



RESPONSIBILITY STATEMENT AND DATA STEWARDSHIP AGREEMENT

--

INFORMATION SECURITY AND CONFIDENTIALITY

Indiana University Health (“IUH”) is committed to protecting the privacy and security of its confidential information. As a system user you play a crucial role in ensuring the privacy and security of this confidential information.

IUH owns, controls and stores paper, digital and electronic data about services, programs, systems, finances, patients, families, employees, physicians, payers, and other personally identifiable information (“Data”) – most of which is CONFIDENTIAL information. Access to such Data is available through different formats and media and this Statement and Agreement applies to ALL of the data regardless of how it is accessed.

You have requested access as a user of IUH’s systems containing Data. As a user and steward of this Data, including in some instances protected health information (“PHI”) about IUH’s patients– as that term is defined in the HIPAA Privacy Rules – you must agree to the following terms and obligations before being granted access – please read your responsibilities carefully before agreeing to them by signing below:

- 1) I understand that in order to perform my clinical, research-related, and administrative duties at IUH I may be granted access to proprietary, patient or protected health information (“Data”). I agree that privacy and security of Data is my personal duty and responsibility.
- 2) I agree to take reasonable precautions to protect Data from unintentional or unauthorized inquiry, update, alteration, access, use, disclosure, destruction or removal; I understand that such precautions apply both while I am on and off duty.
- 3) I agree that I will only use, access or disclose Data as minimally necessary for the purpose for which I have been granted access, including business operations, treatment obligations, or approved research duties.
- 4) I agree that I will protect my identity and passwords to maintain my individual authentication to Data (“credentials”) and will not disclose my credentials to anyone else.
- 5) I agree that I am personally responsible for completing relevant privacy and security training at least annually and for complying with IUH’s relevant privacy and security policies and procedures .
- 6) I agree that it is my responsibility to obtain appropriate direction when I am unsure of the confidentiality or security precautions that apply to certain Data.
- 7) I agree to immediately report known or suspected confidentiality breaches to my manager/IUH sponsor, the IU Health Trust Line or the IU Health Privacy Office at hipaa@iuhealth.org or 317-963-1940.
- 8) I agree not to use or disclose IUH’s PHI except as minimally necessary to provide health care to patients, process payments or for authorized health care operations or legitimate business purposes as permitted under contract.
- 9) I agree to use, create, access, transmit, or store electronic PHI using only approved equipment with encryption technology or equivalent appropriate protections.
- 10) I agree not to download to or transmit PHI using equipment that does not meet the IUH standards for security.



Indiana University Health

- 11) Except as otherwise authorized in writing by IUH, I hereby represent that I do not have any IUH PHI in my possession, electronic or otherwise, for any purpose other than the purpose for which I have been granted use of or access to the PHI.
- 12) In order to maintain the integrity of IUH's Data, I agree that I will not search for, view, access, change, or otherwise manipulate my own PHI, as this constitutes a misuse of IUH's systems..
- 13) I agree that I will not search for, view, access, change, manipulate, or use PHI of friends or family members except as otherwise permitted (e.g. to perform my IUH-related or approved job duties or responsibilities).
- 14) I will not use or disclose PHI for marketing or fundraising purposes except as specifically approved by IUH.
- 15) If I must store or transmit electronic PHI for patient care or other IUH authorized purpose, then I shall ensure that it is encrypted at all times (e.g. PHI on any mobile device: thumb drive, smart phone, or laptop computer).
- 16) I agree to access PHI using only the credentials I have been given by IUH or a reasonable third party acting on their behalf, and that I will keep those credentials confidential. I will not use the credentials of other individuals or generic credentials not specific to me.
- 17) I agree that when my employment, affiliation, privileges, or assignment with IUH ends, I will not take any PHI with me.
- 18) I agree to immediately report to IUH any suspected unauthorized use or disclosure of PHI, such as the theft of a mobile device containing PHI or inappropriate use or access
- 19) I understand that if I do not maintain the privacy and security of IUH Data and PHI that I may be subject to immediate disciplinary or corrective action, up to and including suspension or termination of employment or clinical privileges and termination of my access to IU Health systems.
- 20) I understand that unauthorized use or disclosure of PHI may violate federal or state law and could result in criminal or civil penalties.

I have had the opportunity to read and understand this Responsibility Statement and Data Stewardship Agreement and agree to its terms and conditions as indicated by signing my name below:

Printed Name – User

Signature

Date

IU Health Employee Number (if any)

IU/ IUSOM ID Number

Physician Number

Non-IU Health Last 5 SSN