PHI or record:

1) was not created by ISU unless the patient provides a reasonable basis to believe that the original party that had the PHI is no longer available to act on the amendment;
2) is not part of the designated record set;
3) would not be available for patient inspection under this manual;
4) is accurate and complete.

ISU shall provide the patient with a written denial within sixty (60) days of the date the request was received. The person authorized by the HIPAA Compliance Officer, such as a Clinic Director, shall provide the written denial, which shall be in plain language and contain:

1) the basis for denial;
2) the patient’s right to submit a written rebuttal to the denial and how to file the rebuttal (ISU may reasonably limit the length of the rebuttal);
3) a statement that if the patient does not submit a written rebuttal, the patient may request that ISU provide the patient’s request for amendment and the denial with any future disclosures of PHI;
4) a description of how the patient may complain to the HIPAA Compliance Officer or the Secretary of the U.S. Department of Health and Human Services for failure to comply with the request.

If ISU cannot provide a written denial within sixty (60) days of the date the request was received, the authorized person(s) may provide a written statement to extend the time by no more than thirty (30) days, and include the reasons for the delay and the date by which ISU shall respond. There shall be no other extension of time.

The HIPAA Compliance Officer may prepare a written response to the patient’s rebuttal, which shall be provided to the patient. ISU shall identify the record or PHI in the designated record set that is the
subject of the amendment and the patient’s request for any amendment, ISU’s denial of the request, the patient’s rebuttal, if any, and ISU’s response, if any, to the designated record set. ISU shall include this information with any subsequent disclosure of PHI. If a subsequent disclosure is made using a standard transaction (as defined by HIPAA Transaction Rules) that doesn’t permit additional material to be included with the disclosure, ISU may separately transmit the request for amendment, ISU’s denial of the request or summary of such information to the recipient of the standard transaction.

If ISU grants the requested amendment, it shall act on the request for amendment within sixty (60) days after receipt of the request. If ISU is unable to act on the request within the time required, the time may be extended by no more than thirty (30) days if the patient is provided with a written statement of the reasons for the delay, and the date by which ISU will complete the request. No other extension of time is allowed.

ISU shall identify the records in the designated record set that are affected by the amendment and append or otherwise link the amendment to the record. ISU will inform the patient in writing, that the amendment is accepted. If the patient agrees, ISU shall notify any other party with which the amendment needs to be shared, such as business associates, or any other party that may rely on or could rely on such information to the detriment of the patient.

If ISU is notified by another healthcare provider or agency of an amendment to a patient’s PHI, ISU shall amend the PHI in designated record sets.

ISU shall document the title of the person(s) and covered entity(s) responsible for receiving and processing requests for amendments by patients. Such requests, and if applicable, denials, will be retained for six (6) years from the date the document was created or the date it was last in effect, whichever is later.

**Right to File a Complaint**
ISU recognizes that patients have the right to file a formal complaint concerning privacy issues. Workforce members shall not retaliate against any person who files a complaint through intimidation, threats, coercion, discrimination, or any other retaliatory action. Allegations may include, but are not limited to:

1) inappropriate use or disclosure of PHI;
2) wrongful denial of access or amendment rights;
3) inaccurate Notice of Privacy Practices.

Complaints shall be directed to the HIPAA Compliance Officer by telephone, email, fax, or in person. The HIPAA Compliance Officer shall document each complaint and investigate promptly. Upon completion of the investigation, the HIPAA Compliance Officer shall respond to the complainant in writing noting his or her findings and what action, if any, shall be taken in response to the complaint. Complaint files shall be kept for six (6) years after the date it is created or the date when it was last in effect, whichever is later.

Complaints made to the Secretary of the U.S. Department of Health and Human Services must:

1) be in writing, either on paper or electronically,
2) name the covered entity that is the subject of the complaint and describe the acts or omissions that are allegedly in violation of the privacy or security regulations;
3) be filed within 180 days of when the complainant became aware, or should have known, that
the act of omission complained about occurred, unless the Secretary waives this time limit.

ISU acknowledges that the Secretary of the U.S. Department Health and Human Services is empowered to investigate any complaint. ISU shall:

1) cooperate with any investigation or compliance review;
2) maintain records, including pertinent policies and procedures or practices, and the circumstances surrounding any alleged violation;
3) submit compliance reports or corrective action plans in a timely manner as required by the Secretary.
Security

**Physical Safeguards**
ISU shall ensure that physical safeguards are in place to guard the integrity, confidentiality and availability of PHI. These physical safeguards relate to the protection of physical computer systems and devices from intrusion, environmental hazards, and natural disasters.

Workforce members shall limit the use of assigned portable computers, tablets, or devices that contain or can access patient ePHI. ISU shall ensure that all portable devices are encrypted and have appropriate password and security programs installed. No portable device shall be set up to automatically back up files to the cloud; such backup must be disengaged. Workforce members shall not access ePHI where it could be seen by persons who do not have a need to know. Workforce members shall close connections to email and other programs that contain ePHI immediately when finished using the program.

Workforce members shall only attempt to log onto systems and programs that they have been approved to access after they have properly obtained valid access credentials.

Workforce members shall not load any software on ISU hardware unless it has been appropriately vetted by the HIPAA Compliance Officer or designee.

Workforce members shall not store ePHI on removable media or memory devices such as flash drives/thumb drives unless necessary and approved by the HIPAA Compliance Officer. If such storage is necessary, the device shall be encrypted, kept on the person or securely stored, not left attached to a computer, and only contain the minimum amount necessary.

The Clinic Directors or designee shall maintain a current list of portable devices, serial number, ISU inventory tag number, if encrypted, and who is assigned to the device. If portable devices, removable media, or memory devices are lost or stolen, the HIPAA Compliance Officer shall investigate and take corrective action as necessary.

ISU shall keep an accurate inventory of hardware, and conduct periodic physical inventory to maintain accuracy.

**Access Controls**
ISU shall ensure that access to information in the possession of, or under the control of, ISU will be provided based on a need-to-know in order to perform job duties. ISU has established access controls that will restrict access to PHI to those workforce members who have a business need to access or use PHI.

Business associates will be given access to PHI only when there is a legitimate business need for the information and a BAA is in place.

Workforce members and business associates shall not attempt to access PHI unless they have been granted appropriate access rights and have a clear business reason to do so.

ISU recognizes that each covered entity is the true custodian of the PHI, but ISU is the “owner” of such PHI, as well as billing information, copies of records, and any other data and information delivered or
submitted for billing purposes is also “owned” by ISU. ISU shall determine workforce member access rights for security of the information. The level of access shall be assigned based on a need-to-know that is directly related to the workforce member’s duties and responsibilities.

All workforce members, business associates, outside contractors, and temporary employees who perform work remotely shall comply with the requirements for remote access. Remote access must be reviewed by IT Security.

Any ISU workforce member who is also a patient is required to comply with the same procedures as all other patients related to accessing and amending his or her medical record. Such workforce member may not use the privileges associated with his or her position at ISU to view personal medical records or related PHI, including billing records, or the records of family or friends.

ISU’s information systems shall authenticate using unique user IDs and passwords and multi-factor authentication when available. The password must be at least 8 characters in length, use upper and lower case letters, numbers, and symbols. When a workforce member receives a temporary password, he or she shall change it when logging in for the first time. The password is valid for 180 days, then the workforce member shall change his or her password. Workforce members shall not write passwords down where they are accessible by others, nor shall they share passwords with others. If someone requests the password, the workforce member shall not provide it, and shall report the request to the HIPAA Compliance Officer.

Software that provides access to ePHI that includes an auto logoff function to terminate the session after a maximum period of thirty (30) minutes of inactivity shall be configured to do so. All workstations shall have screensaver software or user lockout after a period of fifteen (15) minutes of inactivity.

Error logs shall be reviewed by the HIPAA Compliance Officer or designee monthly to identify threats to the system, abnormalities, and possible security issues.

ISU shall require all workforce members to have a unique password to access ISU networks. ISU shall also require that each covered entity workstation has a username and password to gain access. If the workstation is shared by several workforce members, each individual user shall have a unique username and password.

Files containing ePHI shall not be saved on an unencrypted workstation drive. ISU has purchased a subscription to Box, and the minimum necessary sensitive information shall be saved in Box for the minimum amount of time.

ISU shall maintain, including updates to network monitoring software, intrusion detection and reporting. If a security incident is detected, the HIPAA Compliance Officer or designee shall immediately begin an investigation into the nature, scope, and source of the incident, as well as the potential harm from the incident. This includes determining what information is at risk and at what level of risk. The HIPAA Compliance Officer or designee shall determine the best strategy to contain the incident, and implement such strategy, including isolating the systems that have been compromised. Such systems shall remain isolated until the incident is resolved. Once resolved, the HIPAA Compliance Officer or designee shall investigate and determine if ePHI was lost or altered, the extent of loss or alteration, and shall restore lost or altered information. If ePHI was disclosed during the incident, the HIPAA Compliance Officer shall log the disclosure. The HIPAA Compliance Officer shall document the incident, including date, extent,
duration, response, and other pertinent information he or she believes is necessary. The HIPAA Compliance Officer shall complete a risk assessment of risks and vulnerabilities associated with the systems and processes of the incident and determine if changes are required to minimize the risk of reoccurrence.

ISU shall ensure that every workforce member that needs access to PHI is authorized to access the minimum necessary PHI to perform his or her duties by the appropriate data custodian. When authorizing access, the data custodian shall refer to the job descriptions and PHI needs, and establish the workforce member’s access to the system, by instituting the appropriate accounts and account permissions. If the workforce member’s position changes or the need for access to PHI changes, the data custodian shall review the change and revise the authorization accordingly.

**Security of Physical Offices**
Physical access to the covered function will be controlled by keys or card reader access. The HIPAA Compliance Officer shall ensure that the appropriate workforce members have keys or cards, and shall audit key issuance on a periodic basis. All external doors shall be locked after business hours.

Visitors who require access to areas not available to the general public shall be escorted by a workforce member who has appropriate access to the areas the visitor needs to visit.

**Retention, Disposal, and Storage of PHI**
ISU shall destroy ePHI contained on electronic storage devices when it is no longer needed in such a manner that it is no longer readable, retrievable, or accessible. If ePHI is being erased, a method that overwrites existing data, such as DoD 5220.22-M shall be used. If the hardware is going to be reused, the HIPAA Compliance Officer or designee shall reinstall the operating system and necessary software the new user requires.

Magnetic storage media, such as external hard drives, floppy disks, thumb drives, and other removable storage media that is no longer needed shall be given to the HIPAA Compliance Officer. Such magnetic storage media shall be magnetically erased, physically destroyed, or wiped using a method such as DoD 5220.22-M before being properly disposed of in accordance with laws, rules, and regulations.

Optical storage, such as CDs and DVDs that are no longer needed shall be given to the HIPAA Compliance Officer to ensure that such optical storage is rendered physically unusable prior to disposal.

If medical records will be stored in a separate facility, ISU shall securely transport them in a locked container, bag, or case that can be closed. Such container, bag, or case shall be placed in the vehicle in a manner that it is not visible from outside the vehicle. PHI shall not be left in an unattended vehicle, unless absolutely necessary, and not for an unreasonable amount of time. PHI shall never be left in a vehicle overnight. If PHI is lost or stolen, the HIPAA Compliance Officer shall be notified immediately and a police report shall be filed.

ISU shall ensure that the storage facility has appropriate environmental standards to minimize risk of damage from fire, theft, water, natural disasters, and other potential threats. ISU shall enter into a BAA with such facility, and the HIPAA Compliance Officer shall be responsible for managing and properly retaining the records.
**Mitigation**

ISU shall mitigate, to the extent possible, any harmful effect of a use or disclosure of PHI in violation of this manual or federal or state laws, rules, and regulations.

The HIPAA Compliance Officer or designee shall ensure that workstations that can access ePHI have antivirus software that automatically scans local disks, downloaded files, and electronic media connected to the workstation. The software shall detect and remove malicious software. The antivirus software shall be regularly updated with the most current virus definitions and patches.

ISU shall ensure that a firewall is configured between the internet and its local area network. The firewall shall be configured to allow workforce members to use the internet when necessary, but should prevent unauthorized access into the local area network. Downloaded software shall be screened with virus detection software prior to being run or opened.

Any electronic health record system used by workforce members that contains ePHI shall track log-in history and shall be periodically audited.

**Security Breach**

A breach can be a security incident, which includes but is not limited to:

1. unauthorized use of workstation;
2. denial or disruption of service;
3. unauthorized altered or destroyed input, processing, storage, or output of PHI;
4. unauthorized changes to information system hardware, firmware, or software;
5. successful attack vector;
6. unauthorized use of computer accounts and computer systems;
7. complaints of improper use of information resources;
8. compromise of system integrity;
9. malicious use of system resources;
10. any type of damage to a system.

Any person who believes that ISU is out of compliance with the applicable requirements of privacy and security laws may file a complaint with the HIPAA Compliance Officer and/or the Secretary of the U.S. Department of Health and Human Services. ISU shall include contact information for filing a complaint in its Notice of Privacy Practices, including name, title, and telephone number of the HIPAA Compliance Officer.

The HIPAA Compliance Officer shall investigate any alleged violation as soon as reasonably practicable, and workforce members shall cooperate in such investigation. Workforce members shall report any known or suspected violation of privacy or security regulations to the Clinic Director and the HIPAA Compliance Officer immediately.
Administration

Organizational Structure and Responsibilities
The HIPAA Compliance Officer is the single point of contact responsible for the management of both privacy and IT security compliance. The HIPAA Compliance Officer shall oversee the privacy and security of covered entity activities and work closely with the covered entity’s directors, administrators, the IT Security Department, and other staff. The HIPAA Compliance Officer shall report significant violations to the Vice President for Health Sciences, the Chief Information Officer, and the General Counsel and Chief Compliance Officer.

The HIPAA Compliance Officer is responsible for the development and implementation of all privacy and security procedures, and may delegate duties as necessary. The HIPAA Compliance Officer shall coordinate with appropriate covered entity personnel to ensure proper implementation of privacy and security measures. The HIPAA Compliance Officer shall:

1) develop HIPAA privacy and security objectives and procedures;
2) develop implementation plans and propose support mechanisms for the objectives and procedures;
3) implement the objectives and procedures;
4) determine the methodology for accomplishing the goals of the objectives and procedures;
5) manage and update the procedures;
6) direct training and awareness programs;
7) oversee ongoing monitoring of processes by performing privacy and security risk assessments of each covered entity at least twice a year;
8) provide corrective action plans for any findings of risk assessments;
9) research and understand federal and state regulatory requirements;
10) research and understand privacy and security technology;
11) maintain written or electronic copies of documentation related to communications, actions, activities, investigations, and training for a period of six (6) years from the date of creation or the date when it was last in effect, whichever is later.

The HIPAA Compliance Committee shall be managed by the HIPAA Compliance Officer. This committee shall meet regularly to:

1) review the current status of privacy and security compliance;
2) review and monitor privacy and security incidents;
3) review and approve of privacy projects;
4) review and approve of security projects;
5) perform other necessary privacy and security management activities.

The HIPAA Compliance Officer and HIPAA Compliance Committee shall develop a risk management plan that includes:

1) conducting an accurate and thorough risk assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI;
2) reducing exposure to identified risks;
3) implementing security measures or new procedures to reduce the risks and vulnerabilities to a reasonable and appropriate level.
Clinic Directors are responsible for implementing the privacy and security procedures in a manner consistent with the criticality, value, and sensitivity of the PHI being handled. Clinic Directors are responsible for documenting patient complaints and escalating such complaints to the HIPAA Compliance Officer for investigation, tracking, and trending purposes, and for administering any corrective actions consistent with procedure.

Outside consultants, contractors, and temporary workers are subject to the same privacy and security requirements as workforce members. This includes, but is not limited to, physicians, students, outsourced employees. Any outside consultant, contractor, or temporary worker shall be monitored with regard to presence in areas that are restricted because of proximity to PHI.

**Onboarding and Offboarding**

All new workforce members shall participate in an orientation program to receive detailed training about the procedures and methods for safeguarding the privacy and security of PHI before beginning work. If the workforce member cannot participate before his or her start date, the Clinic Director shall be responsible for providing an overview of responsibilities related to privacy and security. The workforce member shall complete the detailed training as soon as practicable.

Privacy and security obligations shall be clearly communicated to workforce members who have access to PHI. Performance related to privacy and security responsibilities shall be evaluated each year on performance evaluations.

Clinic Directors shall inform the HIPAA Compliance Officer, or his or her designee when a workforce member separates from service with ISU. In the event of an involuntary termination, the workforce member shall:

1) be immediately relieved of all duties;
2) return all ISU equipment, information, and documentation;
3) be accompanied by another ISU employee when retrieving personal effects;
4) have all system access removed immediately.

If the workforce member voluntarily terminates, his or her immediate supervisor shall:

1) ensure all ISU equipment, information, and documentation is returned by the termination date;
2) remove system access on the final day of employment.

**Training**

The HIPAA Compliance Officer is responsible for annual HIPAA training, either in person or online. Workforce members, contractors, and subcontractors shall be trained:

1) within thirty (30) days of start of work;
2) within thirty (30) days after a material change to this manual;
3) within thirty (30) days of the HIPAA Compliance Officer determination that the person has disregarded privacy laws or has been involved in a privacy or security incident.

The HIPAA Compliance Officer shall provide periodic privacy and security reminders to workforce members at meetings, through email, or when visiting the covered entities. Such reminders may include items such as password protection, email attachments, verifying requestor identity, ensuring authorizations are valid, etc. In the event of a security incident, or recurring lapses in security, the HIPAA
Compliance Officer shall issue a reminder to all workforce members that focuses on the incident and how to avoid future incidents.

The HIPAA Compliance Officer shall maintain documentation of training for six (6) years after the date of training.

Any workforce member, contractor, or subcontractor who fails to complete the training as required shall not be able to access, use, or disclose PHI.

Confidentiality Agreements
ISU shall ensure that all workforce members sign a confidentiality agreement each year. Such agreements shall be kept in a secure location. Such agreements shall be retained for seven (7) years from the date of creation or from the date when it was last in effect, whichever is later.

Whistleblowers
A workforce member or a business associate may disclose PHI and de-identified PHI as permitted by HIPAA in accordance with this manual, provided that:

1) the workforce member or business associate believes in good faith that ISU has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by ISU may endanger one or more persons served or supported by ISU or the public;
2) the disclosure is made to a health oversight agency or public health authority that is authorized by law to investigate or oversee the relevant conduct or conditions of ISU;
3) the disclosure is made to an appropriate healthcare accreditation organization for the purpose of reporting an allegation of failure to meet professional standards or misconduct by ISU;
4) the disclosure is made to an attorney retained by the workforce member or business associate to determine the legal options of the workforce member or business associate with regard to the conduct.

ISU shall not require a patient to waive his or her right to file a complaint with the Secretary of U.S. Department of Health and Human Services for a privacy violation as a condition for treatment or payment.

Retaliation
Workforce members shall not intimidate, threaten, coerce, discriminate against, or take any retaliatory action against:

1) any person who exercises his or her rights in this manual or in the HIPAA regulations;
2) any person who files a complaint with the U.S. Secretary of the Department of Health and Human Services;
3) any person who testifies, assists in, or participates in an investigation, review, proceeding, or hearing conducted by a government agency; or
4) any person who opposes any act or practice that is made unlawful by HIPAA regulations if the person has a good faith belief that the practice opposed is unlawful, the manner of opposition is reasonable, and the opposition does not disclose PHI in violation of HIPAA or this manual.
Sanctions
ISU shall apply the appropriate sanctions against workforce members, contractors, temporary employees, and business associates who fail to comply with ISU’s privacy and security manual. Sanctions include disciplinary actions, up to and including termination of employment or termination of a contract. The type of discipline taken against a workforce member who violates the provisions of this manual will be determined on a case-by-case basis, in a fair and equitable manner. Disciplinary actions will be consistently applied and enforced.

Violations may be the result of simple negligence, gross negligence, willful acts or omissions, or intentional or reckless behavior. Mitigating factors for sanctions include:

1) whether the workforce member promptly reported the violation;
2) whether this is the first violation;
3) whether the workforce member fully cooperates in the investigation;
4) whether the workforce member cooperates in correcting the violation.

A corrective action plan may include remedial training in the form of one-on-one training, an online training module, or other organized training session to prevent similar violations in the future.

Whatever discipline is imposed is left to the discretion of ISU.

A Severity Level 1 violation includes a workforce member inadvertently or mistakenly accessing PHI that he or she does not have a need to know to carry out responsibilities, or carelessly accessing or disclosing information that he or she has authorized access to. This includes, but is not limited to:

1) leaving PHI in a public area;
2) sending email or fax with PHI to the wrong recipient;
3) discussing PHI in an area where it can be overheard;
4) leaving a computer with PHI unattended and accessible to nonauthorized persons;
5) losing an unencrypted electronic device that has unsecured PHI;
6) improperly disposing of PHI;
7) failing to report a potentially compromised password.

A Severity Level 2 violation includes a workforce member intentionally accessing and/or using PHI without authorization and without disclosure. This includes, but is not limited to:

1) intentional, unauthorized access to another individual's PHI;
2) obtaining PHI under false pretenses;
3) failing to verify the identity of individuals requesting PHI, which results in an unauthorized disclosure, access to, or use of PHI;
4) connecting a device to the network or uploading software without authorization;
5) a second occurrence of a Severity Level 1 violation (which does not have to be the same offense).

A Severity Level 3 violation includes a workforce member intentionally accessing, using, and/or disclosing PHI without authorization and without malice or personal gain. This includes, but is not limited to:

1) sharing PHI with the news media;
2) modification of an electronic document to expedite a process;
3) intentionally helping another individual to gain unauthorized access to PHI;
4) disclosing patient condition, status or other PHI to a workforce member who does not have a legitimate need to know;
5) logging into a system and allowing another person to access PHI;
6) a second occurrence of a Severity Level 2 violation (which does not have to be the same offense);
7) a Severity Level 1 violation with a Severity Level 2 violation.

A Severity Level 4 violation includes a workforce member intentionally accessing, using, and/or disclosing PHI without authorization for personal or financial gain; or causing physical or emotional harm to another person; or causing reputational or financial harm to ISU. This includes, but is not limited to:
1) unauthorized and intentional disclosure of PHI to anyone;
2) intentionally assisting another person to gain unauthorized access to PHI in order to cause harm;
3) accessing, using, or disclosing PHI for personal gain;
4) accessing, using, or disclosing PHI for financial gain;
5) accessing, using, or disclosing PHI in a manner that results in personal, financial, or reputational harm to the patient;
6) a second occurrence of a Level 2 or 3 violation (which does not have to be the same offense);
7) a Severity Level 1 violation along with a Severity Level 2 violation or Severity level 3 violation;
8) multiple occurrences of any Severity Level 1 violation.

**Emergency Operations**

ISU is aware that an emergency may damage or render unavailable, systems containing ePHI, such as system crash, virus, hardware failure, natural disaster, or malicious attack. ISU shall backup critical network data on a daily basis, and maintain off-site data storage as well. Removable media and storage shall be located in a fireproof safe. If reinstallation of systems is required, the HIPAA Compliance Officer shall work with the IT department to ensure it is properly performed. No unauthorized workforce member shall attempt to reinstall any program.

If the ePHI, and other data and files can be recovered from the backup copies, ISU shall use this method of restoration. If this is not possible, restoration shall occur from the off-site storage.

ISU recognizes that under emergent situations, if wi-fi and Internet systems are unavailable, access to medical records may be accessed through ISU-owned wireless devices. If electronic records cannot be accessed, handwritten records shall be created and stored in a secure filing cabinet. Wireless devices may be used for dictation for transcription at a later date.

If access to current medical records is not available, the workforce member shall document his or her findings and a paper chart shall be completed on the patient. These medical records shall be merged with the patient’s other records as soon as practicable.

If a covered entity is unable to provide services during the emergent situation, it shall secure the office until normal operations can resume.

**Social Media**

ISU recognizes that workforce members participate in social media and chat rooms. ISU also recognizes that workforce members may use their @isu.edu email address for personal use. If workforce members
use their ISU email address, they shall make it clear that any opinions they express are their own and not that of ISU. Workforce members shall not publicly disclose any confidential information.

Workforce members shall not create any website that is hosted on ISU computers or accessed through ISU’s network.
Appendix

Accounting of Disclosures of PHI for Research
Accounting of Disclosures of Protected Health Information
Authorization to Use and/or Disclose PHI
Business Associate Agreement Template
Confidentiality Agreement
Consent for Alternative Communication
Disclosure of PHI Without Authorization
Electronic Health Record Access
Electronic Health Record Roles and Permissions
Hybrid Entity Policy ISUPP 10010
Information Security Incident Response
Information Technology Services Compliance and Sanctions ISUPP 2460
Limited Data Set Request
Minimum Necessary Forms
Notice of Privacy Practices
Request for Amendment of Health Information
Request for Confidential Communication
Request for De-Identified Information
Request to Restrict the Use and Disclosure of PHI
Revocation or Termination of Restriction of the Use and Disclosure of PHI
Risk Assessment Form
Use and Disclosure of PHI for Research
Accounting of Disclosures of PHI for Research

Name and Address of Clinic Making Disclosure:

Patient Name: _____________________________ Medical Record Number: _____________________________

Billing Number: ___________________________ Request Date: _____________________________

Accounting Period: From: ___________ To: ___________ Accounting Date: ___________

During the accounting period listed above, I participated in Institutional Review Board or Privacy Board approved research activities where the protected health information of fifty (50) or more patients was disclosed to another entity or researcher. Information about the research activity is listed below. My PHI may or may not have been included in the research activity. (If you need assistance in contacting the entity that sponsored the research and the researcher(s), please contact the HIPAA Compliance Officer at [Address and telephone number]).

Name of Protocol or Research Activity: _____________________________

Description of 1) the protocol or research activity; 2) purpose of the research; and 3) criteria for selecting records: _____________________________

Brief description of the type of PHI disclosed: _____________________________

Date or period of time disclosures occurred: _____________________________

Date of last disclosure: _____________________________

Name of research sponsor to whom PHI was disclosed: _____________________________

Address: _____________________________

Telephone number: _____________________________

Name of research sponsor to whom PHI was disclosed: _____________________________

Address: _____________________________

Telephone number: _____________________________
# Accounting of Disclosures of Protected Health Information

**Name and Address of Clinic Making Disclosure:**

Patient Name: ___________________________ Medical Record Number: ___________________________

Billing Number: ___________________________ Request Date: ___________________________

Accounting Period: From: ____________ To: ____________ Accounting Date: ____________

<table>
<thead>
<tr>
<th>Date of Disclosure</th>
<th>Name of Person or Entity Receiving PHI</th>
<th>Brief Description of PHI Disclosed</th>
<th>Brief Statement of Purpose of Disclosure</th>
<th>Copy of Written Request Attached?</th>
<th>Multiple Disclosures to Same Person or Entity During Period Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>No ___ Yes ___</td>
<td>No ___ Yes ___ If yes, describe frequency, periodicity, or number of disclosures</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Date of last disclosure in period:</td>
</tr>
</tbody>
</table>


Authorization to Use and/or Disclose Protected Health Information

Patient Identification

Printed Name: ____________________________ Date of Birth: ________________
Address: ________________________________________________

Social Security #: ____________________________ Telephone: _______________________

Information To Be Released – Covering the Periods of Health Care

From (date) ____________________________ to (date) ____________________________

From (date) ____________________________ to (date) ____________________________

Please check type of information to be released:

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>___ Entire medical record</td>
<td>___ Pathology report</td>
<td>___ Discharge summary</td>
</tr>
<tr>
<td>___ History and physical exam</td>
<td>___ Consultation reports</td>
<td>___ Progress notes</td>
</tr>
<tr>
<td>___ Laboratory test results/reports</td>
<td>___ X-ray reports</td>
<td>___ X-ray films / images</td>
</tr>
<tr>
<td>___ Operative report</td>
<td>___ Emergency room record</td>
<td>___ Itemized bill</td>
</tr>
</tbody>
</table>

___ Other, (specify) ____________________________

Purpose of Request

___ Treatment or consultation

___ At the request of the patient

___ Billing or claims payment

___ Other, (specify) ____________________________

Person Authorized to Receive Information

Name: ____________________________________________
Address: ____________________________________________

Drug and/or Alcohol Abuse and/or Psychiatric and/or HIV/AIDS Records Release

I understand that if my medical or billing record contains information in reference to drug and/or alcohol abuse, psychiatric care, sexually transmitted disease, Hepatitis B or C testing, and/or other sensitive information, I agree to its release. Check One: ___ Yes ___ No Initials ______

I understand that if my medical or billing record contains information in reference to HIV/AIDS (Human Immunodeficiency Virus/Acquired Immunodeficiency Syndrome) testing and/or treatment, I agree to its release. Check One: ___ Yes ___ No Initials ______
**Time Limit and Right to Revoke Authorization**
Except to the extent that action has already been taken in reliance on this authorization, at any time I can revoke this authorization by submitting a notice in writing to the ISU HIPAA Compliance Officer at [location and mailing address]. Unless revoked, this authorization will expire on the following date or event ____________.

**Re-disclosure**
I understand the information disclosed by this authorization may be subject to re-disclosure by the recipient and will no longer be protected by the Health Insurance Portability and Accountability Act of 1996.

**Signature of Patient or Personal Representative Who May Request Disclosure**
I understand that ISU may not condition my treatment on whether I sign this authorization form unless specified above under Purposes of Request. I can inspect or copy the protected health information to be used or disclosed. I authorize ________________ (Name of Facility or Provider) ________________ to use and disclose the protected health information specified above.

Signature: ___________________________ Date: ___________________________

Authority to Sign if not patient:

____________________________________________________________________

Identity of Requestor Verified via: ___ Photo ID ___ Matching Signature ___ Other, specify ______

____________________________________________________________________

Verified by: ___________________________
Denial of Access to Protected Health Information

Date: ______________________________

To: [Name and address of patient or personal representative] ______________________________

From: [Name and Title of ISU HIPAA Compliance Officer] ______________________________

Idaho State University (“ISU”) is denying you access to inspect and copy your protected health information (PHI) as requested by you on [date]. The portions of your health information you are denied access to, include:

___ All records; or
___ Portions specified here*: __________________________________________

*If access to only a portion of the record described in your request is denied, we will provide access to those other portions of your records included in your request.

Reason for Denial of Access to PHI

A. ISU has denied your access, and you may not request a review of this denial because of the following circumstance(s):

___ The PHI is either psychotherapy notes, information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative proceeding; or subject to the Clinical Laboratory Improvement Amendments of 1988.

___ ISU is acting under the direction of a correctional institution where the patient is an inmate and it is judged that obtaining a copy would jeopardize the patient’s health, safety, security, custody, or rehabilitation, or of other inmates, or the safety of an officer, employee, or other person at the correctional institution or those responsible for transporting the inmate.

___ The PHI was obtained in the course of research, and the patient agreed to the denial of access in consenting to participate in the research. The research is in progress; once the research has concluded, access to these records may be permitted.

___ The PHI is contained in records subject to the Privacy Act, 5 U.S.C. 522a.

___ The PHI was obtained under a promise of confidentiality from someone other than a health care provider and the inspection and copying is likely to reveal the source of the information.

B. ISU has denied your access, and you may request a review of denial by a licensed healthcare professional designated by ISU who did not participate in this decision to deny access. Submit your written request for review of denial to [Name and address of ISU Privacy Officer].
Your request is denied because:

___ A licensed healthcare professional has determined the inspection and copying of this PHI is reasonably likely to endanger the life or physical safety of the patient or another person.
___ The PHI contains data about another person and a licensed healthcare professional has determined that the inspection and copying is reasonably likely to cause substantial harm to that person.
___ The request for access has been made by the patient’s personal representative and a licensed healthcare professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the patient or another person.

C. ISU does not maintain the protected health information you requested.

___ ISU does not know who maintains the PHI you requested.
___ Please contact the provider or facility that maintains your PHI: [Name and address of Provider or Facility]

How to Complain About this Denial of Access to PHI

You have the right to complain about this action to [Name or title, and telephone number or ISU HIPAA Compliance Officer] and to the Secretary of the United States Department of Health and Human Services at:
BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (“Agreement”) between Idaho State University, on behalf of its ___________________________ Clinic (“Covered Entity”) and ___________________________________________ (“Business Associate”) (each individually, a “Party,” and collectively, the “Parties”) takes effect on the _____, day of ____________, 202_ (“Effective Date”).

I. Purpose and Intent

1.1 Business Associate has agreed to perform certain services for or on behalf of Covered Entity, which services may involve the use or disclosure of Protected Health Information within the meaning of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) as it may be amended from time to time and its implementing regulations, 45 CFR Parts 160 and 164 (“the Privacy Rule”) and the Health Information Technology for Economic and Clinical Health Act included in the American Recovery and Reinvestment Act of 2009, (the “HITECH Act”). This Agreement supplements the Parties’ agreement(s) for services and is intended to satisfy the requirements for Business Associate Agreements as set forth in the Privacy Rule, including 45 CFR § 164.50(e) and the HITECH Act. Business Associate hereby agrees to comply with applicable provisions of the Privacy Rule and the HITECH Act and to assist Covered Entity with its compliance as explained below.

II. Definitions

2.1 HITECH Act means the “HITECH Act” the Health Information Technology for Economic and Clinical Health Act included in the American Recovery and Reinvestment Act of 2009.

2.2 Designated Record Set means (1) medical records and billing records about individuals maintained by or for Covered Entity; and (2) other records used by or for Covered Entity to make decisions about Individuals. See 45 CFR § 164.501.

2.2 Individual means the person who is the subject of Protected Health Information, and any person who qualifies as a personal representative of such person in accordance with 45 CFR § 164.502(g). See 45 CFR § 164.501.

2.3 Protected Health Information (PHI) means any information which is created or received by Business Associate from or on behalf of Covered Entity, whether oral or recorded in any form or medium, that 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. See 45 CFR § 160.103.
2.4 Secretary shall mean the Secretary of the Department of Health and Human Services or his or her designee.

2.5 Terms used but not otherwise defined in the Agreement shall be defined as set forth in 45 CFR Part 160 and Part 164, Subparts A and E and the HITECH Act.

III. Obligations of Business Associate

3.1 Business Associate agrees to not use or disclose PHI other than as permitted or required by the Agreement or as required by law.

3.2 Business Associate agrees to use appropriate safeguards to maintain the privacy of the PHI and to prevent use and/or disclosure of the PHI other than as provided for by this Agreement.

3.3 Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.

3.4 Business Associate agrees to immediately report to Covered Entity any use or disclosure of the PHI not provided for by this Agreement of which it becomes aware.

3.5 Business Associate agrees to ensure that any agent to whom it provides PHI, including a subcontractor, agrees to the same restrictions and conditions concerning the information that apply through this Agreement with Business Associate. Business Associate may comply with this section by entering into a contract with such agent or subcontractor, which contract requires the agent or subcontractor to comply with the terms of the Agreement.

3.6 Upon a request by Covered Entity, Business Associate agrees to provide access to PHI maintained in a designated Record Set to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR § 164.524. Business Associate shall provide access to the PHI in the time and manner designated by Covered Entity.

3.7 Upon a request by Covered Entity or an Individual and at Covered Entity’s direction or agreement, Business Associate agrees to make any amendment(s) to PHI maintained in a Designated Record Set in order to meet the requirements under 45 CFR § 164.526. Business Associate shall act on the amendments in the time and manner designated by Covered Entity.

3.8 Business Associate agrees to make internal practices, books, and records (including policies and procedures and PHI) relating to the use and disclosure of PHI received from Covered Entity or created or received by Business Associate on behalf of Covered Entity, available to Covered Entity or to the Secretary for purposes of the Secretary determining Covered Entity’s compliance with the Privacy Rule. Business Associate shall make the documents available in the time and manner designated by Covered Entity or the Secretary.
3.9 Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528.

3.10 Business Associate agrees to provide to Covered Entity or an Individual information collected in accordance with the section 3.9 of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528. Business Associate shall act in the time and manner designated by Covered Entity or the Individual.

3.11 Business Associate shall notify Covered Entity of any change(s) in Business Associate’s internal practices and procedures, to the extent that such changes may affect Business Associate’s use and disclosure of PHI and such changes shall be subject to the approval by Covered Entity.

3.12 Business Associate shall comply with the security policies and procedures adopted by the Covered Entity.

3.13 Business Associate shall comply with the additional requirements set forth in the HITECH Act.

IV. Permitted Uses and Disclosures by Business Associate

4.1 General Use and Disclosure Provisions. Except as otherwise limited in the Agreement, Business Associate may use or disclose PHI on behalf of, or to provide services to, Covered Entity for the following purposes, if such use or disclosure of PHI would not violate (1) the Privacy Rule if done by Covered Entity or (2) Covered Entity’s policies and procedures which limit disclosures to the minimum necessary:

Business Associate’s authorized activities are:

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

All other uses or disclosures of Covered Entity’s PHI are not authorized by this Agreement and shall be prohibited.

4.2 Specific Use and Disclosure Provisions

4.2.1 Except as otherwise limited in this Agreement, Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

4.2.2 Except as otherwise limited in this Agreement, Business Associate may disclose PHI for the proper management and administration of the Business Associate,
provided that disclosures are required by law or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

4.2.3 Except as otherwise limited in this Agreement, Business Associate may use PHI to provide data aggregation services to Covered Entity as permitted by 45 CFR § 164.504(e)(2)(i)(B).

4.2.4 Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR § 164.502(j)(i).

4.2.5 In the event Business Associate receives a subpoena, court order or other legal process which mandates the disclosure of PHI, Business Associate agrees to promptly notify and allow the Covered Entity to respond to such legal process.

4.3 Ownership of Protected Health Information. Business Associate acknowledges and agrees that any and all PHI which Covered Entity provides to Business Associate is owned by Covered Entity.

V. Obligations of Covered Entity

5.1 Covered Entity shall notify Business Associate of any limitation(s) in Covered Entity’s Notice of Privacy Practices in accordance with 45 CFR § 164.520, to the extent that such limitation may affect Business Associate’s use or disclosure of PHI.

5.2 Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect Business Associate’s use or disclosure of PHI.

5.3 Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI to which Covered Entity has agreed in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate’s use or disclosure of PHI.

5.4 Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule or HITECH Act if done by Covered Entity.

VI. Term and Termination

6.1 Term. The Term of this Agreement shall be effective as of the Effective Date identified below and shall terminate when the last of the Parties’ related agreements for Business Associate’s services terminate, or when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed.
or returned to Covered Entity or if it is not feasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provision in this section.

6.2 Termination for Cause. Upon Covered Entity’s knowledge of a material breach of the Agreement by Business Associate, Covered Entity shall either:

6.2.1 Provide an opportunity for Business Associate to cure the breach or end the violation and, if Business Associate fails to cure the breach or end the violation within the time specified by the Covered Entity, Covered Entity shall terminate this Agreement and all related agreements for Business Associate’s services involving the use or disclosure of PHI.

6.2.2 Immediately terminate this Agreement together with any related agreement for Business Associate’s services involving the use and disclosure of PHI if Business Associate has breached a material term of this Agreement, and if cure is not possible, Covered Entity shall be entitled to seek any and all available remedies to compensate it for any damages, losses, costs, and/or expenses it incurs.

6.2.3 If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary of the Department of Health and Human Services.

6.2.4 Business Associate acknowledges that remedies at law for the breach or violation of this Agreement by Business Associate may be inadequate and, therefore, Covered Entity shall also be entitled to injunctive relief, and to all costs and expenses, including reasonable attorney’s fees, relating to the pursuit of such injunctive relief. Such injunctive relief shall not be exclusive, but shall be in addition to any other rights and remedies that Covered Entity may have for such breach or violation.

6.3 Effect of Termination. Except as provided in subsection 6.3.1, upon termination of this Agreement for any reason, Business Associate shall return or destroy (at Business Associate’s election) all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI.

6.3.1 In the event that Business Associate determines that returning or destroying the PHI is not feasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon Covered Entity’s determination that return or destruction of PHI is not feasible, Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

VII. Insurance and Indemnification

7.1 Insurance. Business Associate shall provide Covered Entity with a Certificate of Insurance evidencing general liability insurance with limits of at least $1,000,000 per occurrence
and three million dollars ($3,000,000) aggregate to cover any and all claims, causes of action, and demands whatsoever made by Covered Entity for loss, damage, or injury to any person arising from the breach of the security, privacy, or confidentiality obligations under this Agreement by Business Associate, its agents or employees. Business Associate shall provide a certificate of insurance to Covered Entity prior to commencement of Business Associate activities.

7.2 Indemnification. In addition to any indemnification obligations undertaken by Business Associate under the Parties’ separate agreement for services, Business Associate shall indemnify, defend, and hold harmless Covered Entity from any and all claims, causes of action, and demands whatsoever made for loss, damage, or injury to any person to the extent caused by the breach by Business Associate, or its agents or employees, of the security, privacy or confidentiality obligations set forth under this Agreement.

VIII. Miscellaneous

8.1 Regulatory References. A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.

8.2 Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of Privacy Rule and HIPAA.

8.3 Survival. The respective rights and obligations of Business Associate under Section 6.3, “Effect of Termination,” of this Agreement shall survive the termination of the Agreement.

8.4 Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule and the HITECH Act.

8.5 Governing Law and Venue. The laws of the State of Idaho shall govern the validity, construction, interpretation, and effect of this Agreement, and any disputes pertaining hereto shall be adjudicated in the state courts of Idaho with venue being located in Bannock County, Idaho.

8.6 No Third-Party Beneficiary Rights. This is not a third-party beneficiary contract. This is an Agreement between Covered Entity and Business Associate, and it can only be enforced by Covered Entity and Business Associate. Covered Entity and Business Associate do not intend to create in any third-party a right to enforce this Agreement or to claim losses or damages under this Agreement.

8.7 Notices. Any notices to be given hereunder to a Party will be made by U.S. Mail or express courier to such Party’s address as below:

If to Covered Entity: General Counsel
If to Business Associate:

<table>
<thead>
<tr>
<th>Covered Entity:</th>
<th>Business Associate:</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDAHO STATE UNIVERSITY</td>
<td></td>
</tr>
<tr>
<td>By: ______________________________</td>
<td>By: ______________________________</td>
</tr>
<tr>
<td>Name: ______________________________</td>
<td>Name: ______________________________</td>
</tr>
<tr>
<td>Title: ______________________________</td>
<td>Title: ______________________________</td>
</tr>
<tr>
<td>Date: ______________________________</td>
<td>Date: ______________________________</td>
</tr>
</tbody>
</table>

IX. Effective Date

9.1 By their authorized signatures below, the Parties have executed this Agreement, which shall be effective as of the Effective Date.
IDAHO STATE UNIVERSITY
Kasiska Division of Health Sciences
Confidentiality Agreement

I understand that I am a workforce member of one of ISU’s health clinics (Clinic) and I will have access to patient information and will be required to follow specific regulations and policies to ensure the privacy and security of patient information. I am aware that patient information is subject to applicable federal and state regulations, as well as University and clinic policies regarding the use of patient information. I am aware that the use and disclosure of patient information is subject to federal law pursuant to the Health Insurance Portability and Accountability Act and I have received training regarding the applicable regulations. I am aware that failure to follow applicable federal and state regulations, and University and clinic policies regarding the use of patient information will subject me to sanctions, up to and including termination of employment or dismissal from a University program. I agree to the obligations below regarding the use of patient information.

A. I will use and disclose protected health information only in connection with and for the purpose of performing my assigned duties.

B. I will request, obtain or communicate protected health information only as necessary to perform my assigned duties and shall refrain from requesting, obtaining or communicating more protected health information than is necessary to accomplish my assigned duties.

C. I will take reasonable care to secure confidential health information on electronic devices including: clinic laptop, iPad, and will take steps to ensure that others cannot view or access such information. I will not download or store protected health information on any personal electronic device. I will not access any ISU electronic health record system on my personal electronic device without permission from the ISU HIPAA Committee. When I am away from my workstation and/or electronic device, or when my tasks are completed, I will log off my device in order to prevent access by unauthorized users.

D. I am prohibited from using portable storage devices such as floppy disks, jump or flash drives, CDs, DVDs, Zip drives unless specifically authorized by the HIPAA Privacy Officer. Employees and students may be authorized to use secure Box account for storing patient information.

E. I will only use a clinic authorized secure email account to send protected health information in electronic form.

F. I will not text patient information unless it has been authorized in written form by the HIPAA Security Officer.

G. I will not disclose my password to electronic medical record systems to another individual and will take reasonable measure to secure my password.
H. I will use and disclose protected health information solely in accordance with all state and federal laws and clinic procedures and policies set forth above or elsewhere. I also agree to familiarize myself with any periodic updates or changes to such procedures/policies in a timely manner.

I. I will immediately report any unauthorized use or disclosure of protected health information that I become aware of to the appropriate supervisor. I am aware that failure to report a breach of protected health information is a violation of clinic and University policy.

J. All patient data, email, and other data gathered or used while acting as a workforce member is the property of the University.

K. I will successfully complete ISU’s HIPAA Training for ISU Clinics on an annual basis.

I also understand and agree that my failure to fulfill any of the obligations set forth in this Agreement and/or my violation of any terms of this Agreement shall result in my being subject to appropriate disciplinary action.

__________________________________
Workforce Member Printed Name

__________________________________   _________________________________
Workforce Member Signature    Date
Consent for Alternative Communication

ISU understands that some forms of communication may not be suitable for everyone. In an effort to ensure that your communication needs are met, the following methods of communication are available. Please choose the method of communication that you would prefer for discussion of related healthcare issues:

Email

☐ Yes  ☐ No  Email: ________________________________________________________

Text

☐ Yes  ☐ No  Carrier: _____________________  Cell No. __________________________

Consent for Communication of Healthcare Information Through Alternative Means

The clinic cannot guarantee the confidentiality or integrity of unencrypted email or text messages and cannot be held liable for such breaches.

Risks of using email and text messaging:

• Due to the nature of the technology, unauthorized individuals may be able to intercept, read, and modify email and text messages used to correspond regarding your health treatment.
• Messages can be misaddressed, misdelivered, forwarded, or delivery can simply fail to occur.
• Service providers have the right to access and archive messages transmitted through their systems.
• Friends and family members may see and forward your messages if you do not restrict their access.

Best practices when using email and text messaging:

• Minimize the amount of sensitive data that is contained in the message
• Do not use for urgent or emergency communications.
• Maintain control of the personal accounts used for messaging.
• If you do not receive a response in a reasonable amount of time, call the clinic to confirm receipt.

☐ I acknowledge that I have read and fully understand the risks and best practices regarding the use of email and text messaging for communications with the clinic, and consent to the use of such email and text messaging for my healthcare needs.

_______________________________________________ ______________________________________
Patient/Client/Guardian Signature    Date
Disclosure of Protected Health Information Without Authorization

**Instructions:** Please complete this form for each disclosure of protected health information (PHI) to an outside person, entity or organization where the patient’s written authorization was **not** obtained. Do not complete this form if the PHI was released for continuing care or treatment, payment purposes, or health care operations.

<table>
<thead>
<tr>
<th>Patient Name:</th>
<th>Last Four Digits of Social Security Number:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medical Record Number:</td>
<td>Billing Number:</td>
</tr>
<tr>
<td>Date(s) of Disclosure:</td>
<td>Date(s) of Service/Visit Disclosed:</td>
</tr>
</tbody>
</table>

**Name of Person or Entity Receiving PHI:**
(Include address if known)

**If a Written Request was Received, attach the request and check box to the right.**

- [ ] A written request for disclosure of the PHI was received from someone other than the patient and is attached to this form.

**Brief Description of PHI Disclosed:** (Check one, or all that apply)

- [ ] Demographic Information; such as name, address, telephone number or other contact data
- [ ] Diagnosis or procedure information
- [ ] Lab test results, specify: __________________________
- [ ] Radiology results, specify: __________________________
- [ ] History or physical examination
- [ ] Discharge summary
- [ ] Consultation
- [ ] Entire medical record
- [ ] Emergency record of treatment
- [ ] Itemized bill or billing information
- [ ] Other, specify: __________________________
Brief Statement of Purpose of Disclosure:

- State or federal law required reporting (such as reporting births, deaths, communicable diseases, FDA, suspected abuse, crime victims and injuries)
- Organ donation or transplantation
- Medical examiner
- Funeral home
- Research
- Subpoena, court order, or other lawful process; see attached document
- Other, specify: ____________________________

Person Completing Form: ____________________________ Title: ____________________________

Telephone: ____________________________ Date: ____________________________

Please forward this completed form to the HIPAA Compliance Officer

For Internal Use Only
I. PROCEDURE STATEMENT

Idaho State University Kasiska Division of Health Sciences (KDHS) is committed to conducting business in accordance with the highest ethical and legal standards. This procedure establishes the process for granting and removing Electronic Health Records (EHR) access for workforce employees.

II. PROCEDURE

This procedure details the guidelines set forth to define those individuals by job function or title who require access to the patient EHR at KDHS clinics. Define those circumstances under which access will be permitted or limited and to define how the process of determining eligibility for access and for granting and removing access will be implemented.

III. ACCESS REQUIREMENTS

The HIPAA Privacy and Security team oversees the compliance and implementation of this procedure. The following sections detail how to obtain access and the individuals by job function or title who require access to the KDHS clinic’s EHR as well as the different categories of access.

III.1 Obtaining Access. Requests for access to the EHR or changes to current access must be requested by sending an email to help@isu.edu. Please include a list of new users including: name, ISU email, cell phone number (PNC users only), type of user as listed in Section III.2 and clinic name. This request should be submitted prior to the semester start date or new hire date to ensure timeliness in creating the accounts. PNC users will require a DUO account for dual authentication. The HIPAA Privacy Security Officer will approve access and notify one of the following EHR Administrators that access has been approved.

- ISU Health Center (Pointnclick) – Crystal Ross
- ISU Clinics (Pointnclick / WebPT) – Cindy Rock
- Dental Clinics (Dentrix Enterprise) – Julie VanLueven

Individuals who have been granted access approval to their clinic’s EHR, will be required to complete annual HIPAA Training for ISU Clinics through ISUs Moodle training platform or via paper for those without access to Moodle and sign a Confidentiality Agreement prior to gaining access to the EHR. Once complete, an individual login and password will be assigned to the new user.

III.2 Individuals by Job Function or Title

- **MD/PA/Nurses** providing student/faculty/staff services at the University Health Center will be granted appropriate access to their security division of the EHR in order to perform their respective functions.
- **Clinical Faculty** providing supervisory and/or individual patient services will be granted access to their security division of the EHR in order to perform their respective functions. Security divisions are set up based upon discipline and
clinic locations. Therefore, some providers may be granted access to additional security divisions when they provide services in multiple clinics.

- **Student Clinicians** who provide patient services at KDHS’s teaching clinics will be issued limited access to the EHR and will be assigned to their appropriate security division.

- **Workforce Staff Members** including IT, Clinics Director of Operations, Administrative, Technical Records Specialists, and Student CPIs who may perform a variety of duties such as: EHR management, front office and billing functions will be granted access based upon their job description or by specific activity to certain areas of the EHR. These members may belong to multiple security divisions subject to IT approval.

- **Faculty Researchers** who are performing research involving KDHS clinic’s EHR data and that research has been approved by ISU’s Office of Research may be issued limited access to the EHR, subject to approval.

- **Others** may request access and be granted on an as-needed basis.

### III.3 Roles and Permissions

Roles and permissions of the EHR may include:

- Full access to health data, including some or all information systems and security divisions.

- Limited access may include access:
  - to a specific security division and/or department;
  - for a specific time duration;
  - for specific patient records;
  - for specific types of records (e.g., by security access level).

- Functional limitations of access such as view only, write access, and print access.

Roles for each EHR are defined in EHR Roles and Permissions.

### IV. TERMINATION OF ACCESS

All access to the clinic’s EHR will be terminated if an individual:

- is no longer a student, faculty, staff member, or CPI; or
- completes the approved research project for which access was approved; or
- no longer requires access for the performance of their job; or
- violates the Confidentiality Agreement.

Students working in the clinics will automatically be deactivated at the end of their clinical experience, usually the end of the year. When faculty and staff leave the clinic and no longer need access, it is the responsibility of the Clinic Director to submit a request for their access to be deactivated by sending an email to help@isu.edu.
Electronic Health Record Roles and Permissions

Point and Click:

- Administrator, Clinical
- Administrator, PNC
- Administrator, Reg/Scheduling/Billing
- Administrator, System
- Athletic Trainer
- Audiologist, Director (sub-role)
- Audiologist, Faculty
- Audit Logs (sub-role)
- Billing
- Business Manager
- Cashier
- Contract Tracer/Pandemic Management/Clearances
- Enterprise Reports
- Health Educator
- Laboratory Manager
- Laboratory Technician
- Mass Tester
- Mass Tester Reports
- Mass Tester with Registration
- Medical Assistant/Non-Registered Nurse
- Medical Clinician
- Medical Records
- Medical Records – Student Assistant
- Medical Records Manager
- Non-Clinician Dispense Meds (sub-role)
- Nutrition AID-IC Study Manager
- Nutrition AID-IC Study Provider
- Nutritionist
- Physical Therapist, Faculty
- Physical Therapy, Director (sub-role)
- Physical Therapy, Student
- Radiology Technician
- Registered Nurse
- Schedule Edit Template (sub-role)
- Scheduler
- Scheduler Encounter Note (sub-role)
- SHS Student Level 1 – Read Only
- SHS Student Level 2 – Data Entry/Orders
• Speech-Hearing Clinician
• Transcriptionist

Dentrix
• Admin
• General user/Timeclock Admin
• General user
• Hygiene
• Resident
• Front Office

Eagle Soft
• Admin
• Office Manager
• Clinic Director
• Clinical Faculty
• Dental Hygiene Student
• CPI student

WebPT
• **View Patients**: Provides view-only access to the Patient Manager on the navigation panel.
• **Edit Patients**: Provides edit access to the Add Patient and Quick Add Patient in the patient manager on the navigation panel.
• **View Users**: Provides access to the User Manager link under the clinic name. The User Manager page allows users to request license adjustments and add additional users.
• **Edit Users**: Allows edit permissions for all other user profiles in the clinic as well as change the status (e.g., Active or Inactive) for other users.
• **Start SOAP Notes**: Allows users to add documentation to a patient’s chart.
• **Forward SOAP Notes**: Allows users to forward notes to other users for co-signature.
• **Finish SOAP Notes**: Allows users to finalize patient documentation. The user manager must complete an attestation if enabling this permission for an assistant user type.
• **Calendar Admin**: Provides access to Calendar Settings and User Permissions tab and Clinic Settings tab in Scheduler.
• **Clinic Admin**: Provides access to Clinic Settings, Patient Intake Admin, Medicare Fee Schedule, Reminder Usage, Reminder Setup, and Referral Report. This permission also allows users to remove location access from patients.
• **Company Admin**: Provides access to WebPT Outcomes Report, Company Fee Schedule, and Company Settings. Company Admins do not see Clinic Settings, Patient Intake Admin, or Medicare Fee Schedule.
• **Edit/Delete Patient Transactions**: Allows users to edit/delete Patient Payments.
• **Insurance Admin**: Provides edit access to the Insurance Manager. This will prevent any accidental changes to insurance settings.

• **Billing Report Admin**: Provides access to the Billing Report. This will ensure that only permissioned users can review patient billing details.

• **Analytics Access**: Provides access to the Analytics feature. Only those with this permission will see the Analytics icon in the header menu.
I. INTRODUCTION

Idaho State University (ISU) is a state institution of higher education providing both general education and specialized programs. ISU is a single legal entity comprised of separate departments and clinics, some of which provide Covered Functions as Health Care Components of ISU, as these terms are defined below.

II. POLICY STATEMENT

To define ISU as one legal entity, specifically a Hybrid Entity, and identify ISU’s Health Care Components, in accordance with the privacy and security regulations (the “Privacy and Security Standards”) promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and the Health Information Technology for Economic and Clinical Health Act of 2009 (the “HITECH Act”). This policy specifically addresses the requirements of 45 C.F.R. §§ 164.103 and 164.105.

III. AUTHORITY AND RESPONSIBILITIES

A. A legal entity that performs both Covered Functions and non-covered functions may designate itself as a Hybrid Entity under HIPAA. A Hybrid Entity may exclude from its covered entity status the following non-covered functions: (1) non-health care components of the organization (e.g., the university’s academic programs), and/or (2) Health Care Components of the facility that do not engage in electronic transactions (e.g., a clinic that provides health care services but does not bill for its services). All covered Health Care Components of the designating legal entity must comply with HIPAA.

B. A Hybrid Entity must designate as part of its Covered Functions any component that would meet the definition of a covered entity if it were a separate legal entity. For example, a health clinic that performs Covered Functions and that conducts covered transactions electronically (e.g., electronic claim submission) must be designated as a Health Care Component of the facility, and will be subject to the Privacy and Security Standards.
C. ISU has designated itself a Hybrid Entity in accordance with 45 C.F.R. §§ 164.103 and 164.105.

IV. DEFINITIONS

A. Covered Functions – Those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

B. Hybrid Entity – A single legal entity:
   1. That is a covered entity;
   2. Whose business activities include both covered and non-covered functions; and
   3. That designates its Health Care Components, documents the designation and establishes appropriate firewalls in accordance with HIPAA between covered and non-covered functions.

C. Health Care Component – A component or combination of components of a Hybrid Entity designated by the Hybrid Entity in accordance with 45 C.F.R. 164.105(a)(2)(iii)(C).

V. PROCEDURES TO IMPLEMENT

A. Procedures:

   1. ISU has determined that it performs both Covered Functions (e.g., outpatient services, including medical and dental care) and non-covered functions (e.g., academic departments conducting teaching activities), and has designated itself as a Hybrid Entity.

      a. Attachment A lists the ISU Health Care Components, including business associate-like division(s) that are designated as part of the Health Care Component.

      b. Attachment A designating ISU’s Health Care Components shall be retained for at least six (6) years following any decision to terminate any division or department from the Health Care Components. Designations should be retained indefinitely for on-going Health Care Components.

   2. Hybrid Entity safeguard requirements: As a covered entity that is a Hybrid Entity, ISU must ensure that a Health Care Component of the entity complies with the applicable requirements of HIPAA. Firewalls must be implemented between health care functions and non-health care functions. ISU shall operationally segregate all non-covered functions from the Covered Functions. In particular, ISU will ensure that:

      a. Each Health Care Component does not disclose protected health information (“PHI”) to another non-health care component of the covered entity in circumstances in which HIPAA would prohibit such disclosure if the Health Care Component and the non-health care component were separate and distinct legal entities; this includes the separation of academic and research functions from Health Care Component functions, even is performed by the same person.
b. Business associate-like departments or divisions designated as part of the Health Care Component:
   
i. Do not use or disclose PHI that it creates or receives from or on behalf of the Health Care Component in a way that is prohibited by HIPAA’s Privacy and Security Standards; and
   
ii. Comply with the HIPAA Privacy and Security Standards.

c. Where possible, staff and office space should be segregated between covered and non-covered functions.

d. ISU recognizes that healthcare functions performed within a covered Health Care Component must be separated from academic or other functions of ISU performed by personnel. If a person performs duties for both the Health Care Component in the capacity of a member of the workforce and also performs work for another component of the entity in the same capacity with respect to that component, such workforce member must not use or disclose PHI created or received in the course of or incident to the member's work for the Health Care Component in a way prohibited HIPAA regulations.

3. ISU has established a HIPAA Privacy Officer. The HIPAA Privacy Officer is authorized to develop and implement procedures for all covered entities at ISU and for those ISU departments that provide Covered Functions. The HIPAA Privacy Officer is also responsible for receiving and responding to complaints related to PHI; ensuring workforce members are trained appropriately; auditing workforce compliance with all policies and procedures; implementing sanctions against students, employees, or volunteers; and for maintaining overall compliance with HIPAA regulations throughout all Health Care Components and those departments that perform Covered Functions.

4. ISU has established a HIPAA Security Officer. The HIPAA Security Officer is responsible for the implementations of policies and procedures to ensure compliance with the HITECH Act throughout all healthcare.

5. ISU will maintain a HIPAA Advisory Committee (HAC) that is responsible for approving all procedures as relates to the creation, storage and transmission of ePHI or PHI within any ISU covered entity, or ISU department that performs any Covered Function. The HAC will include but is not limited to the following: the HIPAA Privacy Officer, the HIPAA Security Officer, the ISU Chief Information Officer, a director of clinical operations, and the manager of ISU networking. The HAC will meet at least monthly.

VI. ATTACHMENTS
Attachment A – ISU Health Care Component Designation
Attachment A

ISU Health Care Component Designation

The following business associate-like department(s) are considered part of the Health Care Components of ISU:

- ISU Information Technology Services personnel assigned to the ISU Health Care Components
- Office of General Counsel insofar as they perform services for the ISU Health Care Components
- ISU business or financial departments insofar as they perform services on behalf of ISU Health Care Components

The following clinics, departments and programs are considered Health Care Components of ISU:

- Audiology Clinic
- ISU Athletic Training Department
- Dental Hygiene Clinic (Pocatello and Idaho Falls)
- Dentistry Clinics (Pocatello and Meridian)
- Physical and Occupational Therapy Clinic (Pocatello)
- Speech, Language and Hearing Clinics (Pocatello and Meridian)
- University Health Center
INFORMATION SECURITY INCIDENT RESPONSE REPORT

Date of Incident (or approximate if unknown): ____________________________

Date the Incident Became Known: ____________________________

Date Reported to HIPAA Compliance Officer and/or IT Security: ____________________________

Describe the Incident:

Location, Type, and Scope of Data Exposed:

Has anyone else been contacted? If yes, who and when?

Contact Information of Individual Reporting the Incident:

Name: ____________________________  Title: ____________________________

Department: ____________________________  Phone: ____________________________

Email: ____________________________

Incident Team Members:
<table>
<thead>
<tr>
<th>Date Complete</th>
<th>Task</th>
<th>Responsible Party</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Preliminary assessment of type and scope of data potentially exposed</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Consult with HIPAA Compliance Officer, CIO, Marcom, General Counsel regarding communication strategy (if necessary)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Obtain, preserve, and analyze forensic evidence</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Final assessment of type and scope of data exposed and the availability and type of contact data for affected individuals</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Issue press release (if necessary)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Notify affected individuals: compile list, draft letter, prepare and mail letters</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Create notice for website</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Prepare telephone support for affected individual calls: identify appropriate person to receive calls, identify telephone number to use, write talking points</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Prepare email support for affected individual emails: identify appropriate person to receive email, identify/set up email address to use, write talking points</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contact outside agencies if required by law: OCR, credit reporting agencies, banks, etc.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Schedule debriefing meeting: why did this happen, could more have been done to avoid the incident, were any procedures violated, what could have been done better, how can similar incidents be avoided in the future, what other issues did this incident bring to light</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Document remediation steps</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Implement remediation steps</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IDAHO STATE UNIVERSITY
POLICIES AND PROCEDURES (ISUPP)
Information Technology Services
Compliance and Sanctions
ISUPP 2460

I. INTRODUCTION
The greatest threat to privacy and security rests within an organization's workforce. In an attempt to hold organizations accountable, federal and state laws have mandated breach prevention and penalties, which are becoming more stringent. It is the objective of Idaho State University (ISU or University) to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements. The University must be prepared to respond fairly and appropriately (1) to violations of law, regulation, or University policy relating to information security, (2) when questionable or unacceptable computing practices occur, or (3) where there is non-compliance with information security policy requirements or with reasonable requests for action or cooperation necessary to implement the University's information security policies.

II. POLICY STATEMENT
ISU requires that faculty, staff, students, volunteers, and contractors comply with all applicable laws, regulations, statutes and University policies relating to information security and information technology. Lack of compliance will result in sanctions or other appropriate action which are consistent and relevant not only to the incident but to the potential for harm.

III. AUTHORITY AND RESPONSIBILITIES
All members of the ISU community, including faculty, staff, volunteers, contractors, and visitors are responsible for protecting Information and the IT System.

The Information Technology Services department is charged with auditing the use of ISU IT systems by all faculty, staff, students, volunteers, contractors, and visitors to ensure the security of all ISU information through compliance with University policies.

IV. DEFINITIONS
A. Chief Information Officer - The ISU executive in charge of Information Technology Services.
B. Critical Information - Information identified by applicable laws, regulations or policies as personal information, individually identifiable health information, education records, personally identifiable information, non-public personal or institutional data, confidential personal information, or sensitive scientific or sponsored project information.
C. Information - A data set that is considered valuable to an organization. Information is classified in the Information Technology Services Asset Management ISUPP 2430.
D. Information Network - A telecommunications network that allows Information Systems to electronically exchange data.
E. Information Owner – The ISU employee or department responsible for
accuracy, integrity, and timeliness of a defined subset of ISU’s Information, and authorized to grant or deny access to that Information.

F. Information Security Manager - The ISU employee that is responsible for leading information security activities at ISU.

G. Information System - A computing device that stores, processes, or transmits ISU Information.

H. Information System Administrator - The ISU employee that is responsible for the protection and proper use of a specific Information System as assigned by an Information Owner.

I. IT System – ISU’s data processing hardware, software, data transmission equipment and infrastructure, data storage devices, and the digital information stored, processed, or transmitted via these components.

J. Workforce or Workforce Member – Faculty, staff, contractors, and volunteers at ISU. Excludes students, unless they are performing a specific work function similar to faculty or staff.

V. PROCEDURES TO IMPLEMENT

A. Compliance with Legal Requirements.

All Information Systems containing Critical Information will be compliant with applicable government laws and industry regulations and ISU policies and Procedures.

B. Compliance with Security Policies, Standards and Technical Compliance

1. Managers of all administrative and academic units will ensure compliance with ISU Information Security Policies within their areas of responsibility by performing regular review of compliance and promoting awareness amongst faculty, staff, and student employees.

2. The Information Security Manager will periodically review compliance with ISU information security policies across all organizations within ISU through onsite interviews, inspections, and audits.

3. All Workforce Members are required to report any actual or suspected violation of the ISU information security policies. The report is to be made to the Information Security Manager via an email sent to security@isu.edu.

4. Violations of ISU information security policies will be recorded, monitored, and updated (as remediation occurs) by the Information Security Manager.

C. Sanctions

1. Sanctions for privacy and information security-related violations shall be applied consistently irrespective of the status of the violator, with comparable discipline imposed for comparable violations.
1. **Sanctions Standard:**

1.1. The Chief Information Officer shall be responsible for determining whether a violation has occurred. Human Resources (for faculty or staff) or Student Affairs (for students) will be responsible, in consultation with the Chief Information Officer and the Chief Compliance Officer, to determine what sanctions should be imposed.

1.2. ISU defines categories that establish the significance and impact of the privacy or security incident to help guide corrective action and remediation.

- **Category 1:** Unintentional breach of security that may be caused by carelessness, lack of knowledge, or lack of judgment, such as an error that causes a billing statement to be mailed to the wrong individual or organization.

- **Category 2:** Deliberate unauthorized access to confidential or sensitive information without disclosure. Examples: snoopers accessing confidential information without legitimate business reason, password sharing, or other failure to follow policy without legitimate reason.

- **Category 3:** Deliberate unauthorized disclosure of or tampering with confidential or sensitive information without malice or personal gain. Examples: sharing unauthorized confidential or sensitive information with the news media, unauthorized modification of an electronic document to expedite a process.

- **Category 4:** Deliberate unauthorized disclosure of or tampering with confidential or sensitive information for malice or personal gain. Examples: identity theft, or selling of confidential or sensitive information.

1.3. Factors that may modify application of sanctions:

1.3.1. Sanctions may be modified based on mitigating factors.

- Multiple offenses

1.3.2. Factors that could mitigate sanctioning could include:

- Offender voluntarily admitted the breach and cooperated with the investigation,
- Offender was inadequately trained or not aware of policy.

1.3.3. Possible Sanctions could range from a verbal warning to suspension and/or dismissal.
Limited Data Set Request

REQUESTOR/RECIPIENT INFORMATION

A. I/we are the requestor(s) and recipient(s) of the Limited Data Set identified in this document and agree to provisions of the Data Use Agreement (If necessary, use a separate page to identify all names of individuals or organizations requesting or receiving the Limited Data Set information, and attach to this document):

1. Name: ________________________________
   Title: ________________________________
   Organization: __________________________
   Address: ________________________________
   Telephone: __________________ Fax: __________________
   E-mail: ________________________________
   Signature: ____________________________ Date: __________

2. Name: ________________________________
   Title: ________________________________
   Organization: __________________________
   Address: ________________________________
   Telephone: __________________ Fax: __________________
   E-mail: ________________________________
   Signature: ____________________________ Date: __________
Review decision. Check one:
1. __ Request Denied
2. __ Request Approved
3. __ Request Approved with the following modification:

   ______________________________________________________________________
   ______________________________________________________________________

Fees Due, if applicable:

1. Amount Due: $__________________________

2. Date Fees Collected: ______________________________

Signature: ___________________________ Date: ________________

Title: _________________________________

Department: __________________________
# USES of Minimum Necessary Protected Health Information Worksheet

<table>
<thead>
<tr>
<th>Department</th>
<th>Job Title</th>
<th>Work Duties and Responsibilities</th>
<th>Form of Access</th>
<th>Conditions on Use of PHI (if applicable)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1.</td>
<td>1.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Minimum Necessary PHI and Frequency of Access</th>
<th>Conditions on Use of PHI (if applicable)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>1.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Approved/Revised</th>
<th>Name/Title/Department</th>
<th>Date</th>
<th>Privacy Task Force Member</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Routine **DISCLOSURES** of Minimum Necessary Protected Health Information Worksheet

<table>
<thead>
<tr>
<th>Type or Description of Routine Disclosure</th>
<th>Purpose of Disclosure</th>
<th>Frequency of Disclosure</th>
<th>Departments or Parties Involved in the Routine Disclosure</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>who may disclose the PHI</th>
<th>Who May Receive the PHI</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>1.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Criteria or Protocol for Minimum Necessary</th>
<th>Data Types or Records Disclosed</th>
<th>Method of Disclosure</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Approved/Revised By Name</th>
<th>Approved/Revised By Title</th>
<th>Date</th>
</tr>
</thead>
</table>

...
Notice of Privacy Practices

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY, SIGN THE ACKNOWLEDGEMENT OF RECEIPT, AND GIVE TO THE RECEPTIONIST.

Protecting Your Personal and Health Information

Our clinic is committed to protecting the privacy of its patients’ personal and health information. Applicable Federal and State laws require us to maintain the privacy of our patients’ personal and health information. This Notice explains our clinic’s privacy practices, our legal duties, and your rights concerning your personal and health information. In this Notice, your personal and health information is referred to as “health information” and includes your name, age, address, income or other financial information. We follow the privacy practices described in this Notice while it is in effect. This Notice takes effect April 14, 2003 and will remain in effect until replaced.

How We Protect Your Health Information

We protect your health information by:

- Treating all of your health information that we collect as confidential.
- Stating confidentiality policies and practices in our medical and clinical staff handbooks as well as disciplinary measure for privacy violations.
- Restricting access to your health information only to those medical and clinical staff who need to know your health information in order to provide our services to you.
- Only disclosing your health information that is necessary for an outside service company to perform its function on our behalf, and the company has by contract agreed to protect and maintain the confidentiality of your health information.
- Maintaining physical, electronic, and procedural safeguards to comply with federal and state regulations guarding your health information.

Uses and Disclosures of Your Health Information

We will use and disclose health information about you for treatment, payment and health care operations. For example:

- **Treatment**: We may provide another physician or subsequent healthcare provider who is treating you with copies of various reports of your health information that should assist him or her with your treatment.
- **Payment**: We may use and disclose your health information to obtain payment for services we provide to you.
- **Healthcare Operations**: We may use and disclose your health information in connection with our healthcare operations. Healthcare operations include quality assessment and improvement activities, reviewing the competence or qualifications of healthcare professionals, evaluating practitioner and provider performance, conducting training and educational programs, accreditation, certification, licensing, or credentialing activities.
- **Your Authorization**: In addition to our use of your health information for treatment, payment, or healthcare operations, you may give us written authorization to use your health information or to disclose it to anyone for any purpose. If you give us an authorization, you may revoke it in writing at any time. Your revocation will not affect any use or disclosures permitted by your authorization while it was in effect. Unless you give us a written authorization, we cannot use or disclose your health information for any reason except those described in this Notice.
• To Your Family and Friends: We must disclose your health to you, as described in the Patient Rights section of this Notice. We may disclose your health information to a family member, friend, or other person to the extent necessary to help with your healthcare or with payment for your healthcare, but only if you agree that we may do so.

• Persons Involved in Care: We may use or disclose health information to notify, or assist in the notification of (including identifying or locating) a family member, your personal condition, or death. If you are present, then prior to use or disclosure of your health information, we will provide you with an opportunity to object to such uses or disclosures. In the event of your incapacity or emergency circumstances, we will disclose health information based on a determination using our professional judgment disclosing only health information that is directly relevant to the person’s involvement in your healthcare. We will also use our professional judgment and our experience with common practice to make reasonable inferences of your best interest in allowing a person to pick up filled prescriptions, medical supplies, x-rays, or other similar forms of health information.

• Marketing Health-Related Services: We will not use your health information for marketing without a written authorization from you.

• Required by Law: We may use or disclose your health information when we are required to do so by law, including, but not limited to, court or administrative orders, subpoenas, discovery requests, or other lawful process.

• Abuse or Neglect: We may disclose your health information to the extent necessary to avert a serious threat to your health or safety or the health or safety of others.

• National Security: We may disclose to military authorities the health information of Armed forces personnel under certain circumstances. We may disclose to authorize federal officials health information required for lawful intelligence, counterintelligence, and other national security activities. We may disclose health information to a correctional institution or law enforcement official having lawful custody of protected health information of an inmate or patient under certain circumstances.

• Appointment Reminders: We may also use health information about you to call, leave a voice message, text, email, or send a postcard or letter to you as a reminder about an appointment.

• Research: Under certain limited circumstances, we may use and disclose health information about you for research purposes. All research projects, however, are subject to a special approval process.

Rights You Have Regarding the Use and Disclosure of Your Health Information

You have the right to request all of the following:

• Access to Your Health Information: You have the right to request a copy of your health information. A nominal fee may be charged for providing copies. However, this right does not include the following types of records: psychotherapy notes; records compiled in reasonable anticipation of a court action or administrative action or proceeding; and protected health information whose release is prohibited by federal or state laws. Access to your records may also be limited if it is determined that by providing the information it could possibly be harmful to you or another person. If access is limited for this reason, you have a right to request a review of that decision.

• Amendment: You have the right to request in writing an amendment to your health information. The request must identify which information is incorrect and an explanation of why you think it should be amended. If the request is denied, a written explanation stating why will be provided to you. You may also make a statement disagreeing with the denial which will be added to the information of the original request. If your original request is approved, we will make reasonable effort to include the amended information in future disclosures. (Amending a record does not mean that any portion of your health information will be deleted.

• Accounting or Disclosures: If your health information is disclosed for any reason other than treatment, payment, or operation, you have the right to an accounting for each disclosure of the previous six (6) years. The accounting will include the date, name of person or entity, description of the information disclosed, the reason for disclosure, and other applicable information. If more than one (1) accounting is requested in a twelve (12) month period, a reasonable fee may be charged.
• **Restriction Requests:** You have the right to request that the clinic place additional restrictions on uses and disclosures of your health information. We may not be able to accept your request, but if we do, we will uphold the restriction unless it is an emergency.

• **Confidential Communication:** You have the right to request that communication regarding your health information be done in an alternate way or be sent to an alternate location.

• **Electronic Notice:** If you received this notice by accessing a web site or by email, you are also entitled to have a paper copy which is available by request from the clinic or department.

**Changes to this Notice**

We reserve the right to change our privacy practices and terms of this Notice at any time, as permitted by applicable law. We reserve the right to make changes in our privacy practices and the new terms of our Notice effective for all health information that we maintain, including health information we created or received before we made the changes. Before we make such changes, we will update this Notice and post the changes in the waiting room or lobby of the facility. You may also request a copy of the Notice at any time.

**Questions and Complaints**

For questions regarding this notice or our privacy practices, please contact our office.

If you are concerned that your privacy rights may have been violated, you may contact either of the people listed below to make a complaint. You may also make a written complaint to the U.S. Department of Health and Human Services whose address can be provided upon request.

If you choose to make a complaint with us or the U.S. Department of Health and Human Services, we will not retaliate in any way.

**ISU Clinic Operations:**

Cindy Rock, Clinics Director of Operations
1311 E. Central Dr.
Meridian, ID  83642
(208) 373-1743
rockcind@isu.edu

**ISU HIPAA Compliance Officer:**

HIPAA Compliance Officer
921 S. 8th Ave, Stop 8055
Pocatello, ID  83209
(208) 282-4899
HIPAA@health.isu.edu
Request for Amendment of Health Information

Patient Name: ____________________________

Patient Account No.: ___________________ Medical Record No.: ____________________

Patient Address: _________________________

Date of entry to be amended: __________ Type of entry to be amended: ________________

Please explain how the entry is incorrect or incomplete. What should the entry say to be more accurate or complete?

________________________________________________________________________________

________________________________________________________________________________

I authorize the release of the amended information described on the form to the following parties (additional parties can be listed on the back of this form):

Name

Address

City

State

Zip

Signature of Patient or Personal Representative ____________________________ Date __________

For Healthcare Organization Use Only:

Date Received: ______________ Amendment is ___ Accepted ___ Denied

If denied, check reason for denial:

___ PHI was not created by this organization ___ PHI is not a part of patient’s designated record set

___ PHI is not available to the patient for inspection as required by federal law (e.g. psychotherapy notes) ___ PHI is accurate and complete
Comments of Healthcare Practitioner (Clinician-author):

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

Name of Healthcare Practitioner  Title

Signature of Healthcare Practitioner  Date

Copies to: Medical/Billing Record of Patient
            Author
            Requestor
Letter for Delay in Processing Request for Amendment of Health Records

Date

Patient or Representative
Address
City, State, ZIP Code

Dear (Patient Name):

Your request for an amendment of your health records, dated ________________, is still under consideration. ISU is experiencing a delay in responding to your request because:

__________________________________________________________

and ISU will act upon your request within the next thirty (30) days.

ISU will notify you of its decision by _____________________________(date).

Sincerely,

ISU HIPAA Compliance Officer (or his/her designee)

cc: Medical or Billing Record of Patient
Letter of Denial for Request to Amend Health Records

Date

Patient or Representative
Address
City, State, ZIP Code

Dear {Patient Name}:

This is to inform you that your request to amend information in your medical or billing records has been denied because the:

___ Information was not created by ISU. Please contact the person or entity that created this information. (1)
___ Information may be amended only by the clinician or author of the record, and such clinician or author has not approved the amendment.
___ Information is not part of the medical information kept by or for ISU.
___ Information is not part of the medical information you would be permitted to inspect and copy.
___ Information is accurate and complete.

If you disagree with ISU’s conclusion, you may file a statement of disagreement. Submit your written statement to {name, title, phone number of contact person or office responsible for handling amendments of medical or billing records.}

If ISU does not agree with your statement of disagreement, ISU will provide you with a copy of our rebuttal.

If you do not wish to submit a written statement of disagreement, you may still request that ISU provide your request for amendment and our denial with any further disclosures of the related protected health information. Submit your written request to {name, title, phone number of contact person or office responsible for handling amendments of medical or billing records.}

Should you wish to file a complaint regarding this issue, you may submit your complaint in writing to the HIPAA Compliance Officer at {ISU, phone number}. You may also file a complaint with the Secretary of the Department of Health and Human Services {name, address, phone number}.

Signature of ISU Representative

(1) If you can provide a reasonable basis for ISU to believe the originator of your protected health information is no longer available to act on your request, ISU will reconsider this decision and may proceed with the amendment. If you believe this to be the case, please contact the person named above at {phone, address}.

Original to Requestor Copy to Patient’s Medical Record or Billing Record
Request for Confidential Communication of Protected Health Information

I, ________________________________, request communication of my protected health information (PHI) from ISU by alternative means or at alternative locations. I understand this request applies only to communications from ISU to the patient, and communications that would be sent to the named insured of an insurance policy that covers the patient as a dependent of the named insured.

Please indicate the methods and/or locations by or at which we may contact you.

<table>
<thead>
<tr>
<th>Telephone Number</th>
<th>Mail Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Other __________________________________________________________

Describe _________________________________________________________

_______________________________________________________________

NOTE: This request will remain in effect until you notify us of a change.

Signature ___________________________ Date ______________

Printed Name ____________________________________________

Relationship if Not Patient __________________________________

Patient’s Date of Birth _______________ Last four digits of patient’s SS# ________________

Original: Medical Record

Copy: Billing Record
Request for De-identified Information

Idaho State University ("ISU") requires a written request for de-identified information that provides a detailed explanation of why the information is required and how it will be used by the requestor. It is within the discretion of ISU to approve or deny requests for de-identified information. Please complete the following to assist us in the review process. Submit this completed form to the HIPAA Compliance Officer or his/her designee at [Mailing Address].

Requestor Name________________________ Title __________________________

Department/Organization __________________________

Address __________________________

Street City State Zip Code

Business Phone: (_____) __________________ E-mail __________________

Date Information is Needed __________________

A. Purpose of the Request:

________________________________________________________________________

B. Will the de-identified information be used or accessed by someone other than the requestor?

[ ] YES [ ] NO

If YES, list by name (or title) the individual(s) who will use or have access to this information:

<table>
<thead>
<tr>
<th>Name/Title</th>
<th>Organization</th>
<th>Phone Number (extension)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

C. Describe the parameters or selection criteria needed to process this request for de-identified information (e.g., diagnosis, procedure, drug use).

<table>
<thead>
<tr>
<th>Time Period</th>
<th>Minimum number of records</th>
<th>Selection Criteria</th>
<th>Type of patient record</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

D. Describe or attach the requested format (and record layout parameters) of the information (i.e., hard copy, electronic, etc.)

________________________________________________________________________

________________________________________________________________________
E. List any planned publications that will result from use of the information provided:


F. Will you ever need to determine the identity of any of the individuals included in the de-identified data set?
   [ ] YES   [ ] NO   If Yes, please explain how often and why – be specific:


YOUR SIGNATURE BELOW INDICATES YOU HAVE READ AND AGREE TO ABIDE BY THE FOLLOWING REQUIREMENTS FOR USE AND DISCLOSURE OF THE DE-IDENTIFIED HEALTH INFORMATION YOU ARE REQUESTING.

1. The recipient(s) will not give, sell, loan, show or disseminate the de-identified information to any parties other than those listed in item B above, without the express written permission of ISU.
2. The recipient(s) will not link the ISU de-identified data to any other data that the recipient may have access to, where the linked data identifies the individual patients. For example, linking de-identified data from ISU with publicly available census data and the linkage reveals the identity of individual patients.
3. If the recipient accidentally identifies an individual, the recipient will not retain such identification and will not contact any patient, or their relatives, employers, or other household members.

Requestor Signature: __________________________ Date of Request: _________________

Printed Name: ________________________________
FACILITY USE ONLY:  [ ] APPROVED  [ ] DENIED

If denied, reason: ____________________________________________________________
__________________________________________________________________________
__________________________________________________________________________

If approved:

The requestor of the de-identified data agrees to pay the established fees: [ ] YES [ ] NO

Appropriate fees have been collected: [ ] YES  Amount Paid: $__________________________

De-identification Method to be Used: [ ] Statistical Model  [ ] Removal of Direct Identifiers

Department/Organization to Perform the De-identification: ________________________________

Date PHI was De-identified and Delivered to Requestor: ________________________________

Request Approved by:

Signature: ___________________________________________ Date: _________________________

Printed Name/Title: ______________________________________________________________

Department: _____________________________________________________________________
Request to Restrict the Use and Disclosure of Protected Health Information

I request that ISU restrict the use and disclosure of the following protected health information (PHI). I understand that ISU may not agree to this request; provided, however, that ISU may be required by law to grant a restriction preventing disclosure to my health plan concerning services or items for which I have paid ISU out of pocket.

Describe the restriction requested: __________________________________________________________

This restriction shall be in effect until (date or event): _______________________________________

Patient Name, printed: _________________________________________________________________

Signature: ___________________________ Date: __________________________

Relationship if not patient: ______________________________________________________________

Mailing Address for future correspondence regarding this restriction: __________________________

ISU Response to Patient Request for Restrictions of Use and Disclosure of Protected Health Information

ISU has reviewed the above request to restrict the use and disclosure of protected health information (PHI) and (check one)

___ Denies the request as ISU cannot reasonably assure or guarantee the restriction can be met.

___ Accepts and will honor the request for the above stated restriction. If you need emergency treatment and the restricted PHI is needed to provide emergency treatment, ISU may use the restricted PHI or may disclose this information to another healthcare provider to provide you with the emergency treatment. ISU will ask the health care provider to not further use or disclose the PHI. In the future, to the extent permitted by law, ISU may need to terminate or revoke its acceptance of this restriction. ISU will notify you of such unilateral termination.

Signed: ___________________________ Date: __________________________

Title: ________________________________________________________________
Revocation or Termination of the Restrictions of Use and Disclosure of
Protected Health Information

Check One:

__ Patient:  
I hereby **revoke** the restriction of the use and disclosure of my protected health
information (PHI) effective______________________(date).

__ ISU:
ISU previously agreed to the restriction of the use and disclosure of your protected health
information (PHI). To the extent permitted by law, ISU **terminates this previous
agreement** and shall no longer restrict the use and disclosure of your protected health
information effective______________________(date).

Signed:_________________________________________  Date:__________________

Printed Name: __________________________________________________________

Relationship if not patient: ________________________________________________

Or

ISU HIPAA Compliance Officer: ___________________________________________

File copies in medical record and or billing record.
RISK ASSESSMENT FORM

WHEN TO USE THIS FORM: This form should be used to identify any physical and security risks regarding confidential information, PHI, ePHI, (“Information”) and other vulnerabilities that may exist at the clinic.

Clinic Name: ___________________________ Date: __________________

Inspection Performed By: ___________________________

FACILITY ACCESS CONTROLS

1. Does the clinic utilize procedures to limit physical access to the areas that contain Information?
   __ Yes  __ No  __Don’t Know  This is managed by: ___________________________

2. Are the procedures practiced consistently in the clinic?
   __ Yes  __ No  __Don’t Know

3. Does the clinic utilize procedures that define the steps to be taken in the event that access to Information is not available through normal channels?
   __ Yes  __ No  __Don’t Know  This is managed by: ___________________________

4. If yes, have these procedures been tested and the results documented?
   __ Yes  __ No  __Don’t Know

5. Does the clinic use procedures to safeguard the premises and equipment from unauthorized physical access, tampering, and theft?
   __ Yes  __ No  __Don’t Know  This is managed by: ___________________________

6. If yes, are the procedures practiced consistently in the clinic?
   __ Yes  __ No  __Don’t Know

7. Does the clinic use procedures to validate and control a person’s access to Information based on the person’s role or function?
   __ Yes  __ No  __Don’t Know  This is managed by: ___________________________

8. Does the clinic use procedures for visitor control?
   __ Yes  __ No  __Don’t Know  This is managed by: ___________________________

9. Does the clinic use procedures to control access to systems for testing and revision?
   __ Yes  __ No  __Don’t Know  This is managed by: ___________________________

10. If yes, are the procedures practiced consistently in the clinic?
    __ Yes  __ No  __Don’t Know
11. Does the clinic use procedures to document repairs and modifications to the physical components of the premises which relate to security, such as hardware, walls, doors, and locks?
   __ Yes  __ No  __Don’t Know  This is managed by: ______________________________

12. If yes, are the procedures practiced consistently in the clinic?
   __ Yes  __ No  __Don’t Know

WORKSTATION USE AND SECURITY

1. Has the clinic implemented physical safeguards and restricted access to all workstations (PCs, dumb terminals, portable devices) that have access to Information?
   __ Yes  __ No  __Don’t Know  This is managed by: ______________________________

2. Has the clinic implemented procedures that specify proper workstation functions be performed and the manner in which those functions are to be performed?
   __ Yes  __ No  __Don’t Know  This is managed by: ______________________________

3. Does the clinic utilize procedures that specify the physical attributes of the surroundings of workstations that can access Information?
   __ Yes  __ No  __Don’t Know  This is managed by: ______________________________

4. If yes, are these procedures practiced consistently in the clinic?
   __ Yes  __ No  __Don’t Know

DEVICE AND MEDIA CONTROLS

1. Does the clinic utilize procedures that govern the receipt and removal of hardware and electronic media that contains Information, and into and out of the premises?
   __ Yes  __ No  __Don’t Know  This is managed by: ______________________________

2. Does the clinic utilize procedures that govern the movement of hardware and electronic media that contains Information within the premises?
   __ Yes  __ No  __Don’t Know  This is managed by: ______________________________

3. Does the clinic utilize procedures to address the final disposition of Information and/or the hardware or electronic media on which it is stored?
   __ Yes  __ No  __Don’t Know  This is managed by: ______________________________

4. Does the clinic utilize procedures for removal of Information from electronic media before the media is made available for re-use?
   __ Yes  __ No  __Don’t Know  This is managed by: ______________________________
5. Does the clinic utilize procedures for maintaining a record of the movements of hardware and electronic media and any person responsible for these movements?
   __ Yes  __ No  __ Don’t Know  This is managed by: ______________________________

6. Does the clinic utilize procedures for the creation of a retrievable, exact copy of Information, when needed, before movement of equipment?
   __ Yes  __ No  __ Don’t Know  This is managed by: ______________________________

7. If yes, are these procedures practiced consistently in the clinic?
   __ Yes  __ No  __ Don’t Know

ADDITIONAL ASSESSMENT QUESTIONS

1. Does the clinic have fire suppression systems?
   __ Yes  __ No  __ Don’t Know

2. Does the clinic have working modems attached to any desktop workstations?
   __ Yes  __ No  __ Don’t Know

3. Are there any ancillary or free-standing computer systems in the clinic that are not attached to the network?
   __ Yes  __ No  __ Don’t Know

4. Are there any wireless access points or wireless workstations within or managed from this clinic?
   __ Yes  __ No  __ Don’t Know

5. Are there any closets or rooms that contain networking equipment?
   __ Yes  __ No  __ Don’t Know

6. Are there any network connections that are not in use in the clinic?
   __ Yes  __ No  __ Don’t Know

7. Are there any fax machines in the clinic?
   __ Yes  __ No  __ Don’t Know

8. If yes, are these fax machines accessing Information (imaging or faxback service), or are they plain paper faxes?
   __ Plain paper faxes only  __ Imaging  __ Faxback service

9. Have all workforce members been trained in HIPAA compliance?
   __ Yes  __ No  __ Don’t Know
Idaho State University Authorization for Use and Disclosure of Protected Health Information for Research

Patient Identification

Printed Name: ___________________________ Date of Birth: ___________________________
Address: _________________________________________________________________________
Social Security #: ___________________________ Telephone: _____________________________

Information To Be Released – Covering the Periods of Health Care

From (date) ___________________________ to (date) ___________________________

Please check type of information to be released:

___ Entire medical record   ___ Pathology report   ___ Discharge summary
___ History and physical exam   ___ Consultation reports   ___ Progress notes
___ Laboratory test results/reports   ___ X-ray reports   ___ X-ray films/images
___ Operative report   ___ Emergency room record   ___ Itemized bill
___ Other, (specify) __________________________________________________________________

Purpose of Request Related to Research

___ Treatment during clinical trial is conditional upon authorization
___ Treatment during clinical trial is not conditional upon authorization
___ At the risk of the patient
___ Billing or claims payment
___ Other, (specify) __________________________________________________________________

Person Authorized to Receive Information

Name: ___________________________________________________________________________
Address: _________________________________________________________________________
_________________________________________________________________________________

Drug and/or Alcohol Abuse and/or Psychiatric, and/or HIV/AIDS Records Release

I understand that if my medical or billing record contains information in reference to drug and/or alcohol abuse, psychiatric care, sexually transmitted disease, Hepatitis B or C testing, and/or other sensitive information, I agree to its release. Check One: ___ Yes ___ No  Initials ______

I understand that if my medical or billing record contains information in reference to HIV/AIDS (Human Immunodeficiency Virus/Acquired Immunodeficiency Syndrome) testing and/or treatment, I agree to its release. Check One: ___ Yes ___ No  Initials ______
**Time Limit and Right to Revoke Authorization**

Except to the extent that action has already been taken in reliance on this authorization, at any time I can revoke this authorization by submitting a notice in writing to the ISU HIPAA Compliance Officer at [location and mailing address]. Unless revoked, this authorization will expire on the following date or event 

______________________________

**Re-disclosure**

I understand the information disclosed by this authorization may be subject to re-disclosure by the recipient and will no longer be protected by the Health Insurance Portability and Accountability Act of 1996. ISU, its employees, officers and physicians are hereby released from any legal responsibility or liability for disclosure of the above information to the extent indicated and authorized herein.

**Signature of Patient or Personal Representative Who May Request Disclosure**

I understand that ISU may not condition my treatment on whether I sign this authorization form unless specified above under Purposes of Request. I can inspect or copy the protected health information to be used or disclosed. I authorize Idaho State University to use and disclose the protected health information specified above.

Signature: ____________________________ Date: __________________

Authority to Sign if not patient: ____________________________

Identity of Requestor Verified via:   ____ Photo ID   ____ Matching Signature   ____ Other, specify ____________

__________________________________________  Verified by: ____________________________
Accounting of Disclosures of Protected Health Information for Research

<table>
<thead>
<tr>
<th>Name and Address of Clinic Making Disclosure:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of Protocol or Research Activity</td>
</tr>
<tr>
<td>Description of the Protocol or Research Activity; Purpose of the Research; and Criteria for Selecting Records</td>
</tr>
<tr>
<td>Brief Description of the Type of PHI Disclosed</td>
</tr>
<tr>
<td>Date or Period of Time Disclosures Occurred, Including Date of Last Disclosure</td>
</tr>
<tr>
<td>Name, Address, Telephone Number of Research Sponsor to Whom PHI was Disclosed</td>
</tr>
<tr>
<td>Name, Address, Telephone Number of Research Sponsor to Whom PHI was Disclosed</td>
</tr>
</tbody>
</table>

During the accounting period listed above, we participated in Institutional Review Board or Privacy Board approved research activities where the protected health information of 50 or more patients was disclosed to another entity or researcher. Information about the research activity is listed below. Your PHI may or may not have been included in the research activity. If you need assistance in contacting the entity that sponsored the research and the researcher(s), please contact our HIPAA Compliance Officer at [Address, and telephone number of HIPAA Compliance Officer.]