UNIVERSITY OF SOUTHERN INDIANA
Kinney College of Nursing and Health Professions

HIPAA Compliance Policy

Health Information Privacy Policies and Procedures

Adopted Effective: April 14, 2003. Revised: January 2014; January 2021; June 2026

These Health Information Privacy Policies and Procedures implement the Kinney College of Nursing and Health Professions' obligations to protect the privacy of individually identifiable health information that we create, receive or maintain.

We implement these Health Information Privacy Policies and Procedures to protect the interests of our clients/patients and workforce; and to fulfill our legal obligations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), its implementing regulations at 45 CFR Parts 160 and 164 (65 Fed. Reg 82462 [Dec. 28, 2000]) ("Privacy Rules"), as amended (67 Fed. Reg. 53182 [Aug. 14, 2002]), and state law that provides greater protection or rights to individuals than the Privacy Rules.

As a member of our workforce or as a third-party person or entity providing us services ("Business Associate"), you are obligated to follow these Health Information Privacy Policies and Procedures faithfully. Failure to do so can result in disciplinary action, including termination of employment or dismissal from your educational program. In addition, federal penalties for privacy violations can result in fines up to $250,000 and prison sentences of up to 10 years. The workforce includes any individual whose work performance at the University of Southern Indiana Kinney College of Nursing and Health Professions (the "College"), is under the direct control of the College. The workforce defined as, but is not limited to, all clinical, administrative, and academic full-time, part-time, temporary and contract employees, as well as volunteers and students.

These Policies and Procedures address the basics of HIPAA and the Privacy Rules that apply to the College. They do not attempt to cover everything in the Privacy Rules. The Policies and Procedures of the College utilize the terms "individual" to refer to prospective clients/patients, clients/patients of record, former clients/patients, those whose health information is retained by the College, or the authorized representatives of these identified individuals.

On a yearly basis, every member of the College workforce must participate in online HIPAA education and testing which is accessed through the College website, USI.edu/health/faculty-staff-resources/hipaa-module. The HIPAA quiz must be completed with a score of 75% or higher. If a score of 75% or higher is not achieved the quiz must be repeated until a passing score is achieved.

If you have questions or doubts about any use or disclosure of individually identifiable health information or about your obligations under these Health Information Privacy Policies and Procedures, the Privacy Rules or other federal or state law, consult the Kinney College Infection Control and HIPAA Committee at 812-464-1151 before you act.

1. General Rule: No Use or Disclosure

The College must not use or disclose protected health information (PHI), except as these Privacy Policies and Procedures permit or require.

2. Acknowledgement and Optional Consent

The College will make a good faith effort to obtain a written Acknowledgement of receipt of our Notice of Privacy Practices from an individual before we use or disclose their protected health information ("PHI") for

treatment, to obtain payment for that treatment, or for our healthcare operations ("TPO").

The College's use or disclosure of PHI for payment activities and healthcare operations may be subject to a "need to know" basis.

Consent from an individual will be obtained before use or disclosure of PHI for TPO purposes – in addition to obtaining an Acknowledgement of receipt of our **Notice of Privacy Practices**.

a) **Obtaining Consent** - Upon the individual's enrollment in a College education program, employment in the College, or first visit as a client/patient (or next visit if already a client/ patient), consent for use and disclosure of the individual's PHI for treatment, payment and healthcare operations will be requested. The consent form will be retained in the individual's file.
b) **Exceptions** - Consent does not need to be obtained in emergency treatment situations; when treatment is required by law; or when communications barriers prevent consent.
c) **Consent Revocation** - An individual from whom consent is obtained may revoke it at any time by written notice. The revocation will be included in the individual's file.
d) **Applicability** - Consent for use or disclosure of PHI should not be confused with informed consent for client/patient treatment.

3. Oral Agreement

The College may use or disclose an individual's PHI with the individual's oral agreement. The College may use professional judgment and our experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up health records, dental/medical supplies, radiographs or other similar forms of PHI.

4. Permitted Without Acknowledgement, Consent Authorization or Oral Agreement

The College may use or disclose an individual's PHI in certain situations without authorization or oral agreement.

a) **Verification of Identity** – The College will always verify the identity and authority of any individual's personal representative, government or law enforcement official, or other person, unknown to us, who requests PHI before we will disclose the PHI to that person.

   The College will obtain appropriate identification and evidence of authority. Examples of appropriate identification include photographic identification card, government identification card or badge and appropriate document on government letterhead. The College will document the request for PHI and how we responded.

b) **Uses, Disclosures or Access Permitted under this Section 4** – Except where specifically authorized by the individual or appropriate representative or as required by law, protected individual information may only be used, disclosed or accessed by:
   i. The individual or the individual's personal representative
   ii. The College workforce members who **require** access to protected individual information as defined by their job role. Reasons for which protected individual information are generally needed include:
      - delivery and continuity of the individual's treatment or care,
      - educational or research purposes, or
      - college business or operational purposes
   iii. Non-College healthcare providers who need such information for the individual's care
   iv. Third-party payers or non-College healthcare providers for payment activities of such entities
   v. Business associates from whom the College has received written assurance that protected individual information will be appropriately safeguarded

The College may use or disclose PHI in the following types of situations, provided procedures specified in the Privacy Rules are followed:

1. For public health activities;
2. As necessary to receive payment for any health care provided;
3. To health oversight agencies;
4. To coroners, medical examiners and funeral directors;
5. To employers regarding work-related illness or injury;
6. To the military;
7. To federal officials for lawful intelligence, counterintelligence, and national security activities;
8. To correctional institutions regarding inmates;
9. In response to subpoenas and other lawful judicial processes;
10. To law enforcement officials;
11. To report abuse, neglect, or domestic violence;
12. As required by law;
13. As part of research projects; and
14. As authorized by state worker's compensation laws.

5. Required Disclosures

The College will disclose protected health information (PHI) to an individual (or to the individual's personal representative) to the extent that the individual has a right of access to the PHI); and to the U.S. Department of Health and Human Services (HHS) on request for complaint investigation or compliance review. The College will document each disclosure made to HHS.

6. Minimum Necessary

All College workforce members must access and use protected individual information on a "need to know" basis as defined by their job role. In addition, when using or disclosing an individual's information the amount of information used or disclosed should be limited to the minimum amount necessary to accomplish the intended purpose. When requesting an individual's information from other healthcare providers, staff should limit the request to the minimum amount necessary. Minimum necessary expectation does not generally apply to situations involving treatment or clinical evaluation.

7. Business Associates

The College will obtain satisfactory assurance in the form of a written contract that our Business Associates will appropriately safeguard and limit their use and disclosure of the protected health information (PHI) we disclose to them.

These Business Associate requirements are not applicable to our disclosures to a healthcare provider for treatment purposes. The Business Associate Contract Terms document contains the terms that federal law requires be included in each Business Associate Contract.

a) **Breach by Business Associate** - If the College learns that a Business Associate has materially breached or violated its Business Associate Contract with us, we will take prompt and reasonable steps to ensure the breach or violation is corrected.

If the Business Associate does not promptly and effectively correct the breach or violation, we will terminate our contract with the Business Associate or, if contract termination is not feasible, report the Business Associate's breach or violation to the U.S. Department of Health and Human Services (HHS).

8. Notice of Privacy Practices

The College will maintain a Notice of Privacy Practices as required by the Privacy Rules.

a) **Our Notice** - The College will use and disclose PHI only in conformance with the contents of our Notice of Privacy Practices. We will promptly revise a Notice of Privacy Practices whenever there is a material change to our uses or disclosures of PHI due to legal duties, to an individual's rights, or

to other privacy practices that render the statements in that Notice no longer accurate.

b) **Distribution of Our Notice** –The College will provide our Notice of Privacy Practices to each individual who submits health information to the College.

c) **Acknowledgement of Notice** –The College will make a good faith effort to document receipt of the Notice of Privacy Practices.

9. Individual's Rights

The College workforce will honor the rights of individuals regarding their PHI.

a) **Access** – The College will permit individuals or workforce members access to their own PHI we or our Business Associates maintain. No PHI will be withheld from an individual unless we confirm that the information may be withheld according to the Privacy Rules. We may offer to provide a summary of the health information. The individual must agree in advance to receive a summary and to any fee we will charge for providing the summary.

b) **Amendment** – Individuals and workforce members have the right to request to amend their own PHI and other records for as long as the College maintains them.

The College may deny a request to amend PHI or records if: (a) we did not create the information (unless the individual provides us a reasonable basis to believe that the originator is not available to act on a request to amend}; (b) we believe the information is accurate and complete; or (c) we do not maintain the information.

The College will follow all procedures required by the Privacy Rules for denial or approval of amendment requests. We will not, however, physically alter or delete existing notes. We will inform the individual or workforce member when we agree to make an amendment. We will contact any individuals whom the individual or workforce member requests we alert to any amendment to the PHI. We will also contact any individuals or entities of which we are aware that we have sent erroneous or incomplete information and who may have acted on the erroneous or incomplete information to the detriment of the individual or workforce member.

When we deny a request for an amendment, we will mark any future disclosures of the contested information in a way acknowledging the contest.

c) **Disclosure Accounting** – Individuals or workforce members have the right to an accounting of certain disclosures the College made of their PHI within the 6 years prior to their request. Each disclosure we make, that is not for treatment payment or healthcare operations, must be documented showing the date of the disclosure, what was disclosed, the purpose of the disclosure, and the name and (if known) address of each person or entity to whom the disclosure was made. Documentation must be included in the individual's or workforce member's record.

The College is not required to account for disclosures we made: (a) before April 14, 2003; (b) to the individual (or the individual's personal representative); (c) to or for notification of persons involved in an individual's healthcare or payment for healthcare; (d) for treatment, payment, or healthcare operations; (e) for national security or intelligence purposes; (f) to correctional institutions or law enforcement officials regarding inmates; or (g) according to an Authorization signed by the patient or the patient's representative; (h) incident to another permitted or required use disclosure.

The College will charge a reasonable, cost-based fee for every accounting that is requested more frequently than every 12 months, provided that the College has informed the individual in advance of the fee and provides the individual with an opportunity to modify or withdraw the request.

d) **Restriction on Use or Disclosure** – Individuals have the right to request the College to restrict use or disclosure of their PHI, including for treatment, payment or healthcare operations. The College has no obligation to agree to the request, but if we do, we will comply with our agreement (except in an appropriate dental/medical emergency).

We may terminate an agreement restricting use or disclosure of PHI by a written notice of termination to the individual. We will document any such agreed to restrictions.

e) **Alternative Communications** – Individuals have the right to request the use of alternative means or alternative locations when communicating PHI to them. The College will accommodate an individual's request for such alternative communications if the request is in writing and deemed reasonable by the College. The College will inform the individual of our decision to accommodate or deny such a request.

10. Staff Training and Management, Complaint Procedures, Data Safeguards, Administrative Practices

a) **Staff Training and Management Training** – The College will train all members of our workforce in these Privacy Policies & Procedures, as necessary and appropriate for them to carry out their functions. Workforce members will complete privacy training prior to having access to PHI and on a yearly basis thereafter. The College will maintain documentation of workforce training.

b) **Violation Levels and Disciplinary /Corrective Actions** – Below are examples of privacy and security violations and the minimum disciplinary/ corrective actions that will be taken. **Depending on the nature, violations at any level may result in more severe action or termination.**

Level I: Carelessness
Examples:
- Failing to log off/close or secure a computer with *protected health information* displayed
- Leaving a copy of *protected health information* in a non-secure area
- Discussing *protected health information* in a non-secure area (lobby, hallway, elevator)

Minimum Disciplinary/Corrective Action:
- Staff: verbal warning with documentation by immediate supervisor
- Students: verbal warning with documentation by clinical faculty and/or program chair
- Faculty: verbal warning with documentation by program chair or dean

Level II: Undermining Accountability
Examples:
- Sharing ID/password with another coworker or encouraging a coworker to share ID/password
- Repeated violation of previous level

Minimum Disciplinary/Corrective Action:
- Staff: written performance counseling by immediate supervisor
- Students: written performance counseling by clinical faculty and/or program chair
- Faculty: written performance counseling by program chair or dean

Level III: Unauthorized Access
Examples:

- Accessing or allowing access to *protected health information* without a legitimate reason
- Repeated violation of previous level

Minimum Disciplinary/Corrective Action:

- Staff: final performance counseling by immediate supervisor
- Students: final performance counseling and program chair determines outcome
- Faculty: final performance counseling and program chair or dean determines outcome

Level IV: Blatant Misuse
Examples:

- Accessing or allowing access to *protected health information* without a legitimate reason and disclosure of abuse of the *protected health information*
- Using protected patient information for personal gain
- Tampering with/or unauthorized destruction of information
- Repeated violation of previous level

Minimum Disciplinary/Corrective Action:

- Staff: initiate termination of employment
- Students: initiate dismissal from educational program in line with College procedures
- Faculty: initiate termination from employment in line with College procedures

c) **Complaints** – The College will implement procedures for individuals to complain about compliance with our Privacy Policies and Procedures or the Privacy Rules. The College will also implement procedures to investigate and resolve such complaints.

The complaint form can be used by the individual to lodge the complaint. Each complaint received must be referred to the College Compliance Committee immediately for investigation and resolution. We will not retaliate against any individual or workforce member who files a complaint in good faith.

d) **Data Safeguards** – The College will strengthen these Privacy Policies and Procedures with such additional data security policies and procedures as are needed to have reasonable and appropriate administrative, technical, and physical safeguards in place to ensure the integrity and confidentiality of the PHI we maintain.

The College will take reasonable steps to limit incidental uses and disclosures of PHI made according to an otherwise permitted or required use or disclosure.

e) **Documentation and Record Retention** – The College will maintain in written or electronic form all documentation required by the Privacy Rules for six years from the date of creation or when the document was last in effect, whichever is greater.

f) **Privacy Policies and Procedures** – The Kinney College of Nursing and Health Professions Infection Control and HIPAA Committee will make any needed changes to the Privacy Policies and Procedures.

g) **State Law Compliance** – The College will comply with state privacy laws that provide greater protections or rights to individuals than the Privacy Rules.

h) **HHS Enforcement** – The College will give the U.S. Department of Health and Human Services (HHS) access to our facilities, books, records, accounts, and other information sources (including individually identifiable health information without individual authorization or notice) during normal business hours (or at other times without notice if HHS presents appropriate lawful administrative or judicial

process). We will cooperate with any compliance review or complaint investigation by HHS, while preserving the rights of the College.

i) **Designated Personnel** – The Dean of the Kinney College of Nursing and Health Professions will serve as Privacy Officer and contact person for the College

Notice of Privacy Practices

This notice describes how health information about you may be used and disclosed and how you can get access to this information.

Please review it carefully. The privacy of your health information is important to us.

Our Legal Duty

We are required by applicable federal and state law to maintain the privacy of your health information. We are also required to give you this Notice about our privacy practices, our legal duties, and your rights concerning your health information. We must follow the privacy practices that are described in this Notice while it is in effect. This Notice takes effect April 14, 2003, and will remain in effect until we replace it.

We reserve the right to change our privacy practices and the terms of this Notice at any time, provided such changes are permitted by applicable law. We reserve the right to make the changes in our privacy practices and the new terms of our Notice effective for all health information that we maintain, including health information we created or received before we made the changes. Before we make a significant change in our privacy practices, we will change this Notice and make the new Notice available upon request.

You may request a copy of our Notice at any time. For more information about our privacy practices, or for additional copies of this Notice, please contact us using the information listed at the end of this Notice.

Uses and Disclosures of Health Information

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

Treatment: We may use or disclose your health information to a physician or other healthcare provider providing treatment to you.

Payment: We may use and disclose your health information to obtain payment for services we provide to you.

Healthcare Operations: We may use and disclose your health information in connection with our healthcare operations. Healthcare operations include quality assessment and improvement activities, developing clinical guidelines, reviewing the competence or qualifications of healthcare professionals, evaluating practitioner and provider performance, conducting training programs, accreditation, certification, licensing or credentialing activities.

Your Authorization: In addition to our use of your health information for treatment, payment, or healthcare operations, you may give us written authorization to use your health information or to disclose it to anyone for any purpose. If you give us an authorization, you may revoke it in writing at any time. Your revocation will not affect any use or disclosures permitted by your authorization while it was in effect. Unless you give us a written authorization, we cannot use or disclose your health information for any reason except those described in this Notice.

To Your Family and Friends: We must disclose your health information to you, as described in the Client Rights section of this Notice. We may disclose your health information to a family member, friend or other person to the extent necessary to help with your healthcare or with payment for your healthcare, but only if you agree that we may do so or as described in the Person Involved in Care section.

Persons Involved In Care: We may use or disclose health information to notify or assist in the notification of (including identifying or locating) a family member, your personal representative or another person responsible for your care, of your location, your general condition, or death. If you are present, then prior to use or disclosure of your health information, we will provide you with an opportunity to object to such uses or

disclosures. In the event of your incapacity or emergency circumstances, we will disclose health information based on a determination using our professional judgment disclosing only health information that is directly relevant to the person's involvement in your healthcare. We will also use our professional judgment and our experience with common practice to make reasonable inferences of your best interest in allowing a person to pick up filled prescriptions, medical supplies, x-rays, or other similar forms of health information.

Marketing Health-Related Services: We will not use your health information for marketing communications without your written authorization.

Required by Law: We may use or disclose your health information when we are required to do so by law.

Abuse or Neglect: We may disclose your health information to appropriate authorities if we reasonably believe that you are a possible victim of abuse, neglect, or domestic violence or the possible victim of other crimes. We may disclose your health information to the extent necessary to avert a threat to your health or safety or the health or safety of others.

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

Appointment Reminders: We may use or disclose your health information to provide you with appointment reminders (such as voicemail messages, postcards, or letters).

Client Rights

Access: You have the right to look at or get copies of your health information, with limited exceptions. You may request that we provide copies in a format other than photocopies. We will use the format you request unless we cannot practicably do so. (You must make a request in writing to obtain access to your health information. You may obtain a form to request access by using the contact information listed at the end of this Notice. We will charge you a reasonable cost-based fee for expenses such as copies and staff time.

You may also request access by sending us a letter to the address at the end of this Notice. If you request copies, we may charge a cost-based fee to cover the cost of processing. If you request an alternative format, we may charge a cost-based fee for providing your health information in that format. If you prefer, we will prepare a summary or an explanation of your health information for a fee.)

Disclosure Accounting: You have the right to receive a list of instances in which we or our business associates disclosed your health information for purposes, other than treatment, payment, healthcare operations and certain other activities, for the last 6 years, but not before April 14, 2003. If you request this accounting more than once in a 12-month period, we may charge you a reasonable, cost-based fee for responding to these additional requests.

Restriction: You have the right to request that we place additional restrictions on our use or disclosure of your health information. We are not required to agree to these additional restrictions, but if we do, we will abide by our agreement (except in an emergency).

Alternative Communication: You have the right to request that we communicate with you about your health information by alternative means or to alternative locations. (You must make your request in writing.) Your request must specify the alternative means or location and provide satisfactory explanation how payments will be handled under the alternative means or location you request.

Amendment: You have the right to request that we amend your health information. (Your request must be in

writing, and it must explain why the information should be amended.) We may deny your request under certain circumstances.

Electronic Notice: If you receive this Notice on our Web site or by electronic mail (e-mail), you are entitled to receive this Notice in written form.

Notice of Breach: You have the right to be notified following a breach of your unsecured protected health information and we will notify you in accordance with applicable law.

Questions and Complaints

You may complain to us or to the Secretary of Health and Human Services if you believe your privacy rights have been violated by us. You may file a complaint with us by notifying our privacy contact of your complaint. We will not retaliate against you for filing a complaint.

This notice was published and becomes effective on or before April 14, 2003.
Revised: January 2014; January 2021; June 2026

Privacy Contact:
Dr. Julie McCullough, Dean of the Kinney College of Nursing and Health Professions
Address: 8600 University Bouvard. Evansville, IN 47712
Telephone: 812-465-1151