THE UNIVERSITY OF ARIZONA

Health Information Access Policy

POLICY INFORMATION

Policy Sponsor: Chief Privacy Officer
Responsible Unit: Privacy Office
E-mail: Privacy@email.arizona.edu

PURPOSE AND SUMMARY

The purpose of the Health Information Access Policy is to document and establish how the University of Arizona (University) facilitates the Access, Exchange, and use of Electronic Health Information (EHI).

SCOPE

This Policy applies to all Actor-Units that collect, use, produce, transmit, display, process, or store EHI.

DEFINITIONS

Access means, including Electronic Access, the ability or means necessary to make EHI available for Exchange or Use. Access is used throughout to also refer to all three practices, i.e., "Access, Exchange, and Use of EHI" for ease.

Actor-Unit means an Actor is an entity or person subject to the Information Blocking rule. An Actor-Unit is a Unit of the University that functions either as a 1) health care provider or supplier (defined by federal law 42 CFR § 400.202), 2) Health Information Exchange or Network (HIE/HIN), or 3) Health IT Developer.

Designated Record Set has the same definition as in the University HIPAA standard HPP-PRV-005, HIPAA Patient's Right to Access PHI.

Electronic Access means an internet-based method that makes EHI available at the time the EHI is requested and no manual effort is required to fulfill the request.

Electronic Health Information (EHI) means any data that would be considered Electronic Protected Health Information (ePHI) even if the entity or individual is not HIPAA covered. EHI is limited to any ePHI in a Designated Record Set, and excludes 1) Psychotherapy Notes, and 2) information created in reasonable anticipation of legal action.

Electronic Protected Health Information (ePHI) has the same definition as under HIPAA and 45 CFR 160.103.

Exchange means the ability for EHI to be transmitted between and among different technologies, systems, platforms, or networks.

Health Information Network ("HIN") or Health Information Exchange ("HIE") means an individual or entity that determines, controls or has the discretion to administer any requirement, policy, or agreement that permits, enables, or requires the use of any technology or services for Access among more than two unaffiliated individuals or entities (other than the originating organization) that are enabled to Exchange with each other for a treatment, payment, or health care operation purpose, as defined under HIPAA, regardless of whether those individuals or entities are HIPAA covered.

Health IT Developer means an individual or entity, excluding a health care provider self-developing Health IT for its own uses, that develops, offers, or licenses health information technology which has one or more health IT modules certified under an HHS ONC program at the time it engages in Information Blocking practices.

Individual means any person who is the subject of the EHI being Accessed, or a person who legally acts on behalf of such a person making decisions related to health care, i.e., their Legal Representative.

Information Blocking means any act, omission, limitation, or condition that is likely to Interfere with the Access.

Interfere means to prevent, materially discourage, or otherwise inhibit.

Legal Representative means an individual, also called a Personal Representative under HIPAA, who has the legal authority under state law to act for and request information on behalf of the patient (e.g., a parent of a minor).

Psychotherapy Notes has the same definition as defined under HIPAA and 45 CFR 164.501.

Unit means a college, department, school, program, research center, business service center, or other operating Unit of the University.

Use means the ability for EHI once Accessed to be understood and acted upon.

THE UNIVERSITY OF ARIZONA

POLICY

A. Providing Access to EHI

1. The University provides Access to Individuals, Legal Representatives, and other third parties who request it, except as described in this Policy. Actor-Units that maintain EHI will provide access in the manner or the medium requested.

2. Units that maintain EHI will respond to a request for EHI within no less than five (5) business days, in one of two ways:

    a. Approvals and Conditions. If approved, provide the EHI in the manner it was requested. Any conditions on providing the EHI must be in writing and approved by the Privacy Office before being provided (e.g., fees for record access or licensing of data).

    b. Limitations and Denials. Acknowledging receipt of the request in writing and:

        i. *Alternatives*: Offering (if available) to provide the EHI in another manner if the requested manner is unavailable. For example, if the data is in a different format than requested. If the requestor rejects this proposal, proceed to the next paragraph.

        ii. *Denials:* Notifying the Privacy Office of the request and reason for denial (See D.2) and informing the requestor that their request is under review. Actor-Units will then collaborate with the Privacy Office on the request. The Privacy Office may approve written policies and procedures for routine denials by Actor-Units.

B. Responsibilities for Maintaining EHI

1. Data Inventory. Actor-Units that maintain EHI must review on a quarterly basis the systems, assets, and stores where EHI is maintained to determine what access and interoperability is available. This includes access to electronic medical records (EMRs) and electronic health records (EHRs). For example, EHRs certified by HHS ONC (commonly called CEHRT) may have patient portal and data exchange protocols available by default.

2. System Capability. If a system or application containing EHI has an access or exchange capability, Actor-Units must permit Individuals and third parties to utilize these capabilities if requested. Units are under no obligation to purchase or provision resources in upgrading any system or asset to make the EHI more accessible to requests, but features that are already or easily available that increase accessibility of EHI must be enabled. For example, if an EHR has a web portal available to patients, the Unit should enable this feature and provide access to patients unless a significant reason exists not to (e.g., there would be a financial cost to the University to upgrade the system).

C. Information Blocking

1. Blocking Prohibited. The University will not engage in any practice of Information Blocking.

2. Blocking. Information Blocking is defined as any act, omission, limitation, or condition that is likely to Interfere with the Access. A practice is Information Blocking if the Actor-Unit knew or should have known that the practice would Interfere with Access. Depending on the Actor-Unit, the knowledge requirement for Information Blocking varies:

    a. *Health Care Provider*: The University knows that such practice is unreasonable and knows it is likely to Interfere with Access.

    b. *HIE/HIN:* The University knows, or should know, that such practice is likely to Interfere with Access.

    c. *Health IT Developer:* The University knows, or should know, that such practice is likely to Interfere with Access.

D. Exceptions

1. Documented Exception. A practice will not be Information Blocking if it meets all the requirements of a legal exception laid out in in the Information Blocking Rule. These legal exceptions contain specific requirements for denying, limiting, or conditioning access in the event of physical harm, privacy, security, performance, infeasibility, content and manner, fees, and licensing. Exceptions must be documented and follow the requirements of section D.2.

2. Denying, Conditioning, or Limiting a Request. Prior to the denial of a request and without any unreasonable delay, any Unit that intends to deny the sharing of EHI shall contact the Privacy Office at privacy@email.arizona.edu to review and provide approval. Unit staff will supply the Privacy Office with all details and documents necessary in a timely fashion making a timely review of a request, no later than five (5) business days from receiving the request. The Privacy Office may approve Unit procedures for routine denials or limitations on access to EHI.

COMPLIANCE AND RESPONSIBILITIES

All Actor-Units that collect, use, produce, transmit, display, process, or store EHI are responsible for knowing and complying with this Policy.

The Privacy Office is responsible for compliance with this Policy.

FREQUENTLY ASKED QUESTIONS*

There are no FAQs relevant to this Policy.

Sources*

45 CFR Part 171 – Information Blocking Rule
45 CFR Part 164 – HIPAA Regulations

Related Information*

There is no related information relevant to this Policy.

Revision History*

*** Please note the Frequently Asked Questions, Sources, Related Information, and Revision History sections are provided solely for the convenience of users and are not part of the official University policy.**