



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 6/10	Revision Date:	Page: 1 of 1
	Section: ADMINISTRATION		Classification Code: 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

GENERAL STATEMENT OF POLICY

HIPAA Compliance – The Health Insurance Portability and Accountability Act of 1996 (HIPAA regulates health care providers (Covered Entities) that electronically maintain or transmit protected health information (PHI) in connection with a covered transaction. HIPAA requires each covered entity (CE) to maintain reasonable and appropriate administrative, technical and physical safeguards for privacy and security. Entities or individuals who contract to perform services for a CE with access to protected health information (Business Associates) are also required to comply with the HIPAA privacy and security standards.

Declaration of Hybrid Entity Status – The University is a hybrid entity under the HIPAA Privacy and Security Regulations. The University’s primary purpose is education; however, the University is subject to the HIPAA regulations because certain units of the University are covered entities. The University is required to identify its units that meet the CE definition, ensure CE compliance with safeguard and implementation specifications, and enforcement of CE and BA compliance with the HIPAA regulations.

The Vice President for Finance and Administration shall be responsible for issuing and maintaining operating procedures to implement this policy.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 1 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

OPERATING PROCEDURES

HIPAA HYBRID ENTITY

Southeast Missouri State University’s (“University”) business activities include both covered and non-covered functions under the HIPAA law and regulation. It has decided to designate itself as a Hybrid Entity.

The Hybrid Entity is required to ensure that it does not disclose protected health information to any other component of the University in circumstances in which HIPAA regulations would prohibit such disclosure if the health care component and the other component were separate and distinct legal entities.

Purpose - Designates the units within the University which are part of the Hybrid Entity subject to the Privacy and Security regulations of HIPAA.

Definitions - The terms used in this procedure have the same meaning as those terms in the Health Insurance Portability and Accountability Act and the regulations at 45 CFR Parts 160, 162, and 164.

Procedures –

- 1.0 University Health Care Components.** The University hereby designates the following as the health care components included in the Hybrid Entity:

 - The University’s Self-funded Health Plans
 - The University’s Autism Center for Diagnosis and Treatment
 - The University’s Health Clinic

- 2.0 Other University Covered Components:** The following are also designated as part of the Hybrid Entity to the extent that they perform activities that would make them business associates of one of the above health care components if they were separate entities:

 - Human Resources
 - Controller’s Office
 - Vice-President, President and Provost Office
 - Vice Provost and Support Staff
 - Information Technology
 - Student Financial Services

- 3.0 Covered Entity.** Whenever University policies, procedures or guidelines refer to the University as a covered entity under HIPAA, they are referring to the units listed above. The requirements of HIPAA apply only to the units of the University included within the Hybrid Entity.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 2 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

- 3.1 The previously listed units may not use or disclose protected health information that they create or receive from or on behalf of the health care component in a way prohibited by HIPAA.
- 3.2 Although workforce members of the Hybrid Entity perform duties for both the health care components and for other components of the University, they must not use or disclose PHI created or received in the course of or incident to the members' work for the health care component in a way prohibited by HIPAA.

HIPAA ORGANIZATION FOR COMPLIANCE

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, grants certain rights to individuals regarding their protected health information (PHI). This procedure has been drafted to ensure a structure for Southeast Missouri State University's ("University") compliance with applicable elements of the law and to guide University staff in assisting clients to exercise their rights.

Procedures –

- 1.0 HIPAA Chief Privacy Officer.** There shall be a HIPAA Chief Privacy Officer whose responsibilities are listed below.
 - 1.1 Responsibilities:
 - 1.1.1 Is responsible for overall coordination and oversight of compliance with HIPAA; ultimately assures that policies and procedures required by HIPAA are developed and implemented in a timely manner.
 - 1.1.2 Serves or appoints a designee as Privacy Officer At Large for the University components that do not have their own Privacy Officer; assures that these components are kept informed about HIPAA requirements and developments.
 - 1.1.3 Serves as chair of the HIPAA Compliance Committee; assures that responsibilities of this committee, HIPAA Chief Privacy Officer, and HIPAA Privacy Officers are coordinated so that persons best suited to complete tasks in each situation are assigned to those tasks; in cases of disagreement, makes decisions as to which officer and/or committee (in the case of committee creations) shall be primarily responsible for certain tasks.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 3 of 52
			Classification Code: OP 01-13
	Section: ADMINISTRATION		
	Subject: PROTECTION OF HEALTH INFORMATION		

- 1.1.4 Serves as information privacy consultant for all University departments and appropriate entities; works with all University personnel involved with any aspect of release of protected health information, to ensure full coordination and cooperation under the University’s policies and procedures and legal requirements.
- 1.1.5 Oversees privacy and security compliance activities, working closely with HIPAA Privacy Officers and HIPAA Security Officer.
- 1.1.6 Signs off on all HIPAA related policy and procedure statements, including those which are specific to only one component of the University hybrid covered entity.
- 1.1.7 In coordination with the University’s legal counsel,
 - 1.1.7.1 Provides guidance and assists in the identification, development, implementation and maintenance of uniform University HIPAA privacy and security policies and procedures.
 - 1.1.7.2 Prepares uniform business associate agreements for outside vendors; develops the standard privacy procedure to be used by each component of the hybrid covered entity.
 - 1.1.7.3 Identifies designee or serves as member of, or liaison to, University’s Institutional Review Board (IRB). Also serves as the information privacy liaison for users of clinical and administrative systems.
 - 1.1.7.4 Maintains and applies current knowledge of applicable federal and state privacy laws and accreditation standards.
 - 1.1.7.5 Serves as primary contact between the Office of Civil Rights, or other legal entities, and University officials in any compliance reviews or investigations.

2.0 HIPAA Privacy Officers. There shall be HIPAA Privacy Officers reporting to the HIPAA Chief Privacy Officer. The Director of University’s Health Clinic, University’s Self-funded Health Plans and the University’s Autism Center for Diagnosis and Treatment shall serve as the appointees for their respective units. In the event another University component is added to the hybrid covered entity, the Director of that unit shall assume the responsibilities as privacy officer. The HIPAA Chief Privacy Officer or designee shall serve as Privacy Officer At Large for other units that are part of the hybrid that is the covered entity.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 4 of 52
			Classification Code: OP 01-13
	Section: ADMINISTRATION		
	Subject: PROTECTION OF HEALTH INFORMATION		

2.1 Responsibilities:

- 2.1.1 Assist in preparing uniform HIPAA related procedures relating to Uses and Disclosures.
- 2.1.2 Assure implementation and compliance with HIPAA policies and procedures within their component.
- 2.1.3 Establish process and site specific training for all staff within the component who have access to PHI.
- 2.1.4 Collect and maintain current Business Associate agreements with all vendors to their units who are covered by HIPAA regulations.
- 2.1.5 Assure that HIPAA Privacy Notices are available and communicated as required by HIPAA.
- 2.1.6 Oversee patient and employee rights to inspect, request to amend, and restrict access to protected health information.
- 2.1.7 Assure that practices are in place to mitigate harmful effects of use or disclosure of protected health information in violation of University policies and procedures or requirements of law.
- 2.1.8 Serve on the HIPAA Compliance Committee.

3.0 HIPAA Training Officer. The HIPAA Chief Privacy Officer shall appoint the HIPAA Training Officer.

3.1 Responsibilities:

- 3.1.1 Oversees, directs and delivers or ensures delivery of privacy training and orientation to all employees and volunteers, except training specific to one health care component of hybrid entity.
- 3.1.2 Oversees maintenance of the HIPAA website, coordinating with Information Technology and Networks.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 5 of 52
			Classification Code: OP 01-13
	Section: ADMINISTRATION		
	Subject: PROTECTION OF HEALTH INFORMATION		

- 3.1.3 Provides oversight of distribution of information about HIPAA and compliance requirements to employees, students, volunteers and others within the University community.
- 3.1.4 Initiates, facilitates and promotes activities to foster information privacy awareness within University.
- 3.1.5 Maintains records of training completed by University employees within the University hybrid covered entity.
- 3.1.6 Serves on the HIPAA Compliance Committee.

4.0 HIPAA Complaint Officer. The HIPAA Chief Privacy Officer shall appoint the HIPAA Complaint Officer.

4.1 Responsibilities:

- 4.1.1 Establishes and administers a process for receiving, documenting, tracking, investigating and taking action on all complaints and reports of possible violations concerning University’s HIPAA privacy policies and procedures.
- 4.1.2 Assures that the University has effective policies and procedures for protecting an individual from retaliation for exercising rights under HIPAA.
- 4.1.3 Assures consistent application of sanctions for failure to comply with privacy procedures for all individuals in University’s workforce and for all business associates, in cooperation with Human Resources, Faculty Personnel Services and the HIPAA Security Officer.
- 4.1.4 Serves on the HIPAA Compliance Committee.

5.0 HIPAA Security Officer. The HIPAA Chief Privacy Officer and the Chief Information Officer will agree upon a person on the staff of the Office of Information Technology to be appointed HIPAA Security Officer.

5.1 Responsibilities:

- 5.1.1 Reviews all system-related information security plans throughout University’s network to ensure alignment between security and privacy practices.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 6 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

- 5.1.2 Assures compliance with electronic transaction standards.
- 5.1.3 Acts as liaison to the Office of Information Technology and Networks.
- 5.1.4 Monitors advancements in information privacy technologies to ensure University adaptation and compliance.
- 5.1.5 Coordinates establishment of systems, policies and procedures to comply with Security Regulations of HIPAA.
- 5.1.6 Serves on the HIPAA Compliance Committee.

6.0 HIPAA Compliance Committee.

6.1 Composition:

- 6.1.1 HIPAA Chief Privacy Officer (chair)
- HIPAA Privacy Officers
- HIPAA Complaint Officer
- HIPAA Training Officer
- HIPAA Security Officer

6.2 Meetings:

- 6.2.1 Semi-annually, or at call of Chair.

6.3 Responsibilities:

- 6.3.1 Assures communication among all units of the University involved with HIPAA compliance.
- 6.3.2 Engages in problem solving where broad input is needed.
- 6.3.3 Provides feedback on the successes and challenges of communication of HIPAA goals and rules to the campus at large.
- 6.3.4 Advocates for University-wide HIPAA policy and procedure wherever feasible.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 7 of 52
			Classification Code: OP 01-13
	Section: ADMINISTRATION		
	Subject: PROTECTION OF HEALTH INFORMATION		

- 6.3.5 Assures consistency in HIPAA related policies and procedures among components of hybrid covered entity.
- 6.3.6 Designates sub-committees as necessary.
- 6.3.7 Arranges for periodic information privacy risk assessments and compliance monitoring.
- 6.3.8 Arranges for periodic review to assure that University has appropriate administrative, technical and physical safeguards for protected health information, and confidentiality authorization forms and information notices.

PRIVACY PRACTICES

Purpose - The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its rules direct that covered entities provide individuals with adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual’s rights and the covered entity’s legal duties with respect to protected health information. This procedure issues Southeast Missouri State University’s (“University”) Notice of Privacy Practices and a Summary Notice of Privacy Practices for University Health Services, Self-funded Health Plans and Autism Center for Diagnosis and Treatment.

Procedures –

- 1.0** The attached Notice of Privacy Practices and the three Summary Notices of Privacy Practices are hereby issued as the policy and procedure of the University with regard to its obligations under HIPAA.
- 2.0** The names, addresses and contact numbers for health care components, and similar information, may be changed in the Notice of Privacy Practices and the Summary Notices of Privacy Practices, upon authorization of the Chief Privacy Officer.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 8 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

SOUTHEAST MISSOURI STATE UNIVERSITY

**HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)
NOTICE OF PRIVACY PRACTICES**

THIS NOTICE DESCRIBES HOW MEDICAL/PROTECTED HEALTH INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN ACCESS THIS INFORMATION.

PLEASE REVIEW IT CAREFULLY.

Healthcare Components in the Hybrid Entity Covered by this Notice

Southeast Missouri State University (“University”) is a covered entity under HIPAA law. It has decided to designate itself as a hybrid entity. This notice applies to the privacy practices of the following health care components included in the hybrid entity that may share your Protected Health Information as needed for treatment, payment and health care operations.

- **The University’s Autism Center for Diagnosis and Treatment**
- **The University’s Health Clinic**
- **The University’s Self-funded Health Plans**

Our Commitment Regarding Your Protected Health Information

We understand the importance of your Protected Health Information (hereafter referred to as “PHI”) and follow strict policies (in accordance with state and federal privacy laws) to keep your PHI private. PHI is information about you, including demographic data, that can reasonably be used to identify you and that relates to your past, present or future physical or mental health, the provision of health care to you, or the payment for that care.

In this notice, we explain how we protect the privacy of your PHI, and how we will allow it to be used and given out (“disclosed”). We are required to provide you with a summary of our Notice of Privacy Practices, and a copy of the Notice of Privacy Practices upon request. We must follow the privacy practices described in this notice while it is in effect. This notice is effective August 1, 2010, and will remain in effect until we replace or modify it.

We reserve the right to change our privacy practices and the terms of this notice at any time, provided that applicable law permits such changes. These revised practices will apply to your PHI regardless of when it was created or received. Before we make a material change to our privacy practices, we will provide you with a revised Notice of Privacy Practices.

Where multiple state or federal laws protect the privacy of your PHI, we will follow the requirements that provide the greatest privacy protection. *University student medical records are subject to requirements of the Federal Educational Rights and Privacy Act of 1974 (FERPA) rather than HIPAA in certain circumstances.*

Our Uses and Disclosures of Protected Health Information

We do not sell your PHI to anyone or disclose your PHI to other companies who may want to sell their products to you (e.g., catalog or telemarketing firms).



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 9 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

We must have your written authorization to use and disclose your PHI, except for the following uses and disclosures:

- **To You:**

We may disclose your PHI to you, for example:

- Supplying you with information about your diagnosis or treatment
- Communicating with you about treatment alternatives or other health-related benefits and services

- **For Treatment:**

We may use and disclose your PHI to health care providers and our business associates who request PHI in connection with your diagnosis, treatment, management of your care, coordination of benefits, and insurance eligibility, for example:

- Physicians and physician's assistants
- Nurses
- Dentists
- Physical or occupational therapists
- Psychologists, counselors or social workers
- Pharmacies
- Hospitals

We may disclose your PHI to health care providers in connection with:

- Disease and case management programs
- Prescribing medications
- Ordering lab work or diagnostic imaging at an outside facility
- Referring you to an outside provider
- Providing emergency medical treatment
- Psychological consultations
- Other health care services

- **For Payment:**

We may use and disclose your PHI for our payment-related activities and those of health care providers and health plans, including for example:

- Dealing with protected health information in relation to the University's Self-funded Health Plans
- Responding to inquiries, appeals and grievances
- Billing you or a health plan for health care services provided to you through the Autism Center for Diagnosis and Treatment

- **For Health Care Operations:**

We may use and disclose your PHI for the following health care operations, for example:

- Conducting quality assessment and improvement activities, including peer review, credentialing of providers, and accreditation, and conducting training programs
- Auditing billing processes
- Performing outcome assessments and health claims analyses
- Preventing, detecting and investigating fraud and abuse
- Coordinating case and disease management activities
- Performing business management and other general administrative activities, including systems management and customer service
- Scheduling appointments and keeping records



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 10 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

Autism Center for Diagnosis and Treatment (“Autism Center”) clients: Your name, address and telephone number may be used to contact you in connection with fundraising for the Autism Center for Diagnosis and Treatment. We may also send this information to the Southeast Missouri State University Foundation for the same purpose. If you do not want to receive these materials, please contact the Autism Center’s Privacy Officer and request that these fundraising materials not be sent to you. The Autism Center may use or disclose your medical information, as necessary, to provide you with information about treatment alternatives or other health-related benefits and services that may be of interest to you. For example, your name and address may be used to send you a newsletter about our practice and the services we offer. We may also send you information about products or services that we believe may be beneficial to you. You may contact the Autism Center’s Privacy Officer to request that these materials not be sent to you.

The Self-funded Health Plans may disclose your PHI to Southeast Missouri State University personnel solely for purposes of administrating benefits under this plan.

• **To Others Involved in Your Care:**

We may disclose your PHI to someone who has the legal right to act on your behalf. We may under certain circumstances disclose to a designated contact person (e.g.: a member of your family, a relative, a close friend or any other person you identify), the PHI directly relevant to that person’s involvement in or payment for your health care.

• **When Required by Law:**

We will use and disclose your PHI if we are required to do so by law. For example, we will use and disclose your PHI.

- To report infectious diseases
- To respond to court and administrative orders and subpoenas
- To comply with workers’ compensation laws
- To report suspected abuse and neglect to the proper authorities
- To law enforcement under certain circumstances
- To report PHI as required by the U.S. Secretary of Health and Human Services and state regulatory authorities
- To report threats to safety of self or others
- To a health oversight agency, which includes government agencies that oversee the healthcare system, for example, audits, investigations, civil administration or criminal investigations

• **For Matters in the Public Interest:**

We may use or disclose your PHI without your written permission for matters in the public interest, including for example:

- Public health and safety activities, including Food and Drug Administration oversight, reporting disease and vital statistics.
- Averting a serious threat to the health or safety of others, e.g.: as required under the Patriot Act Without your prior authorization.

• **For Research:**

We may use your PHI to perform select research activities, provided that certain established measures to protect your privacy are in place, e.g. as required by the Institutional Review Board.

• **To Our Business Associates:**

From time to time we engage third parties to provide various services for us. Whenever an arrangement with such a third party involves the use or disclosure of your PHI, we will have a written contract with that third party designed to protect



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 11 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

the privacy of your PHI. For example, we may share your information with business associates who bill for medical services, process claims or conduct disease management programs on our behalf.

Disclosures You May Request -

You may instruct us and give your written authorization to disclose your PHI to a designated individual or agency for any purpose. We require that your authorization be on a HIPAA compliant form. To obtain the form, contact the applicable health care component:

- The University's Autism Center for Diagnosis and Treatment** (573) 986-4985
- The University's Health Clinic** (573) 651-2270
- The University's Self-funded Health Plans** (573) 651-2206

Individual Rights -

You have the following rights. To exercise these rights, you must make a written request on our standard form. To obtain the form, contact the designated covered component (see above).

Access - With certain exceptions, you have the right to look at or receive a copy of your PHI contained in the group of records that are used by or for us to make decisions about you, including our enrollment, payment and case or medical management notes. We reserve the right to charge a reasonable cost-based fee for copying and postage. If you request an alternative format, such as a summary, we may charge a cost-based fee for preparing the summary. If we deny your request for access, we will tell you the basis for our decision and whether you have a right to further review. You may request access to PHI in an alternative communication format and/or location. If your PHI is maintained in an electronic health record, you also have the right to request that an electronic copy of your record be sent to you or to another individual or entity. We may charge you a reasonable cost-based fee limited to the labor costs associated with transmitting the electronic health record.

Disclosure Accounting - You have the right to an accounting of certain disclosures of your PHI, such as disclosures required by law. If you request this accounting more than once in a 12-month period, we may charge you a fee covering the cost of responding to these additional requests.

Restriction Requests - You have the right to request that we place restrictions on the way we use or disclose your PHI for treatment, payment or health care operations. We are not required to agree to these additional restrictions, unless you request that your PHI not be disclosed to a health plan for purposes of payment and health operations if you paid out of pocket for that service. If we agree, we will abide by them (except as needed for emergency treatment or as required by law) unless we notify you that we are terminating our agreement.

Revoke Prior Authorization - You may revoke your authorization, except to the extent that we have taken action upon it.

Amendment - You have the right to inspect PHI and request that we amend it in the set of records we described above under Access. If we deny your request, we will provide you a written explanation. If you disagree, you may have a statement or your disagreement placed in our records. If we accept your request to amend the information, we will make reasonable efforts to inform others of the amendment, including individuals you name.

Confidential Communication - You may request to receive confidential communications from us by alternative means or at an alternative location. We will accommodate reasonable requests. We may condition this accommodation by asking you for information as to how payment will be handled or specification of an alternative address or other method of contact.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 12 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

Notice of a Breach - We are required to notify you by first class mail or by e-mail (if you have indicated a preference to receive information by e-mail), of any breaches of Unsecured Protected Health Information as soon as possible, but in any event, no later than 60 days following the discovery of the breach. “Unsecured Protected Health Information” is information that is not secured through the use of a technology or methodology identified by the Secretary of the U.S. Department of Health and Human Services to render the Protected Health Information unusable, unreadable, and undecipherable to unauthorized users. The notice is required to include the following information:

- a brief description of the breach, including the date of the breach and the date of its discovery, if known;
- a description of the type of Unsecured Protected Health Information involved in the breach;
- steps you should take to protect yourself from potential harm resulting from the breach;
- a brief description of actions we are taking to investigate the breach, mitigate losses, and protect against further breaches;
- contact information, including a toll-free telephone number, e-mail address, Web site or postal address to permit you to ask questions or obtain additional information.

In the event the breach involves 10 or more persons whose contact information is out of date we will post a notice of the breach on the home page of our Web site or in a major print or broadcast media. If the breach involves more than 500 persons in the state or jurisdiction, we will send notices to prominent media outlets. If the breach involves more than 500 persons, we are required to immediately notify the U.S. Secretary. We also are required to submit an annual report to the U.S. Secretary of Health and Human Services of a breach that involved less than 500 persons during the year and will maintain a written log of breaches involving less than 500 persons.

Paper Copy - You have the right to obtain a paper copy of this notice from us upon request, even if you have agreed to accept this notice electronically.

Questions and Complaints -

If you need more information about our privacy practices, or a written copy of the Summary Notice of Privacy Practices, please contact us at:

The University’s Health Clinic, Crisp Hall, Rm. 101, (573) 651-2270
 The University’s Self-funded Health Plans, Human Resources, Academic Hall, Rm. 220, (573) 651-2206
 The University’s Autism Center for Diagnosis and Treatment, 611 N. Fountain Street, Cape Girardeau, Missouri 63701 (573) 986-4985

For your convenience, you may also obtain an electronic (downloadable) copy of the Summary Notices of Privacy Practices as well as the University Complaint Form online at <http://www.semo.edu/finadm/> under Forms - HIPAA

If you are concerned that we may have violated your privacy rights, or you believe that we have inappropriately used or disclosed your PHI, please contact: HIPAA Complaint Officer Dr. Fred Janzow, Vice Provost, (573) 651-2062.

You may also submit a written complaint to: Region VII – Office of Civil Rights U.S. Department of Health and Human Services, 601 East 12th Street, Room 248, Kansas City, MO 64106.
 Phone: (816) 426-7277.

We support your right to protect the privacy of your PHI. We will not take action against you if you file a complaint with us or with the U.S. Department of Health and Human Services.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 13 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

**SOUTHEAST MISSOURI STATE UNIVERSITY
AUTISM CENTER FOR DIAGNOSIS AND TREATMENT**

SUMMARY NOTICE OF PRIVACY PRACTICES

This is a summary of the University’s Autism Center for Diagnosis and Treatment (“Autism Center”)’s Notice of Privacy Practices and describes how the Autism Center may use and disclose protected health information (PHI) and how you can access this information. Please review this information carefully. This Summary applies to the clinical programs of the Autism Center. The Health Insurance Portability and Accountability Act (HIPAA) requires that we protect the privacy of health information that identifies clients, or when there is reasonable basis to believe the information can be used to identify a client. This notice describes your rights as a client and our obligations regarding the use and disclosure of PHI.

USES AND DISCLOSURE

Uses and Disclosures Statement

- We may disclose your PHI to you.
- We may use or disclose your PHI without your authorization or opportunity to object to treat you, obtain payment, or operate the Autism Center.
- Other uses and disclosures may be made without your authorization or opportunity to object if the law requires us to disclose PHI.
- In most situations not associated with treatment, payment or operations, we may use or disclose your PHI only **with** your written authorization.

Examples of Uses and Disclosures for Treatment

Authorization Not Required

- We may consult with other health care providers in connection with your diagnosis and treatment.
- We may disclose PHI regarding treatment, coordination, and management of your health care as it related to (1) services related to your psychological care; or (2) other health care services.
- If you are referred to a physician or other psychologist or a new health care provider, we may disclose PHI to the new provider relating to your diagnosis and treatment.

Examples of Uses and Disclosures to Obtain Payment

Authorization Not Required

- We may use and disclose your PHI to 1) submit a claim with your name, birth date, address, insurance or social security number, diagnoses, and procedures performed to your health plan for payment; 2) submit PHI for coordination of benefit purposes; 3) respond to inquiries for purposes of obtaining payment.
- We may disclose PHI to other health care providers in connection with coordination of benefits or insurance eligibility.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 14 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

Examples of Uses and Disclosures to Operate the Autism Center Authorization Not Required

- We may mail you reminders of upcoming appointments.
- We may leave telephone messages asking that you return our call or reminding you of an appointment.
- We may use and disclose your PHI to audit billing processes and evaluate the quality of our services.
- We may share PHI with organizations that assess the quality of care that we provide, e.g., accreditation agencies.
- We may provide PHI to you as needed to supply you with information about your diagnosis or treatment.
- We may communicate with you about our clinic services and therapies, your treatment alternatives or other health related benefits and services.
- Unless you object, we may use your name, address and telephone number to contact you in connection with fundraising for the Autism Center.
- We may use your PHI to file reports required by law, e.g.: when abuse or neglect is suspected, when subpoenaed, etc.
- We may use your PHI if you pose a danger to yourself and or others.
- We may share your PHI with third party “business associates” that perform various activities like billing for the Autism Center. Whenever an arrangement between the Autism Center and a business associate involves the use or disclosure of your medical information, we will have written contract terms that will protect the privacy of your medical information.

YOUR RIGHTS

You have the following rights regarding your PHI, and the Autism Center must act on your request within 60 days.

- You may request restrictions on certain uses and disclosures of PHI, but we are not required to agree to a requested restriction, unless you request that PHI not be disclosed to a health plan for purposes of payment or health operations and you paid out of pocket for that service.
- You may request access to PHI in alternative communication format and/or location.
- You may request that you receive confidential communications of PHI.
- You may request to inspect and/or request a copy of your own PHI.
- You may request that your records be amended.
- You may request a copy of our Notice of Privacy Practices on paper or in an alternative format, e.g., electronic.
- You may revoke an authorization, except to the extent that we have taken action on it.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 15 of 52
			Classification Code: OP 01-13
	Section: ADMINISTRATION		
Subject: PROTECTION OF HEALTH INFORMATION			

OUR RESPONSIBILITIES

The law requires us to maintain the privacy and security of PHI.

- The law requires that we provide individuals with notice of our privacy practices.
- The law requires that we abide by the terms of the Notice of Privacy Practices and provide notice of revisions.
- The law requires that we notify you within 60 days of discovery of a breach of any of your unsecured PHI.

QUESTIONS/CONCERNS

For more information, or a copy of the entire Notice of Privacy Practices, please visit <http://www.semo.edu/finadm/> or contact the Privacy Officer, Connie L. Hébert, Southeast Missouri State University Autism Center for Diagnosis and Treatment, 611 N. Fountain Street, Cape Girardeau, MO 63701 (573) 986-4985.

COMPLAINTS

If you believe your privacy rights have been violated, you may submit a complaint in writing using the University *Health Information Privacy Complaint Form* available at <http://www.semo.edu/finadm/> or from the Privacy Officer or the Reception area of the Autism Center. Send completed complaint forms to the HIPAA Complaint Officer, Southeast Missouri State University, One University Plaza, MS 3400, Cape Girardeau, MO 63701. You may file a complaint directly with the U.S. Department of Health and Human Services, visit <http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html>. No one will retaliate against you for filing a complaint.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 17 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

YOUR RIGHTS

You have the following rights regarding your PHI, and University Health Clinic must act on your written request within 60 days.

- You may request restrictions on certain uses and disclosures of PHI, but we are not required to agree to a requested restriction, unless you request that your PHI not be disclosed to your health plan for payment or healthcare operations and you paid out of pocket for that service.
- You may request access to your PHI in an alternative communication format or location.
- You may request that you receive confidential communications of PHI.
- You may request to inspect and receive a copy of your PHI.
- You may request that your information be amended.
- You may request a copy of our Notice of Privacy Practices on paper or in an alternative format, e.g., electronic.

You may revoke an authorization, except to the extent that we have taken action on it.

OUR RESPONSIBILITIES

The law requires that we maintain the privacy of PHI.

- The law requires that we provide individuals with notice of our privacy practices.
- The law requires us to abide by the terms of the Notice of Privacy Practices and provide notice of revisions.
- The law requires that we notify you within 60 days of discovery of a breach of any of your unsecured PHI.

QUESTIONS/CONCERNS

For more information, or a copy of the entire Notice of Privacy Practices, please visit www.semo.edu/finadm or contact the Privacy Officer, Dr. Bruce Skinner, Office of Residence Life Director, Towers Complex, Rm. 102, (573) 651-2274.

COMPLAINTS

If you believe your privacy rights have been violated, you may submit a complaint in writing using the University Health Information Privacy Complaint Form available at <http://www.semo.edu/finadm> or from the Privacy Officer or the Reception area of the University Health Clinic. Send completed complaint forms to the HIPAA Complaint Officer, Southeast Missouri State University, One University Plaza, MS 3400, Cape Girardeau, MO 63701. You may file a complaint directly with the U.S. Department of Health and Human Services, visit <http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html>.

No one will retaliate against you for filing a complaint.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 18 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

**SOUTHEAST MISSOURI STATE UNIVERSITY
SELF-FUNDED HEALTH PLANS**

SUMMARY OF NOTICE OF PRIVACY PRACTICES

This is a summary of The University's Self-funded Health Plans Notice of Privacy Practices and describes how as a health plan we may use and disclose your protected health information (PHI) and how you can access this information. Please review this information carefully. The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule requires that we protect the privacy of health information that identifies an employee, or when there is reasonable basis to believe the information can be used to identify an employee. This notice describes your rights as a participant in the University's Self-funded Health plans and our obligations regarding the use and disclosure of PHI.

USES AND DISCLOSURE

Uses and Disclosures Statement

- We may use or disclose your PHI *without* your authorization or opportunity to agree or object to treat you, to obtain payment, and to operate the University's Self-funded Health plans.
- Other uses and disclosures can be made *without* your authorization or opportunity to agree or object, e.g., if the law requires us to disclose information to government authorities such as legal requests, suspected abuse, and infectious diseases.
- In most situations not associated with payment, treatment, or operations, we may use or disclose your PHI only *with* your written authorization.

Examples of Uses and Disclosures to Obtain Payment Authorization Not Required

- We may use and disclose your PHI for payment related activities and those of health care providers and other health plans including for example:
- submit a claim form that contains your name, date of birth, address, insurance, social security number, diagnoses, and procedures performed to the health plan for payment
- submit PHI for coordination of benefit purposes
- responding to inquiries for purposes of making or obtaining payment

Examples of Uses and Disclosures to Operate the Health Plan Authorization Not Required

- We may mail PHI to you as we confirm payment from your Self-funded Health Plans.
- We may leave telephone messages asking that you return our call.
- We may use and disclose your PHI to audit billing processes.
- We may share PHI with organizations that assess the quality of care we provide.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 19 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

YOUR RIGHTS

You have the following rights regarding your PHI, and The Self Funded Health Plan through Human Resources must act on your written request within 60 days.

- You may request restrictions on certain uses and disclosures of PHI, but we are not required to agree to a requested restriction, unless you request that your PHI not be disclosed to your health plan for payment or healthcare operations and you paid out of pocket for that service.
- You may request access to your PHI in an alternative communication format or location.
- You may request that you receive confidential communications of PHI.
- You may request to inspect and receive a copy of your PHI.
- You may request that your information be amended.
- You may request a copy of our Notice of Privacy Practices on paper or in an alternative format, e.g., electronic.
- You may revoke an authorization, except to the extent that we have taken action on it.

OUR RESPONSIBILITIES

- The law requires that The University’s Self-funded Health Plans maintain the privacy of PHI.
- The law requires that we provide notice of our privacy practices.
- The law requires us to abide by the terms of the Notice of Privacy Practices and provide notice of revisions.
- The law requires that we notify you within 60 days of discovery of a breach of any of your unsecured PHI.

QUESTIONS/CONCERNS

For more information, or a copy of the entire Notice of Privacy Practices, please visit <http://www.semo.edu/finadm/> or contact Alissa Vandeven, Privacy Officer, Southeast Missouri State University, Human Resources, Self-funded Health Plans at (573) 651-2006.

COMPLAINTS

If you believe your privacy rights have been violated, you may submit a complaint in writing using the University *Health Information Privacy Complaint Form* available at <http://www.semo.edu/finadm> or from Human Resources, Room 220, Academic Hall. Send completed complaint forms to the HIPAA Complaint Officer, Southeast Missouri State University, One University Plaza, MS 3400, Cape Girardeau, MO 63701. You may file a complaint directly with the U.S. Department of Health and Human Services, visit <http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html>. No one will retaliate against you for filing a complaint.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 20 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

CLIENT COMPLAINTS RELATED TO PROTECTED HEALTH INFORMATION REPORTS OF BREACH OF PRIVACY AND SECURITY OF PHI

Background - Southeast Missouri State University (“University”) is a covered entity under the HIPAA law and regulations. According to this law, all University officers, employees, and agents must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client. This IIHI is protected health information (PHI) and shall be safeguarded to the highest degree possible in compliance with the requirements of the security and privacy rules and standards established under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended.

Purpose - The Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, and its rules direct covered entities to provide a process for individuals to lodge complaints regarding the handling of protected health information (PHI) and for employees to report possible violations of HIPAA law or rules or the University’s HIPAA policies and procedures. This procedure establishes a process for persons to register complaints regarding the University’s privacy policy and procedures and/or its compliance with those policies and procedures. This procedure also informs persons of their right to file complaints with the Secretary, U.S. Department of Health and Human Services.

Definitions - The terms used in this procedure have the same meaning as those terms in the Health Insurance Portability and Accountability Act of 1966, as amended, and the regulations at 45 CFR Parts 160, 162, and 164.

Procedures -

- 1.0 Filing a complaint at the University.** Persons who believe that the University or its employees or agents may have violated the requirements of HIPAA law or rules, or the University’s HIPAA policies and procedures may file a complaint either with the HIPAA Complaint Officer or any HIPAA Privacy Officer. Any officer, employee or agent of University who believes another officer, employee or agent of University has breached the University’s HIPAA privacy or security policies and/or procedures or otherwise breached the integrity or confidentiality of patient or client or other sensitive information shall immediately report the alleged breach to his or her supervisor or to the HIPAA Complaint Officer. Supervisors who receive reports of alleged breach of the HIPAA privacy or security policies and/or procedures shall immediately report the allegation to the HIPAA Complaint Officer.
- 2.0 Filing a complaint with the U.S. Secretary.** Persons who believe that the University or its employees or agents may have violated the requirements of HIPAA law or rules may also file a complaint with the of the U.S. Department of Health and Human Services.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 21 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

- 3.0 Documenting Complaints.** The University’s Notice of Privacy Practices, distributed to clients, patients, and participants in the University’s Self-funded Health plans, shall include a notification of the offices with which complaints may be filed or possible violations may be reported. The University HIPAA Complaint Officer shall document all complaints received and the disposition of those complaints. Documentation shall be retained as required by law.
- 4.0 Non-retaliatory.** No University officer, employee or agent shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual who files a complaint with the University or with the U.S. Secretary of Health and Human Services.
- 5.0 Discipline.** An officer, employee or agent who discriminates or retaliates against an individual who files a complaint to University or the U.S. Secretary shall be subject to disciplinary action up to and including termination.
- 6.0 Complaint Process.**
- 6.1 Communicating Process to Clients. The University’s Notice of Privacy Practices shall direct individuals to submit a complaint regarding management of PHI to University’s HIPAA Complaint Officer or any HIPAA Privacy Officer. The Notice shall also indicate that a complaint can be made directly to the U.S. Secretary of Health and Human Services (HHS). The Notice shall notify clients of the availability of complaint forms at the reception desk of the health care component, or from the HIPAA Complaint Officer.
- 6.2 Complaint Form. Complaints regarding the University’s privacy policy and procedures and/or its compliance with those policies and procedures shall be submitted in writing on a complaint form prepared by the University. The form shall be available on the University’s website <http://www.semo.edu/finadm/> under Forms – HIPAA, at the office of the HIPAA Complaint Officer, all HIPAA Privacy Officers, and at the reception desk of the health care components.
- 6.3 Complaints to Health and Human Services. Complaints made to the U.S. of Health and Human Services shall be made in writing using whatever form the client wishes and shall be mailed directly to the U.S. Secretary at:

Secretary
U.S. Department of Health and Human Services
200 Independence Ave., S. W.
Washington, D. C. 20201



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 22 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

- 6.4 University Handling of Complaints. The University’s HIPAA Complaint Officer or Privacy Officer shall receive and handle all complaints regarding the management of an individual’s protected health information according to the procedure entitled *HIPAA: Investigation of Complaints & Reports of Breach of Privacy and Security of PHI; Sanctions for Breach of Privacy and Security of PHI*.

7.0 Documentation of Complaints and Disposition.

- 7.1 Retention of Complaints and Disposition. All complaints to the University regarding its management of protected health information and documentation of the disposition of those complaints shall be filed in the office of the HIPAA Complaint Officer in a manner that all documentation can be easily retrieved for review and/or audit. The documentation shall be retained for a period of six years from the date of the complaint.

Contact for More Information:

HIPAA Privacy Officer
The University’s Self- funded Health Plan
Academic Hall, Rm. 220
Cape Girardeau, MO 63701
Phone: (573) 651-2206

HIPAA Privacy Officer
The University’s Health Clinic
Crisp Hall, Rm. 101
Cape Girardeau, MO 63701
Phone: (573) 651-2270

HIPAA Privacy Officer
The University’s Autism Center for Diagnosis and Treatment
611 N. Fountain Street
Cape Girardeau, MO 63701
Phone: (573) 986-4985



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 23 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

**INVESTIGATION OF COMPLAINTS & REPORTS OF BREACH OF PRIVACY AND SECURITY
OF PHI SANCTIONS FOR BREACH OF PRIVACY AND SECURITY OF PHI**

Background - Southeast Missouri State University (“University”) is a covered entity under the HIPAA law and regulations. According to this law, all University officers, employees, and agents must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client. This IIHI is protected health information (PHI) and shall be safeguarded to the highest degree possible in compliance with the requirements of the security and privacy rules and standards established under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended.

Purpose - The University has adopted this procedure to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, and the privacy regulations, as well as to fulfill our duty to protect the confidentiality and integrity of confidential protected health information as required by law, professional ethics, and accreditation requirements.

Definitions - The terms used in this procedure have the same meaning as those terms in the Health Insurance Portability and Accountability Act of 1996, as amended, and the regulations at 45 CFR Parts 160, 162, and 164.

Procedures –

- 1.0 Grounds for Disciplinary Action:** The University prohibits violations of HIPAA statutory and regulatory requirements, and University policies and procedures in place to uphold them. Any violation of HIPAA rules or University policy and procedures shall constitute grounds for disciplinary action.
- 2.0 Disciplinary Process:** The disciplinary process and sanctions that may be imposed for a violation of HIPAA law, regulations and/or University policies and procedures will vary according to the status of the person who has engaged in the violation.
 - 2.1 Employees, including student employees, will be subject to the disciplinary processes already in place for their employee group. Disciplinary action may include termination. If the seriousness of the offense warrants such action, an employee may be terminated for the first breach of HIPAA law, regulation or University’s HIPAA policy and procedures.
 - 2.2 Students who are engaged in clinical experiences giving them access to protected health information will be subject to discipline by the work site, up to and including termination from the clinical work. If the student is enrolled in a class, he/she will be subject to grading consequences according to the judgment of the instructor for that class. Students enrolled in clinical programs may be further subject to review for their fitness for continuation in the clinical education program according to the criteria and processes established by that clinical program.
 - 2.3 Contractors are subject to termination of the contract.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 24 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

- 3.0 Criminal Prosecution.** Violations of HIPAA law and regulations may also subject the violator to criminal prosecution.
- 4.0 Non-retaliatory.** No University officer, employee or agent shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual who files a complaint or reports a possible breach to the integrity or confidentiality of client or other sensitive information, or who cooperates in the investigation or disciplinary procedure arising out of a complaint or report.
- 5.0 Cooperation with Investigations.** All officers, employees, students, contractors and agents of the University are expected to comply and cooperate with the University’s investigation and sanctioning of violations of HIPAA law, regulations, and University HIPAA procedure.
- 6.0 False Accusations by Employees.** Any employee who knowingly falsely accuses another of a breach of HIPAA rules and procedure shall be subject to disciplinary action up to and including termination.
- 7.0 False Accusations by Students.** Any student who knowingly falsely accuses another of a breach of HIPAA rules and procedures shall be subject to disciplinary action subject to Statement of Student Rights and Code of Student Conduct, up to and including termination from a program.
- 8.0 Report of Alleged Violation of HIPAA law, regulation or University HIPAA policy and procedures.** Any person may report an alleged violation of HIPAA compliance by following the HIPAA Privacy Complaint Procedure.
- 9.0 Investigation of Allegations.**
- 9.1 If an allegation is reported to a Privacy Officer for the health care component where the violation may have occurred, the Privacy Officer may attempt to resolve the allegation. If the allegation is not resolved within one week of its filing, the Privacy Officer must report the allegation to the Complaint Officer.
- 9.1.1 **Conduct of Investigation.** Upon receipt of an allegation, the Complaint Officer will assure that an inquiry or investigation is conducted in coordination with the Privacy Officer of the health care component where the violation may have occurred and Human Resources. The inquiry or investigation and disciplinary process, if any, shall comply with the procedures provided in the University’s procedures. The Complaint Officer shall assure that a thorough and confidential investigation into the allegations is conducted.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 25 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

- 9.1.2 Notification of Complainant. When the investigation has been completed and a decision related to the allegations has been reached and implemented, the Complaint Officer shall notify the complainant of the results of the investigation and any corrective action taken.
- 9.1.3 Resolutions by Privacy Officers. If a Privacy Officer resolves an allegation, he/she shall provide a written report of the allegation and its resolution to the HIPAA Complaint Officer.

10.0 Corrective Action.

- 10.1 If the investigation of an allegation of a violation concludes that one or more employees are responsible for the violation, they may be disciplined according to the established University procedures for disciplining an employee in that employee group. Serious or repeated violations may lead to termination.
- 10.2 If the investigation of an allegation of a violation concludes that a system or procedure or policy of the University is responsible for the violation, corrective action will be taken. The HIPAA Complaint Officer will oversee the implementation of needed changes.

11.0 Criminal Prosecution. Willful and grossly negligent breaches of HIPAA law or regulations may also result in criminal prosecution.

- 11.1 **Agency Cooperation With Criminal Prosecution.** In the event that violation of the University’s procedures and standards for privacy and security of PHI constitutes a criminal offense under HIPAA or other federal or state laws, the violator should expect that the University shall provide information concerning the violation to appropriate law enforcement personnel and will cooperate with any law enforcement investigation or prosecution.

12.0 University Involvement in Professional Discipline. In the event that violation of HIPAA law or rules or the University’s HIPAA procedures and standards for privacy and security of PHI constitutes a violation of professional ethics and is grounds for professional discipline, the violator should expect that the University may report such violations to the appropriate licensure/accreditation agencies and will cooperate with any professional investigation or disciplinary proceedings.

13.0 Treatment of Agents and Contractors. The University will seek to include violations of HIPAA law or rules or the University’s HIPAA policies and procedures as grounds for termination of the contract and/or imposition of contract penalties.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 26 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

14.0 Documentation of Sanctions. The Complaint Officer will maintain a record of allegations received and their disposition, including sanctions that are applied. This documentation will be retained for six years from the date of its creation or the date when it last was in effect.

HIPAA MINIMUM NECESSARY USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

Purpose - The Health Insurance Portability and Accountability Act of 1996 (HIPAA) granted certain rights to patients/clients/employees regarding their protected health information (PHI). This procedure has been drafted to assist Southeast Missouri State University (“University”) to comply with the law and to guide University staff in assisting patients/clients/employees to exercise their rights.

Definitions - The terms used in this procedure have the same meaning as those terms in the Health Insurance Portability and Accountability Act of 1996, as amended, and the regulations at 45 CFR Parts 160, 162, and 164. Minimum Necessary is not defined in the Privacy Rule, but is a term used to describe the amount of PHI needed to perform a particular task or function.

Procedures –

- 1.0 Limited Uses and Disclosures.** The University shall take reasonable steps to limit the uses, disclosures of, and requests for PHI to the minimum necessary to accomplish the intended purpose.
- 2.0 Identification Categories for Access to PHI.** The University shall maintain procedures that identify persons or classes of persons within the University and its business associates who need access to PHI to carry out their job duties, the categories or types of PHI needed, and conditions appropriate for such access.
- 3.0 Access to Entire Medical Record.** When access to an entire medical record is necessary, University procedures shall state so explicitly and include written justification for such access.
- 4.0 The minimum necessary provisions contained in these procedures do not apply to the following:**
 - Disclosures to or requests by a health care provider for treatment purposes
 - Uses and disclosures to the patient/client/employee who is the subject of the information
 - Uses or disclosures made pursuant to an authorization provided by a patient/client/employee
 - Uses or disclosures required for compliance with the standardized HIPAA transactions



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 27 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

- Disclosures to the U.S. Department of Health and Human Services (HHS) when disclosure of information is required under the rule for enforcement purposes
- Uses or disclosures that are required by other law.

5.0 Use of PHI. Persons and Classes of Persons in the University Workforce Who Need Access to PHI. The University recognizes that a number of persons and groups of persons need access to some level of PHI to carry out their job duties. The Privacy Officer for each unit of the hybrid entity shall maintain a list of the classifications of personnel (including student clinicians/interns and volunteers) approved to have routine access to PHI in the performance of their duties.

- 5.1 **Receivable Accounting/Student Financial Services:** Employees in these units of the University may have access to PHI to the extent necessary to fulfill their responsibilities. For example, this office may handle some billing and collections of students and others for services received from the University’s Health Clinic or for medical services provided by the University’s Autism Center. The records to which this unit would have access are limited to those related to billing and usually include only personally identifying information (name, identifying numbers, address, telephone number), amount owed, date of service, general statement of service rendered, and unit of the University rendering service. All employees in Receivable Accounting and student services advisors may have access to those records.
- 5.2 **Internal Audit:** Employees in this unit of the University may have access to PHI to the extent necessary to fulfill their responsibilities. For example, if an employee or unit of the university is accused or suspected of violating certain HIPAA and University procedures regarding the security and privacy of PHI, this office may be involved in reviewing systems and safeguards, both in order to assess what occurred in the past and to recommend changes in the future. Also, this office may audit an area with PHI, such as Student Financial Services or the University’s Autism Center, to determine, among other things, if HIPAA regulations, as well as departmental or University policies and procedures, are being followed. In the process of conducting these reviews, the office may have access to PHI on employees, clients or patients. The Director and auditors would have primary access to those records needed to conduct the review. The support staff in that office might have some access to those records in order to assist (e.g., setting up and organizing the file; putting the file away and retrieving it, preparing letters, typing witness notes, etc.).
- 5.3 **Faculty Personnel Services:** Employees in this unit of the University may have access to PHI to the extent necessary to fulfill their responsibilities. For example, if a faculty member is accused or suspected of violating HIPAA or University procedures regarding PHI, this office would be involved in conducting an investigation and, if necessary, disciplining the employee. The Director and Assistant Directors of Faculty Personnel Services would have



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 28 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

primary access to those records needed. The support staff in that office might have some access to those records in order to assist (e.g., setting up and organizing the file; putting the file away and retrieving it, preparing letters, typing witness notes, etc.).

- 5.4 The University’s Self-funded Health Plans: Employees in this unit of the University administer the Self-funded Health plan, and they may have access to PHI of employees and their dependents to the extent necessary to fulfill their responsibilities. For example, they handle enrollment and eligibility information, claims management, and system design. All employees of this unit will have access to this information maintained by the unit.
- 5.5 The University’s Health Clinic: Employees of this department of the University may have access to PHI to the extent necessary to fulfill their responsibilities. For example, employees of the University may have access to PHI for the purpose of billing and collection fees for health services provided by the entity operating the University Health Clinic.
- 5.6 The University’s Autism Center for Diagnosis and Treatment (“Autism Center”): The Autism Center provides clinical services. The Center provides centralized scheduling and billing and other support services, and its employees may have access to PHI to the extent necessary to fulfill their responsibilities. For example, a receptionist may handle appointments; the billing persons will handle insurance and billing; support staff may provide support services (setting up files; putting the file away and retrieving it, preparing letters, typing notes, etc.). Professional faculty and staff and student clinicians provide clinical services to clients and may have access to PHI to the extent necessary to fulfill their responsibilities. They, and clinical supervisors, will have access to the full clinical record of their clients received from other health care providers and developed by them in order to conduct testing, diagnosis, treatment, and supervision of student clinicians. Student and employee clinicians may consult with other health care providers about diagnosis and treatment or provide information regarding orders and service for hearing instruments, augmentative communication devices, rehabilitation plans.
- 5.7 Controller’s Office: Employees of this department of the University may have access to PHI to the extent necessary to fulfill their responsibilities. For example, employee may be involved in auditing procedures in Student Financial Services that may involve access to information regarding payment for health services.
- 5.8 Vice-President, President, Provost Offices, Vice Provost and Support Staff: These persons and staff may have access to PHI to the extent necessary to fulfill their responsibilities. For example, access may be necessary if a faculty member or other employee is accused of HIPAA violations. The support staff might have some access in order to assist in the paperwork.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 29 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

5.9 Business Associates: The Business Associates of units within the hybrid entity may have access to PHI as described in the Business Associate Agreements.

6.0 Use, Disclosure and Requests for Entire Medical Record. The University will not use, disclose or request an entire medical record, except as allowed by 1.0 above, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request. In general, few members of the University workforce will have access to an entire clinical record. Only clinicians, health information specialists, licensed and unlicensed therapists, and student clinicians/interns will be authorized to review an entire clinical record. Such access will be limited to the records of patients/clients/employees with which the professional has a current therapeutic relationship or for whom a professional consultation has been requested. Access to the entire clinical record of these patients/clients/employees has been determined to be critical to the continuity of the patient/client/employee’s care as well as essential to diagnosis, treatment selection and the health and safety of the patient/client/employee and others.

7.0 Routine Disclosures of and Requests for PHI. The University recognizes that the need for information varies according to the duties performed by the party obtaining the information. Routine disclosures/requests are those that do not require individual review/analysis of the purpose and amount of information necessary before a disclosure/request may be made.

Each unit of the University’s Hybrid Entities shall maintain a list of the classes of persons within the workforce and the types of PHI which are routinely available to that class. The list shall be developed using a worksheet to identify disclosures routinely made by the unit by the following characteristics:

- *The type of PHI to be used or disclosed,*
- *The types of persons who will use or who will receive the disclosure,*
- *The conditions that will apply to the use or disclosure, and*
- *The purpose for which the PHI will be used or disclosed.*

8.0 Non Routine Disclosures and Requests. All non-routine disclosures will be reviewed by the Privacy Officer for the unit of the hybrid entity that houses the information in order to determine that the disclosure complies with the minimum necessary standard, in accordance with criteria contained in this Procedure.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 30 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

The following criteria will be considered when limiting the amount of PHI requested, used, or disclosed by University personnel to the minimum necessary amount:

- The use, disclosure, or request is permissible under HIPAA
- An Authorization for use, disclosure, or request has been obtained, if required
- Additional privacy restrictions do not apply, e.g., FERPA
- The patient has not objected to the disclosure and has had the opportunity to do so
- Written criteria have been established and referred to in evaluating the request
 - Does the requesting individual have the authority/right to receive the requested information?
 - Has the requesting individual clearly stated the purpose for the request, use, or disclosure of the PHI?
 - Are all of the individuals identified for whom the use or disclosure of the PHI is required?
 - Does each of them have the type of access required in order to receive it?

9.0 Reliance on Request for Disclosure as Minimum Necessary. The University will rely on requested disclosure as the minimum necessary when:

- the information is requested by another covered entity or from another entity within the University hybrid; or
- the request comes from a public official who represents that the information requested is the minimum necessary
- the information is requested by a professional who is an employee of University or a business associate of the University for the purpose of providing professional services to the University, if the person represents that the information requested is the minimum necessary; or
- documentation required by the Institutional Review Board (IRB) demonstrates that the request is only for the minimum amount of PHI necessary to accomplish the purpose of IRB review or is consistent with the informed consent of the individual who consents to participate in the research.

BREACH NOTIFICATION REQUIREMENTS

Purpose - Southeast Missouri State University (“University”) has designated itself as a hybrid entity under HIPAA. As a result, the University is mandated to establish a breach notification process applicable to unsecured protected health information (“PHI”).



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 31 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

Definition - The term ‘breach’ means the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

The term ‘breach’ does not include any unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of the University’s components or Business Associate if:

- such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the University’s components or a Business Associate; and
- such information is not further acquired, accessed, used, or disclosed by any person; or
- any inadvertent disclosure from an individual who is otherwise authorized to access PHI at a facility operated by the University’s components or Business Associate to another similarly situated individual at the same facility; and
- any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed by any person without patient authorization.

Procedures –

1.0 Discovery of Unsecured PHI.

- 1.1 In the event one of the components of the University discovers a breach of unsecured PHI, the Privacy Officer of that component or the University’s Chief Privacy Officer will notify each individual whose unsecured PHI has been, or is reasonably believed by that University component to have been, accessed, acquired, or disclosed as a result of such breach. The notification requirement applies to any unsecured PHI accessed, maintained, retained, modified, recorded, stored, destroyed, or otherwise held, used or disclosed by any component of the University. The notification requirements also apply to breaches committed by any components or Business Associates.
- 1.2 A breach will be treated as discovered by the University or a Business Associate as of the first day on which the breach is known to the University, its components or one of its Business Associates, respectively, (including any person, other than the individual committing the breach, that is an employee, officer, or other agent of the University or a Business Associate, respectively or should reasonably have been known to the University, its components or a Business Associate to have occurred).
- 1.3 In the event of a breach, the Privacy Officer of that component shall promptly notify the University’s Compliant Officer.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 32 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

2.0 Deadline for Notice. Unless otherwise specified below, the Privacy Officer of that University’s components must provide all notifications of a breach of unsecured PHI as soon as practicable and in no case later than sixty (60) calendar days after the discovery of a breach.

3.0 Methods of Notice.

3.1 Notice of a breach provided to an individual must meet the following requirements:

- 3.1.1 The notice must be written and delivered to the individual by first-class mail addressed to the individual (or the next of kin of the individual if the individual is deceased) at the individual’s (or next of kin’s) last known address. In the alternative, if the individual (or next of kin) has so specified, the notification may be delivered by electronic mail. The notification may be provided in one or more mailings as information becomes available.
- 3.1.2 In the case in which there is insufficient, or out-of-date contact information (including a phone number, email address, or any other form of appropriate communication) that precludes direct written (or, if specified by the individual, electronic) notification, a substitute form of notice must be provided, including, in the case that there are ten (10) or more individuals for which there is insufficient or out-of-date contact information, a conspicuous posting for a period (determined by the U.S. Secretary) on the home page of the Web site of the University or notice in major print or broadcast media, including major media in geographic areas where the individuals affected by the breach likely reside. Such a notice in media or web posting will include a toll-free number where an individual can learn whether or not the individual’s unsecured PHI is possibly included in the breach.
- 3.1.3 If the Privacy Officer of a component determines that immediate notification is required because of possible imminent misuse of unsecured PHI, the Privacy Officer may provide information by telephone or other means, as appropriate, in addition to the written notification required.

3.2 **Media Notice.** The Chief Privacy Officer shall be responsible to notify prominent media outlets in Missouri following the discovery of a breach of unsecured PHI, if the unsecured PHI of more than 500 residents is, or is reasonably believed to have been accessed, acquired, or disclosed during such breach.

3.3 **Notice to U.S. Secretary.** The Chief Privacy Office shall also notify the U.S. Secretary of Health and Human Services of unsecured PHI that has been acquired or disclosed in a breach. If a distinct breach was with respect to 500 or more individuals, such notice must be



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 33 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

provided immediately. If a distinct breach was with respect to less than 500 individuals, University component will maintain a log of any such breach and submit such log to the Chief Privacy Officer. Such logs must be submitted to the U.S. Secretary documenting the breaches occurring during the year involved.

4.0 Content of Notification. Regardless of the method by which notice is provided to individuals as set forth above, notice of a breach shall include, to the extent possible, the following:

- 4.1 A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
- 4.2 A description of the types of unsecured PHI that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).
- 4.3 The steps individuals should take to protect themselves from potential harm resulting from the breach.
- 4.4 A brief description of what the University is doing to investigate the breach, to mitigate losses, and to protect against any further breaches.
- 4.5 Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

5.0 Delay of Notification. Notification may be delayed if a law enforcement official determines that a notification, notice or posting would impede a criminal investigation or cause damage to national security.

SECURITY PRACTICES
HIPAA BACKGROUND AND DEFINITIONS

Background - Southeast Missouri State University (“University”) is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and regulations. Its business activities include both covered and non-covered functions. It has decided to designate itself as a Hybrid Entity.

According to the law, all University officers, employees and agents of units within the Hybrid Entity must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client. This IIHI is protected health information (PHI) and shall be safeguarded in compliance with the requirements of the security and privacy rules and standards established under HIPAA.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 34 of 52
			Classification Code: OP 01-13
	Section: ADMINISTRATION		
	Subject: PROTECTION OF HEALTH INFORMATION		

Purpose - These procedures enforce compliance with the measures that the University has implemented as a result of the HIPAA security regulations. Compliance by all units in the HIPAA Hybrid entity is necessary in order to minimize any liability the University may face as a result of this legislation. For the University, this procedure applies if the IIHI is obtained by a unit that has been defined by the University as a part of the Hybrid entity.

Definitions -

- 1.0 Electronic Protected Health Information (EPHI).** Individually identifiable health information (IIHI) that is transmitted by electronic media; maintained in electronic media, such as magnetic tape, disc, optical file; or transmitted or maintained in any other form or medium, except that it does not include IIHI in education records covered by the Family Educational Rights and Privacy Act, certain treatment records of University students as described at 20 USC 1232g(a)(4)(B)(iv), and employment records held by a covered entity in its role as employer.
- 2.0 Hybrid Entity.** A department or unit designated as within the Hybrid Definition.
- 3.0 Protected Health Information Network (PHIN).** The secured network established by the University for HIPAA protected health information. Access to this data is only available to authorized personnel who have been properly trained and granted the access appropriate to their job. EPHI may be stored on computers outside of this network, if the host system procedures are compliant with the HIPAA regulations.
- 4.0 Individually Identifiable Health Information (IIHI).** A subset of health information, including demographic information collected from a patient/client/employee, that is created or received by a health care provider, health plan or employer and relates to the past, present, or future physical or mental health or condition of a patient/client/employee, the provision of health care to a patient/client/employee, or the past, present or future payment for the provision of health care to a patient/client/employee, and which identifies the patient/client/employee, or with respect to which there is a reasonable basis to believe that the information can be used to identify the patient/client/employee.
- 5.0 Workforce Member.** A “Workforce Member” includes employees (and student employees), volunteers, trainees, and other persons whose conduct, in the performance of work for a unit in the University Hybrid entity is under the direct control of such entity, whether or not they are paid by the entity. This includes students who have access to PHI in order to satisfy a clinical experience requirement for a program of study.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 35 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

6.0 Workstation. A personal computer that has access to PHI, whether attached to the protected health information network (PHIN) or not. This definition includes personal computers in a typical work area, laptop computers used on campus or in a remote location, and wireless devices, such as PDA's that have been configured to provide access to PHI, and electronic media used by the device to store PHI.

All other terms used in this procedure have the same meaning as those terms in the Health Insurance Portability and Accountability Act of 1996, as amended and the regulations at 45 CFR Parts 160, 162, and 164.

HIPAA SECURITY MANAGEMENT PROCESS

Procedure –

1.0 Risk Analysis.

1.1 A risk analysis will be performed covering components of the University's information systems that store, process, and/or transmit EPHI. The results of the risk assessment will be used to identify changes that must be made to meet the requirements outlined by HIPAA.

2.0 Risk Management.

2.1 Risk management is an ongoing process involving the monitoring and management of risk identified during performance of the risk analysis. To ensure the confidentiality, integrity, and availability of EPHI, the University will do the following:

- 2.1.1 Implement a training program covering HIPAA Privacy Security Rules, the importance of security as it pertains to EPHI, and the University's privacy and security procedures.
- 2.1.2 Encourage workforce members to notify the security officer of known or perceived security threats.
- 2.1.3 A workforce member's access to EPHI will be controlled by their role within the University.
- 2.1.4 Security logs will be reviewed on a regular basis.
- 2.1.5 EPHI will be removed from electronic storage devices prior to their reuse or disposal.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 36 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

2.1.6 Maintain backup copies of EPHI for restoration in the event production systems become inaccessible for any reason.

2.1.7 Perform a yearly review of these procedures.

3.0 Sanction Procedures.

3.1 Any employee violating the security rules outlined in these procedures will be subject to discipline in accordance with University Business Policy 03-20 Personnel, Subject: Separations – Discipline, Separation and Dismissal.

4.0 Information System Activity Review.

4.1 Firewalls

4.1.1 Software on the firewalls will automatically monitor the operating system files for unauthorized modifications and alert the Manager of Technical Services if such a modification is detected. The firewalls will be configured to automatically respond to a number of detectable attacks.

4.2 Windows Network Logins

4.2.1 All logins to the Windows network are recorded. These logs are scanned automatically on a weekly basis for predefined events. As needed, these logs can be reviewed in depth to help identify unusual workstation and network access activity.

4.3 Banner Finance Server

4.3.1 Activity on the Banner finance server is recorded in Oracle logs. These logs are scanned automatically on a weekly basis for predefined events. As needed, these logs can be reviewed in depth to help identify unusual activity.

4.4 Data Local to the PHIN

4.4.1 Data local to the PHIN is generally processed using local applications on individual workstations. These applications operate in standalone mode and don't lend themselves to advanced features such as change logging. If and when logging features become available, their suitability for use will be evaluated.

4.4.2 Information on the source and destination of each packet entering or leaving the PHIN is logged. This and other activity logs are reviewed weekly by the Manager of Technical Services.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 37 of 52
			Classification Code: OP 01-13
	Section: ADMINISTRATION		
Subject: PROTECTION OF HEALTH INFORMATION			

HIPAA ASSIGNED SECURITY RESPONSIBILITY

Procedure –

- 1.0** Where these procedures are concerned, the Assistant Vice President for Information Technology will serve as the Security Officer. Managers of the Campus Health Clinic, Student Financial Services Office, Cashiers Office, Human Resources Office, Autism Center and Information Technology will work with the Security Officer to develop, implement, monitor, and regularly review these procedures to ensure compliance with HIPAA requirements within their respective areas.

HIPAA WORKFORCE SECURITY

Procedures –

1.0 Authorization and/or Supervision.

- 1.1 Initial access to the University's information systems is controlled by an account known as a Southeast Key. Details regarding the issuance and expiration of Southeast Keys are contained in the *Obtaining a Southeast Key (Faculty and Staff)*, *Obtaining a Southeast Key (Students)*, and *Southeast Key Expiration* sections of the *Information Technology Operations Guide*.
- 1.2 The Autism Center, Campus Health Clinic, SFS Office, Cashiers Office, Human Resources Office, and Information Technology determine appropriate access rights for each workforce member position. These rights are communicated to the appropriate Information Technology and/or financial services staff member for implementation.

2.0 Workforce Clearance Procedure.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 38 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

- 2.1 All employees must complete a background investigation prior to employment with the University in accordance with University Business Policy 03-02 Personnel, Subject: Affirmative Action/Equal Employment Opportunity.

3.0 Termination Procedures.

3.1 Network Logins

- 3.1.1 Information Technology will expire an employee's Southeast Key when notified by Human Resources or the employees' supervisor that their employment is terminating. Student Southeast Keys expire automatically based primarily on their enrollment status. Details regarding Southeast Expiration are contained in the *Southeast Key Expiration* section of the *Information Technology Operations Guide*.

3.2 Access Rights

- 3.2.1 When a Southeast Key is expired, any job-related access rights assigned to that Key are removed or disabled.
- 3.2.2 In the event an employee is also a student, their Key will not be expired but their job-related access rights will be removed or disabled.

HIPAA INFORMATION ACCESS MANAGEMENT

1.0 Access Authorization.

- 1.1 Initial access to the University's information systems is controlled by an account known as a Southeast Key. Details regarding the issuance and expiration of Southeast Keys are contained in the *Obtaining a Southeast Key (Faculty and Staff)*, *Obtaining a Southeast Key (Students)*, and *Southeast Key Expiration* sections of the *Information Technology Operations Guide*.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 39 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

- 1.2 Supervisors in the Autism Center, Campus Health Clinic, SFS Office, Cashiers Office, Human Resources Office, and Information Technology determine appropriate access rights for each position. These rights are communicated to the appropriate Information Technology and/or financial services staff member for implementation.

2.0 Access Establishment and Modification.

- 2.1 Workforce members using the PHIN: The supervisor will review the appropriateness of each workforce member and tenants' access rights on a yearly basis. Any necessary changes will be communicated to the appropriate individual for adjustment.
- 2.2 Workforce members not using the PHIN: Supervisors in the Campus Health Clinic, SFS Office, Cashiers Office, Human Resources Office, and Information Technology are responsible for notifying the appropriate Information Technology and/or financial services staff member when the job requirements of a workforce member change so appropriate security adjustments can be made. Access to the Banner financial system is reviewed on a yearly basis independent of the office supervisors.

HIPAA SECURITY AWARENESS AND TRAINING

Procedure -

1.0 Security Awareness and Training Program.

- 1.1 The director of the Autism Center will develop a training program for workforce members on the University's procedures for safeguarding EPHI as appropriate to their job function.

2.0 Security Reminders.

- 2.1 PHIN-based Workforce Members
- 2.1.1 Managers will provide regular security reminders regarding issues specific to the systems and applications utilized by workstations on the PHIN.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 40 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

2.2 Non PHIN-based Workforce Members

2.2.1 Information Technology will distribute periodic security reminders and/or updates regarding known security issues to the workforce members via the Newswire.

3.0 Protection from Malicious Software.

3.1 All workforce member workstations are required to run up-to-date antivirus software and perform routine operating system updates. Details are contained in the following sections of the *Information Technology Operations Guide*:

- Desktop Security
 - Desktop System Standards
 - Anti-Virus Software
 - Anti-Malware Software
 - Operating Systems Updates
 - Application Software Patches

4.0 Log-in Monitoring. Workstation logins to the network are logged to a database. These logs are scanned automatically on a weekly basis for predefined events. When deemed necessary, the logs can be reviewed for specific login information or examined for unusual activity.

5.0 Password Management. Details regarding password management are contained in the following sections of the *Information Technology Operations Guide*:

- Obtaining a Southeast Key
- Southeast Key Expiration
- Password Policies (length, complexity, etc.)

HIPAA SECURITY INCIDENT

Procedures -

1.0 Reporting of Security Incidents. All security incidents must be promptly reported to the Manager of Technical Services for investigation. The Manager is responsible for managing the investigation



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 41 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

as well as logging the occurrence and resolution of each reported security incident. Details are contained in the following section of the *Information Technology Operations Guide*:

- Problem Reporting
- Security Incidents

HIPAA CONTINGENCY PLAN

Procedure-

1.0 Data Backup Plan.

1.1 Workstations attached to the PHIN

1.1.1 Workforce members will manually launch backups of their workstations to disk storage media. The backups will be launched on a daily basis.

1.1.2 Offsite copies of the backups will be made on a weekly basis.

1.2 Servers not attached to the PHIN

1.2.1 Data for workforce members not attached to the PHIN is stored on central servers. An onsite copy of this data is made on a daily basis.

1.2.2 Magnetic tape copies of the backups will be rotated between offsite locations on a weekly basis.

1.2.3 Backup details are contained in the following sections of the *Information Technology Operations Guide*:

- Backups
- Banner System Backup
- Network Server Backup

1.3 Data can be restored using the same tools used to create the backups.

2.0 Disaster Recovery Plan.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 42 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

- 2.1 In the event of a disaster, an assessment will be made to determine the extent of any data loss that might have occurred.
- 2.2 If the physical facility cannot be secured, DPS will be notified.
- 2.3 In the event data loss has occurred, the appropriate managers will be notified to begin restoration operations.
- 2.4 Diagrams of the main system components will be maintained along with configurations of the equipment to support rebuilding the effected systems.

3.0 Emergency Mode Operations Plan.

- 3.1 Operations involving the PHIN
 - 3.1.1 In the event it is necessary to operate from a different location, the University will identify a physically secure location to house existing or replacement workstations.
 - 3.1.2 Information Technology will configure the appropriate networking equipment to communicate with the PHIN firewall.
 - 3.1.3 If necessary, data would be restored from backups to the workstations.
 - 3.1.4 At the time operation resumed, the standard network protections would again be in place.
 - 3.1.5 The damage to existing systems will be assessed, and vendors notified to assist in replacing or repairing any damage to the original equipment.
- 3.2 Operations not involving the PHIN
 - 3.2.1 In the event it is necessary to operate from a different location, the University will identify a physically secure location to house existing or replacement workstations.
 - 3.2.2 If necessary, data will be restored from backups to the appropriate servers.
 - 3.2.3 At the time operation resumed, the standard network protections would again be in place.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 43 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

3.2.4 The damage to existing systems will be assessed, and vendors notified to assist in replacing or repairing any damage to the original equipment.

4.0 Testing and Revision Procedure.

- 4.1 The disaster recovery and emergency operation plans will be reviewed on a yearly basis.
- 4.2 Arrangements insuring both onsite and offsite backups are accessible in a timely manner will be reviewed, as will access to necessary passwords.

5.0 Applications and Data Criticality Analysis.

- 5.1 Operations involving the PHIN
 - 5.1.1 Most of the applications used are necessary for the PHIN attached workstations to operate, and would need to be restored to provide a satisfactory operational environment.
- 5.2 Operations not involving the PHIN
 - 5.2.1 Only the University billing application is involved. This is a low volume, low risk application that has minimal impact on normal operations.

HIPAA EVALUATION

Procedure -

- 1.0 The Assistant Vice President, Information Technology will initiate an annual review of the policies and procedures affecting the security of electronic protected health information. Any changes deemed necessary will be made and documented in cooperation with the affected department.

HIPAA BUSINESS ASSOCIATE CONTRACTS AND OTHER ARRANGEMENTS

Purpose -

The Southeast Missouri State University (“University”) will enter into a business associate agreement with each entity or person who is not a component of the University and who will perform (or assist in the



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 44 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

performance of) any activity which requires the University to disclose or allow access to protected health information (PHI) to such person or entity (“Business Associate”). The University will make reasonable efforts to ensure that Business Associate uses and discloses PHI only in accordance with the terms and conditions of the business associate agreement. To the extent that the University becomes aware of a violation of any business associate agreement, the University will notify the Compliant Officer, who will investigate whether a breach has occurred.

Procedure -

1.0 Existing Contract with Business Associates.

- 1.1 At the outset of implementation of the University’s Privacy Rule compliance program, the privacy officer (PO) will create an inventory of all Business Associates with whom the University has existing service agreements.
- 1.1 The Chief Privacy Officer will enter into valid business associate agreements with any and all Business Associates with whom there is no such agreement in place. The business associate agreement entered into with such Business Associates must incorporate by reference all existing service agreements the University has with that Business Associate.
- 1.2 PO will keep a record of this Agreement on file in the University.

2.0 New Service Agreements.

- 2.1 Prior to entering into any service agreement which will require the University to disclose PHI, the PO will notify the Chief Privacy Officer of new service agreements that require a business associates agreement.
- 2.2 If the University has not entered into a business associate agreement with the service provider, the service provider must execute the business associate agreement, in a form acceptable to the University, before the service agreement is executed.
- 2.3 Once the business associate agreement has been executed by the service provider, the original business associate agreement must be given to PO to place in the University’s “Business Associate Agreement” file. A copy may be affixed to the service agreement.

HIPAA FACILITY ACCESS CONTROLS

Procedures -



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 45 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

1.0 Contingency Operations.

- 1.1 Key staff members are already authorized to access many locations that might be used as emergency operation locations. For others, the University has a key approval process in place that can provide keys to other staff members as necessary.

2.0 Facility Security Plan.

- 2.1 The firewalls (and backups) will be located in environmentally controlled remote locations protected by appropriate locks and electronic security systems.
- 2.2 Offices will be kept locked outside of normal office hours.
- 2.3 The Cashiers office will be kept locked at all times and protected by an electronic security system.
- 2.4 The servers and network equipment will be located in an environmentally controlled room protected with appropriate locks and a security system.

3.0 Access Control and Validation Procedures.

- 3.1 Keys are issued by Facilities Management based on written authorization by supervisors and/or building coordinators.
- 3.2 Only authorized IT staff members are normally permitted to enter the room where the University's servers, core network equipment, firewalls, and backups are stored. If visitors are allowed, they must be accompanied by a staff member.
- 3.3 The Cashiers office is kept locked at all times, and visitors must request permission to enter the office.
- 3.4 Access to software is controlled based on job responsibilities and account authorizations as requested by the supervisor.
- 3.5 Further protection is provided by login accounts and passwords.

4.0 Maintenance Records.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 46 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

- 4.1 Facilities Management will maintain a work order system that logs physical modifications to each facility.

HIPAA WORKSTATION USE

Procedure –

1.0 Proper functions to be performed.

- 1.1 Workforce members are to use University provided workstations to perform their assigned job functions. These may include accessing, storing, and updating EPHI, as well as billing, scheduling, and other standard office duties as assigned.

2.0 Functions not to be performed.

- 2.1 Workforce members must only access EPHI on a need to know basis related to their job functions.
- 2.2 EPHI must not be downloaded and stored on a workstation unless required to complete a job function. The workforce member's supervisor must authorize such use of EPHI.
- 2.3 Electronic media containing EPHI must not be removed from the work location without appropriate authorization.

3.0 Additional requirements for PHIN attached workstations.

- 3.1 Workforce members must not download and/or install unauthorized applications on their workstations.
- 3.2 No unauthorized workstation, communication, or storage device may be attached to the network without appropriate authorization.
- 3.3 Only files received from recognized sources are to be accessed on these workstations.

4.0 Manner in which functions are to be performed.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 47 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

- 4.1 All access must comply with the *Information Technology and Network Systems Acceptable Use Policy and Procedures*, located at <http://www6.semo.edu/infotech/policies.asp> .
- 4.2 Workforce members will use their uniquely assigned Southeast Key when logging in to University information systems.
- 4.3 Workforce members will be responsible for protecting the security of their Southeast Keys.
- 4.4 Workforce members will not share their Southeast Keys.
- 4.5 Workforce members will log off or lock their keyboards before leaving a workstation unattended.

5.0 Physical attributes of workstation surroundings.

- 5.1 Workstations must be located in physically securable locations.
- 5.2 Displays must be located in such a way that unintentional viewing by the public is avoided.

HIPAA WORKSTATION SECURITY

Procedures -

1.0 Locked Offices and Areas.

- 1.1 Offices will be kept locked outside of business hours.
- 1.2 Both the Cashiers Office and Information Technology computer room will be kept locked at all times.

2.0 Desktop Workstations. Whenever possible, desktop workstations will be located in areas restricted to workforce members.

3.0 Portable Computing Devices.

- 3.1 Portable computing devices such as laptops and smartphones used to access EPHI must be kept in a secure location when not in use.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 48 of 52
			Classification Code: OP 01-13
	Section: ADMINISTRATION		
	Subject: PROTECTION OF HEALTH INFORMATION		

- 3.2 Portable computing devices such as laptops or portable storage units must use encryption to store EPHI.
- 3.3 Portable computing devices must be configured with password protection.

HIPAA DEVICE AND MEDIA CONTROLS

Procedures -

1.0 Disposal.

- 1.1 The University's surplus property procedures requiring that hard drives in personal computers be securely wiped or physically destroyed when a computer is permanently taken out of service must be followed.
- 1.2 Electronic devices such as cell phones and PDAs must be securely erased or destroyed when they are no longer in use.

2.0 Media Re-use.

- 2.1 Only media that can be securely erased may be reused. Media that cannot be securely erased and is no longer needed must be destroyed.

3.0 Accountability.

- 3.1 Departments must file Change of Accountability forms with Inventory Control when a PC is transferred to a different location or another department.
- 3.2 Only workstations inside the Autism Center should store EPHI on external electronic media such as CDs, DVDs, or portable storage units. Such media must not leave the Autism Center unless it is in the possession of an Autism Center staff member that has been authorized to do so.
- 3.3 Workstation and server backups must be controlled, rotated on a regular schedule, and kept in secure storage when not in use.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 49 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

- 3.4 Employees are personally responsible for implementing safeguards to protect the confidentiality, integrity, and availability of patient/client information on mobile devices and media.

4.0 Data Backup and Storage.

- 4.1 Information Technology staff must backup hard drives before performing work on equipment that might result in data loss.

HIPAA ACCESS CONTROL

Procedures -

1.0 Unique User Identification.

- 1.1 All workforce members will be assigned a unique user identifier as described in the *Obtaining a Southeast Key* section of the *Information Technology Operations Guide*.

2.0 Emergency Access Procedure.

- 2.1 Operations involving the PHIN
- 2.1.1 In the event it is necessary to operate from a different location, the University will identify a physically secure location to house existing or replacement workstations.
 - 2.1.2 Information Technology will configure the appropriate networking equipment to communicate with the PHIN firewall.
 - 2.1.3 If necessary, data will be restored from backups to the workstations.
 - 2.1.4 At the time operation resumed, the standard network protections would again be in place.
 - 2.1.5 The damage to existing systems will be assessed, and vendors notified to assist in replacing or repairing any damage to the original equipment.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 50 of 52
	Section: ADMINISTRATION		Classification Code: OP 01-13
	Subject: PROTECTION OF HEALTH INFORMATION		

2.2 Operations not involving the PHIN

- 2.2.1 In the event it is necessary to operate from a different location, the University will identify a physically secure location to house existing or replacement workstations.
- 2.2.2 If necessary, data will be restored from backups to the appropriate servers.
- 2.2.3 At the time operation resumed, the standard network protections would again be in place.
- 2.2.4 The damage to existing systems will be assessed, and vendors notified to assist in replacing or repairing any damage to the original equipment.

3.0 Automatic Logoff.

- 3.1 Workstations will be set to automatically lock the keyboard after 15 minutes of inactivity.
- 3.2 The Banner Finance system will timeout after no more than 15 minutes of inactivity.

4.0 Encryption and Decryption.

- 4.1 PHIN based operations
 - 4.1.1 The VPN (virtual private network) connection to the vendor providing insurance billing will be encrypted using IPSEC (Internet Protocol security).
 - 4.1.2 Workstation backups are encrypted.
 - 4.1.3 Encrypted folders will be created on workstations to contain EPHI.

HIPAA AUDIT CONTROLS

Procedures -

- 1.0 All traffic entering and exiting the PHIN's network firewall will be logged. In addition, OSSEC (Open Source Security) will run on the firewall and logs any changes made there.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 51 of 52
			Classification Code: OP 01-13
	Section: ADMINISTRATION		
	Subject: PROTECTION OF HEALTH INFORMATION		

- 2.0 When changes are made to billing data stored in the University’s financial system, they are archived in logs that are retained for approximately four weeks.
- 3.0 The Southeast Keys of workforce members logging into the campus network will be logged.
- 4.0 The Southeast Keys of workforce members logging into Internet Native Banner will be logged.

HIPAA INTEGRITY

Procedures -

- 1.0 Multiple generations of backups will be maintained. In the event data is suspected of having been corrupted or modified, an earlier version of the data will be examined from a backup copy.

HIPAA TRANSMISSION SECURITY

Procedures -

1.0 Integrity Controls.

- 1.1 The VPN connection to the vendor providing insurance billing must be encrypted.
- 1.2 Where possible, if EPHI is displayed via a web page, SSL (secure sockets layer) connection should be used.
- 1.3 Workforce members may be permitted to access the network remotely, but only via a VPN or remote desktop. Such access to the PHIN is discouraged.
- 1.4 Only network communications equipment authorized by Information Technology may be connected to the network

2.0 Encryption.

- 2.1 Where appropriate, VPN, remote desktop, or SSL connections should be used.



BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 8/10	Revision Date:	Page: 52 of 52
			Classification Code: OP 01-13
	Section: ADMINISTRATION		
Subject: PROTECTION OF HEALTH INFORMATION			

- 2.2 Data transiting the internal campus network cannot be encrypted due to the variety of applications that must interact and the lack of standards for doing so.

Southeast Missouri State University reserves the right to make exceptions to, modify or eliminate these guidelines. This document supersedes all previous guidelines relative to its subject.