HIPAA Policy for Notre Dame Researchers

The University of Notre Dame has developed an information technology environment (the "System") consistent with the Privacy Rule and Safeguards Rule of the Health Information Portability and Accountability Act (HIPAA) in order to support the needs of University of Notre Dame research groups and personnel ("System Users") who store, analyze, and transmit protected health information (PHI).

Consistent with the HIPAA requirements that have been adopted for the operation of the System, the University, and the System Users, will be responsible to ensure that:

- Written policies and procedures will be maintained and implemented to comply with the HIPAA Security and Privacy rules and documentation relating to the management of HIPAA compliance program associated with their specific program will also be maintained.

- Appropriate administrative, technical, and physical safeguards will be maintained to protect the privacy of protected health information (PHI), both at the System level as provided by the University and also as appropriate for the requirements of the specific program.

- Appropriate steps to dispose of any documents, film, or hard copy materials that contain protected health information when retention requirements have been fulfilled will be taken. *Source: 45 CFR 164.530(c), 45 CFR 164.530(i), 45 CFR 154.530(j), and 45 CFR 164.316*

- Workforce members who do not comply with Notre Dame Research's HIPAA environment policies and associated procedures will be educated and sanctioned appropriately. *Source: 45 CFR 164.530(e)*

- There is appropriate cooperation with the Secretary of the United States Department of Health and Human Services if the Secretary investigates whether the University or any of its System Users, contractors, or agents associated with the research program has complied with the HIPAA requirements. *Source: 45 CFR 160.310*

- There is no retaliation against or intimidation of any person who files a complaint or provides information regarding a potential HIPAA violation, in compliance with the University's anti-harassment and anti-retaliation policies. *Source*: *45 CFR 160.316*

- Only the minimum necessary protected health information (PHI) will be used, disclosed, or requested to accomplish the intended purpose of the use, disclosure, or request. *Source: 45 CFR 164.502(b), 164.514(d)(1), U.S.C. 17935*

- All complaints regarding privacy practices involving University researchers or research projects utilizing PHI are reported to the Research HIPAA Privacy Officer. The Privacy Officer shall investigate all privacy-related complaints. *Source: 45 CFR 164.530(a), 45 CFR 164.530(d)*

- The University will, as appropriate and when required by HIPAA, enter into Business Associate Agreements with Covered Entities when Notre Dame falls within the definition of a Business Associate and Notre Dame will also enter into Business Associate Agreements with all applicable subcontractors. *Source: 45 CFR 164.308(b)*

- Individuals (or their personal representative) whose PHI is maintained in the System have the right to request access to his or her own PHI. *Source: 45 CFR 164.524*

- When appropriate and consistent with the privacy rights of the individual whose PHI is maintained in the System, an individual's personal representative will be treated as the individual with respect to the individual's rights under HIPAA. For example, accounting of disclosures, right to access to PHI, and amendment of PHI. *Source: 45 CFR 164.502(g)*

- All disclosures for purposes other than treatment, payment, and healthcare operations that are not specifically authorized by the patient/individual whose information is maintained in the System (or an IRB in approved research projects) shall be documented, and an individual whose PHI is maintained in the System shall be able to request an accounting of all such disclosures.

- Disclosures required under each Business Associate Agreement or Data Use Agreement entered with the University of Notre Dame related to the System will be documented and accounted for. *Source: 45 CFR 164.528*

- An individual's protected health information (PHI) in a Designated Record Set will be evaluated for amendment, and amended as appropriate, at the request of the Covered Entity or individual whose PHI is maintained in the System. *Source: 45 CFR 164.526*

- All applicable members of the workforce associated with the System will receive training to comply with HIPAA requirements and the University of Notre Dame's HIPAA policies associated with the System. All new applicable workforce members will receive training during the orientation process

or before receiving access to any protected health information. All current applicable workforce members will receive training every other year and anytime there is a significant change to Notre Dame's HIPAA policies related to the System. *Source: 45 CFR 164.530(b)*

HIPAA Compliance Administrative Procedures

Policy Review / Maintenance Cycle

The Research HIPAA Privacy Officer will review on an annual basis current HIPAA policies and training materials related to compliance with applicable data use agreements and HIPAA privacy / security requirements. Any required changes to policies, trainings, or associated documentation will be tracked, retained, and communicated to campus data stewards.

Document Retention

A centralized repository will be maintained by Notre Dame Research to house all applicable HIPAA compliance documentation. Documents will be maintained for six years from their initial creation / adoption with all changes tracked and retained. Documents will be adequately protected and backed up (when in digital form). Documents that will be retained:

- ✓ Data use agreements with external partners and all applicable contact information
- ✓ HIPAA related policies and procedures
- ✓ HIPAA training materials and training records for applicable staff and collaborators
- ✓ Security risk analysis documentation
- ✓ Tracking of all inadvertent disclosure events

Privacy Violation, Compliant and ePHI Access Inquiry

The HIPAA Research Privacy Officer will investigate all complaints of misconduct or access violations involving HIPAA covered research data. The HIPAA Research Privacy Officer will work with assisting departments such as OIT, CRC, Legal, Research Administration, and Human Resources to determine if an access violation or inadvertent disclosure has occurred. If applicable, the HIPAA Research Privacy Officer or their delegate in consultation with the Office of General Counsel will promptly notify the external data provider per the stipulations of the governing data use agreement of the potential data disclosure.

Notification timeliness may vary depending on data provider. The outcome of investigation will be documented and retained. In general, it is the University of Notre Dame's practice not to communicate directly with subjects whose data may be part of a research data set. If the HIPAA Privacy Officer for

Research receives an inquiry from a potential patient or a patient's personal representative regarding their personally identifiable health information, the HIPAA Research Privacy Officer will proxy that inquiry to the external data provider within 30 days for guidance and processing. If a subject complains about their rights or welfare in a research study, the Research HIPAA Privacy Officer may request information from the patient regarding their complaint for the purpose of Institutional Review Board (IRB) review.

Documenting of Data Stewards

The HIPAA Research Privacy Officer or their delegate will maintain a list of all data stewards or any other person responsible for authorizing access to PHI for their respective research programs. A list of data stewards and their contact information will be maintained and accessible via the Notre Dame Research Compliance webpage, located at https://research.nd.edu/our-services/resource-library/ data-stewards-list/. All HIPAA data stewards can be notified via the group mailing list phi-stewards- list@nd.edu.

Transfer of University Generated PHI

ND researchers are normally consumers of externally generated PHI data. However, in the event that University generated data is to be transferred outside the University, we will de-identify or otherwise transmit in compliance with HIPAA regulations

Roles

- **Research HIPAA Privacy Officer**: Director, Research Compliance. Responsible for overseeing and safeguarding the handling of protected health information (PHI) in compliance with HIPAA regulations through developing, implementing, and maintaining University privacy and security policies and procedures; reporting data breaches to external data sponsor according to applicable protocols; recording, investigating, reporting, and tracking complaints and/or breaches in privacy and security to the HHS Office of Civil Rights; and answering questions from Data Stewards and Principal Investigators.
- **Data Steward:** Responsible for developing specific data security plans for each project/lab under their purview in accordance with HIPAA; communicating HIPAA policies and procedures to the PI and research team; ensuring System Users complete necessary training; and authorizing and tracking the disclosure of and/or transfer of research data.
- **Transfer Agent:** Only data stewards can transfer ePHI data. For non-data files, research projects may choose to use transfer agents to enable the extraction or insertion of a graph, image, code snippet, summary tables, or other artifact needed to further research objectives, or create a publication or report. The transfer agent may be a member of the research program or the data steward. The onboarding process for researchers using the PHI environments should not assume

all researchers are transfer agents. Data stewards are responsible for ensuring that transfer agents receive appropriate training to ensure data is not inserted, extracted or disseminated without proper authorization.

- **Researcher/Principal Investigator:** Responsible for appointing a Data Steward; determining and documenting which members of the research team need access to PHI; executing confidentiality agreements with those research team members and any collaborators; identifying business associates in need of agreements governing their access to project/lab-related PHI; and ensuring the Data Security Plan is followed by all members of the research team.
- **System User**: Responsible for using PHI to conduct research per the project/lab's IRB protocol or data use agreement with the data provider; completing HIPAA training as needed; reading and adhering to the project/lab-specific data security plan developed by the data steward; and adhering to the minimum necessary rule.
- **OIT Security and Policy**: Responsible for advising Data Stewards on new computer systems, including software and hardware for storing and transmitting PHI.

Contacts

Subject	Office or Position	Telephone Number	Office Email or URL
Data Security Plan	Appropriate project/lab Data Steward	N/A	https://research.nd.edu/our-services/resource-library/data-stewards-list/
Policy Enforcement	Research HIPAA Privacy Officer	(574) 631-7432	compliance@nd.edu
New technology for storing or transmitting PHI	OIT	(574) 631-8111	oit@nd.edu
Web Address for this Policy		https://research.nd.edu/our-services/resource-library/	