THE UNIVERSITY OF ARIZONA
Research
Innovation & Impact

Record Reviews

The wealth of data available today holds tremendous promise for informing and directing research. The human subject definition extends to a subject's identifiable private information. As such, the IRB must review research proposing to use identifiable data, including data from medical records (HIPAA protected data).

What is Identifiable Information?

Identifiable data and biospecimens are those that include information where the identity of the individual "is or may readily be ascertained by the investigator." Some of this information may also be considered private, such as information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information that has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public.

Personal identifiers include the following:

- Names
- Home or email addresses
- Telephone numbers
- Fingerprints
- Full face photographs
- Social security numbers
- Account numbers
- Medical record numbers
- Codes that link de-identified data to identifiers (not stored separately from data)
- Audio or video recordings of participants

Potentially Identifiable information may not have direct identifiers, but when combined with other basic demographic data, may become identifiable. For example:

- Demographic information and immigration status of ethnic minorities in a rural county
- Graduates' perspectives from a small high school coupled with their occupation

Indirect identifiers include:

- Age
- Ethnicity
- Gender
- City or state of residence
- Occupation or role
- Job function or title
- Specific time, event, context, or occasion

It is up to the researcher to describe the specific data elements that will be collected so that the IRB can make the necessary determination regarding risk, privacy and confidentiality needs for each particular study.

Record Reviews

HIPAA Protected Health Information (PHI)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that requires the protection of sensitive patient health information (PHI) from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
The following are the 18 HIPAA Identifiers that are considered personally identifiable information, whether that information is coming from a medical record or another source:

- Name
- Address (all geographic subdivisions smaller than state, including street address, city county, and zip code)
- All elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age if over 89)
- Telephone numbers
- Fax number
- Email address
- Social Security Number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate or license number
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web URL
- Internet Protocol (IP) Address
- Finger or voice print
- Photographic image - Photographic images are not limited to images of the face.
- Any other characteristic that could uniquely identify the individual

If a record or biospecimen contains any of these identifiers, or parts of the identifier, such as initials, the data is to be considered "identified". To be considered "de-identified", ALL the 18 HIPAA Identifiers must be removed from the data set. This includes all dates, such as surgery dates, all voice recordings, and all photographic images.

Limited Data Set

A "limited data set" is data that is stripped of certain direct identifiers. For example, a photograph from which "facial" identifiers have been removed. The health information that may remain in the information disclosed includes:

- dates such as admission, discharge, service, DOB, DOD;
- city, state, five digit or more zip code; and
- ages in years, months or days or hours.'

Record Reviews

It is important to note that this information is still protected health information or "PHI" under HIPAA. It is not de-identified information and is still subject to the requirements of the Privacy Regulations. For more information about limited data sets please visit the University of Arizona **HIPAA Privacy Program** website.

The University of Arizona IRB, does not consider projects that are only receiving/reviewing a limited data set as human subject's research.

Types of Records Review

Retrospective Record Review: evaluates data that is existing *at the time the protocol is submitted to the IRB* for initial approval. A retrospective data review's protocol should specify the timeline of data to be reviewed. (i.e., data will be reviewed from October 2020 to July 2021).

NOTE: A waiver of consent and PHI authorization can be granted oftentimes for retrospective records review if the study meets the waiver criteria and data is existing at time of submission to the IRB. However, the IRB will not approve a moving date range beyond one request. If you know you want to collect information into the future, then there is opportunity for consent, and the IRB needs to approve the project as such.

Prospective Record Review: evaluates data that *does not yet exist at the time the protocol is submitted to the IRB* for initial review. The IRB typically requires consent from the participants whose data will be used.

Why is Consent Needed for Some Record Reviews and Not for Others?
Whenever possible the IRB adheres to the Belmont Report principle of 'respect for persons.' This principle says that people should have a say in what happens to them and their information. In addition, some records have a legal or regulatory requirement for consent.

In keeping with the principles of the Belmont Report, all prospective studies should obtain consent unless the study can justify meeting all of the following consent waiver requirements:

- The research involves no more than minimal risk to the subjects;
- The waiver or alteration will not adversely affect the rights and welfare of the subjects;
- The research could not practicably be carried out without the waiver or alteration;
- Whenever appropriate, the subjects or legally authorized representatives will be provided with additional pertinent information after participation; and
- If the research involves using or accessing identifiable private information or identifiable biospecimens, the research could not practically be carried out without using such information or biospecimens in an identifiable format.

The third bullet point about the research not being able to be carried out without a waiver or alteration tends to cause a lot of confusion. The feasibility of getting consent is not based on the difficulty level of obtaining consent, or the inconvenience to the researcher. Instead, it is based on the subject being available or reachable, and what is the right thing to do. If a patient is in the hospital or visiting the researcher routinely, then the individual is available.

Common Record Requests and Requirements

Medical Records: Information contained in a medical record is considered Protected Health information (PHI) and is protected under the Health Insurance Portability and Accountability Act (HIPAA). Written authorization to access PHI must be obtained from the owner of the record before access to the record is permitted or a waiver of PHI authorization can be requested.

Educational Records: Educational records are protected under The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99). FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when s/he reaches the age of 18 or attends a school beyond the high school level. To access identifiable educational records for research purposes, you must obtain written consent from the research participant.

The organization that owns the record is charged with protecting the FERPA information. At the University of Arizona, the Registrar is the designated individual with defining "directory information." Information regarding which data elements are eligible to be considered directory information and from which the University's list is selected can be found at www.registrar.arizona.edu/FERPA. Access to records from schools other than the UA must have site authorization from the district who owns the records.

Access to department specific records may be granted by the individual department. Site authorization for use of large-scale University of Arizona student records (undergraduate, graduate, and professional) is given by the Registrar's Office. The request for release of information and a copy of the protocol must be submitted to the Registrar for a determination of whether the release of information is appropriate under FERPA.

Registrar
PO Box 210066 or REG-reghelp@email.arizona.edu

A copy of the written site authorization to access student records for information beyond the above directory information must be submitted with the appropriate form.

Employment Records: Access to records of employees of the University of Arizona (e.g. medical residents, staff or faculty) requires the written consent of the employee per ABOR Policy 6-912. The policy permits administrative access to personnel records only for authorized purposes (which typically do not include research) unless authorized by the President.