HIPAA: A QUICK REVIEW

The regulations associated with HIPAA are lengthy and complex, but here are the key points:

- HIPAA's privacy protections for health information supplement those of other federal regulations and any applicable state laws.
- HIPAA protects identifiable health information -- also known as "protected health information" or PHI.
- HIPAA's rules on use and disclosure of PHI are generally "purpose-based" -- that is, governed by the intended use. The rules for activities defined as research are different from those for other covered activities.
- De-identified data are not protected, and some identifiable health information may not be considered PHI, depending on how it was generated.
- Limited data sets may be used as a middle ground between PHI and de-identified data, but require a data use agreement.

HIPAA RESEARCH: AUTHORIZATION (CONSENT) OR NOT?

HIPAA only applies to Health Research or any research creating medical data, using medical records/database or interacting with medical facilities. Like the Common Rule, HIPAA begins with the premise that using PHI for research requires a subject's permission. If the data in question meet the definition of PHI and are being used for purposes that fall within HIPAA's definition of research, explicit written authorization (consent) from the subject is required.

However, HIPAA allows for research-related access to individuals' identifiable health data without authorization under certain circumstances:

- 1. The research involves only minimal risk. This research may request a waiver.
- 2. The research is used solely for activities preparatory to research. This research may request a waiver.
- 3. Only deceased individual's information is used.
- 4. It is "grandfathered" research where all legal permissions were in place before HIPAA took effect.

Data that do not identify individuals can be used for research without specific authorization if:

- 1. Only fully de-identified data are used (by definition, it is then no longer PHI).
- 2. A "limited data set" is used, under an approved "data use agreement."

The Cherokee Nation Institutional Review Board (IRB) and Privacy Officer have the authority to make the final determination of HIPAA requirements or waivers, and may require alteration of the any study's authorization forms.

Below is a HIPAA decision tree that will help us determine if your study need to include a HIPAA authorization form or a HIPAA waiver in your application:

Determining When HIPAA Applies to Health Research

NO

(Start) Does your research collect or record any of the 18 HIPAA identifiers for living participants, deceased persons, and/or stored in databases or repositories?

Will all identifiers except geographic information above street level, age and dates be removed from the data? Are you applying to the IRB for a waiver of consent or conducting exempt chart review research?

HIPAA applies submit a HIPAA waiver with your IRB application

NO

You are using deidentified data (<u>not</u>
<u>HIPAA</u>) in your research
project. You will still
submit variables collected
with your IRB
application.

YES

You will be using a
Limited Data Set (not
HIPAA) or a Public
database. You still need
to submit any Data Use
Agreements with your
IRB application.

NO

Will you be interacting or intervening with a living individual's existing medical records? This includes any patient contact lists.

YES

YES

YES

You are using PHI and must get participant permission. Submit your authorization form with your IRB application

HIPAA applies

HIPAA Identifiers

- •Names
- Social Security Numbers

YES

- Device Identifiers
- Biometric Identifiers
- Dates
- •Email Addresses
- •License/Certificate #s
- Photos & Like Images
- ·Postal Addresses Medical
- •Record Numbers Vehicle
- •ID numbers
- Any other unique ID
- Phone Numbers
- •Health Plan Numbers
- •Web URLs
- Fax Numbers
- Account Numbers
- IP Address Numbers

Are all research subjects about whom data will be collected deceased?

NO

NO

Contact the IRB for assistance

Using PHI for individuals that have been deceased for more than 50 years does not require HIPAA protection. If less than 50 years you must submit a HIPAA form with your application.