Indiana University Health

Information Security Responsibility Statement and Data Stewardship Agreement

(All IU (Indiana University) Health Users and Non-IU Health Users)

Indiana University Health and its affiliated entities, including the members of the Indiana University Health Affiliated Covered Entity (collectively "IU Health"), are committed to protecting the privacy and security of its confidential information. As a systems user, you play a crucial role in ensuring the privacy and security of this confidential information.

IU Health owns, controls, uses, transmits, and stores paper, biometric, digital, and electronic data about services, programs, systems, finances, patients, families, guarantors, team members, providers, physician groups, other healthcare providers, payers, individuals, including PHI (Protected Health Information as defined by HIPAA (the Health Insurance Portability and Accountability Act), and other personally identifiable information (collectively "Data"). All IU Health information is to be considered CONFIDENTIAL/CRITICAL information. Access to such Data is available in many formats and media, and this Information Security Responsibility Statement and Data Stewardship Agreement applies to ALL the Data regardless of how it is collected, used, accessed, transmitted, or stored.

You have requested access as a user of IU Health's systems containing Data. As a user, steward and/or provider of this Data, you must agree to the following terms and obligations before being granted access – please read your responsibilities carefully before agreeing to them. In this agreement, I understand that I am referred to as "user", "end user" or "information customer".

1) I agree that I am requesting access as a user of the Data for the purposes of treatment, payment, health care operations (including education and training), research, or as a business associate of IU Health (all purposes as defined by HIPAA); and any other activities approved by IU Health and that privacy and security of the Data is my personal duty and responsibility.
2) All Indiana University Health information is to be considered confidential. Reasonable precautions are to be taken to protect Indiana University Health information from unintentional or unauthorized inquiry, update, alteration, destruction, or removal. It is to be always safeguarded by all information customers, both at work and off duty. It is the responsibility of the information customer to seek and obtain direction regarding the release of information and/or information protection safeguards.
3) Information customers will only access (read, add, change, or delete) or disclose information for which they have a business reason to do so. At no time shall information be accessed or disclosed for an unauthorized, unethical, or illegal reason. It is possible that in the course of business, indirect access to information may become available. All responsibilities outlined in this agreement apply to both direct and indirect access to Data information.
4) I understand that I may not access, change, or update my personal medical records through systems or processes for which I have been granted access. I also understand that I may not access medical records of family members, friends, or colleagues unless such access is a legitimate business purpose, such as for treatment, payment, or health care operations.
5) I agree to use, create, access, transmit, or store Data using only approved equipment with encryption technology or equivalent appropriate protections. If I must store or transmit electronic Data for patient care or other authorized purposes approved by IU Health, then I shall ensure that the data is always encrypted (e.g., Data on any mobile device, USB drive, smartphone, or PC or laptop computer that must be encrypted, and password protected).
6) Information access must be requested, approved, and implemented through established protocols. Access to information will be granted on an appropriately identified, validated, and authorized basis. I understand that my access to Data will be audited periodically, and I agree to fully cooperate with any audit or investigation into my access, use, and disclosure of Data.

7) I agree I will protect my identity, passwords, and authentication mechanisms such as two-factor authentication codes and applications or biometrics to maintain my individual authentication to the Data ("credentials") and will not disclose my credentials to anyone else. I agree to access Data using only the credentials I have been given by IU Health (or a third party acting on IU Health's 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.
8) I will not use IU Health systems for my personal use (e.g., crypto mining, storing non-IU Health data on IU Health servers, equipment, systems, etc.), nor will I access, use, or disclose Data for marketing or fundraising purposes except as specifically approved by IU Health.
9) I understand and agree that it is my responsibility to promptly report suspected confidentiality breaches, known or suspected inappropriate access, use or disclosure of Data and potential Data confidentiality breaches, or other information violations to my IU Health Manager, IU Health Line Manager, IU Health Contingent Worker-Leader, or IU Health Sponsor, the IU Health Privacy Office at 317-963-1940 or HIPAA@iuhealth.org or the IU Health Help Desk immediately in the event of the security incident (e.g. ransomware cyber-attack, phishing email; lost, stolen or compromised computers, devices and systems) at 317-962-2828 or HelpDesk@iuhealth.org.
10) I agree that I am personally responsible for completing privacy and security training at least annually, for complying with IU Health's privacy and security policies and procedures, for maintaining the confidentiality of the Data, and for complying with all applicable state and federal laws governing the Data, including without limitation HIPAA. I understand that unauthorized usage, access, use, or disclosure of Data may violate federal or state laws and could result in criminal or civil penalties or other actions.
11) I understand if I fail to maintain the privacy and security of the Data, fail to comply with IU Health policies and procedures regarding usage or access, or fail to comply with applicable laws governing the Data that I may be subject to immediate disciplinary or corrective action, up to and including suspension or termination of access, employment, and/or clinical privileges and could be banned from being rehired for up to 5 years or a lifetime.
12) I agree when my employment, affiliation, privileges/credentialing, research, training, contract, or assignment, for which I was granted access to the Data ends, I will immediately cease accessing and using the Data and IU Health systems, and I will not take the Data with me.
13) I understand that IU Health may terminate and end my access to the Data at any time within IU Health's sole discretion, and that failure to adhere to this responsibility statement will result in the appropriate disciplinary and/or legal action.
14) If I am an authorized IU Health user who accesses controlled substances or other medications through an automated dispensing system, I agree that my biometric fingerprint Data will be collected, stored, and used to authorize my access to such systems for care delivery and audit purposes. I agree that my image and facial recognition Data will be collected, stored, and used on IU Health's video surveillance systems.

Third-Party Contingent/Non-worker Access User Acknowledgement: by signing this document, I attest to the following:

- I understand that if I no longer need EMR access due to my role changing or I am no longer employed by the affiliate organization/employer my access was granted through, I am responsible for promptly notifying my IU Health Sponsor, Information Security at infosecthirdpartycompliance@iuhealth.org, or the Service Desk at 317-962-2828 HelpDesk@iuhealth.org to ensure that my access is removed.
- I am currently employed with my affiliate and remain in good standing.
- I confirm that I have not been terminated for inappropriate or unethical conduct, or compliance violations such as improper access or disclosure of patient protected health information. If such a situation occurs, I will immediately notify my recruiter, the hiring manager, or my IU Health Sponsor.
- I understand it is my responsibility to immediately notify my IU Health Sponsor or Information Security at infosecthirdpartycompliance@iuhealth.org, if any of my demographic (i.e., home address, personal phone number, name) or contact information (i.e., affiliate leader, affiliate address) has changed.
- I understand that I am required to complete annual IU Health HIPAA/HIPAA Security training, and I will complete HIPAA training annually.

I have had the opportunity to read the above information, have had the opportunity to have questions addressed to my satisfaction, and understand this Information Security Responsibility Statement and Data Stewardship Agreement. I agree to its terms and conditions as indicated by my printed name and signature below.

_____	_____	_____
Printed Name – User	Signature	Date

_____	_____
Employer/Institution's Name (if not IU Health)	Manager Name

_____	_____
IU Health Employee # (if known or Username)	Indiana University ID # (if applicable)