HIPAA Guidance/FAQs

1. What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) includes Administrative Simplification provisions, a Privacy Rule, and a Security Rule requiring the U.S. Department of Health & Human Services (HHS) to adopt national standards for electronic health care transactions and code sets, unique health identifiers, privacy, and security. HIPAA mandates privacy protections for individually identifiable health information in any medium, oral, electronic, or paper. Examples of individually identifiable health information can be located in electronic or paper medical records, during conversations about an individual's care or treatment, or in anything that relates to payment for an individual's care or treatment (i.e. billing/insurance items). Covered entities (health plans, health care providers, and health care clearinghouses) must follow HIPAA, put safeguards in place to protect and limit access to health information, and limit uses and disclosures to the minimum necessary.

Additionally, business associates (contractors, subcontractors, etc.) of covered entities must also follow HIPAA. Covered entities must have contracts in place with their business associates outlining safeguards for use and disclosure of health information and business associates must also have similar contracts with their subcontractors. In 2013, The Final Omnibus Rule implemented a number of provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, to strengthen the privacy and security protections for health information established under HIPAA.

2. What is Protected Health Information (PHI)?

PHI is individually identifiable health information that is transmitted or maintained in any form or medium (electronic, oral, or paper) by a covered entity or its business associates. PHI relates to the past, present or future physical or mental health condition, healthcare services provided, or payment for healthcare.

HIPAA allows researchers to access and use PHI to conduct research according to a valid HIPAA authorization or HIPAA waiver. However, HIPAA only affects research that uses, creates, or discloses PHI that will be entered in to the medical record or will be used for healthcare services, such as treatment, payment or operations. For example, PHI may be used in a research study involving review of existing medical records for research information, such as retrospective a chart review. Also, studies that create new medical information because a health care service is being performed as part of research, such as diagnosing a health condition or a new drug or device for treating a health condition, create PHI that will be entered into the medical record. For example,

sponsored clinical trials that submit data to the U.S. Food and Drug Administration involve PHI and are therefore subject to HIPAA.

3. What is not Protected Health Information?

   Some studies use data that is person-identifiable because it includes personal identifiers such as name, address, but it is not considered to be PHI because the data is not associated with or derived from a healthcare service event not entered into the medical records, nor will the subject/patient be informed of the results. Research health information that is kept only in the researcher's records is not subject to HIPAA but is regulated by other human subject protection regulations.

   Examples of research health information not subject to HIPAA include such studies as the use of aggregate data, diagnostic tests that do not go into the medical record because they are part of a basic research study and the results will not be disclosed to the subject, and testing done without the PHI identifiers. Some genetic basic research can fall into this category such as the search for potential genetic markers, promoter control elements, and other exploratory genetic research. In contrast, genetic testing for a known disease that is considered to be part of diagnosis, treatment, and health care would be considered to use PHI and therefore subject to HIPAA.

   Health information by itself without the 18 identifiers is not considered to be PHI. For example, a dataset of vital signs by themselves do not constitute PHI. However, if the vital signs dataset includes any other identifiers, such as a medical record number, then the entire dataset must be protected since it contains an identifier.

4. What are the 18 HIPAA Identifiers?
   - **Names**
   - **Addresses** -- All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
   - **Dates** -- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
   - **Phone numbers**
   - **Fax numbers**
   - **Electronic mail (e-mail) addresses**
   - **Social Security numbers**
   - **Medical record numbers**
   - **Health plan beneficiary numbers**
   - **Account numbers**
   - **Certificate/license numbers**
   - **Vehicle identifiers and serial numbers, including license plate numbers**
   - **Device identifiers and serial numbers**
   - **Web Universal Resource Locators (URLs)**

- **Internet Protocol (IP) address numbers**
- **Biometric identifiers, including finger and voice prints**
- **Full face photographic images and any comparable images**
- **Any other unique identifying number, characteristic, or code** (note this does not mean the unique code assigned by the investigator to code the data)

There are also additional standards and criteria to protect individual's privacy from re-identification. Any code used to replace the identifiers in datasets cannot be derived from any information related to the individual and the master codes, nor can the method to derive the codes be disclosed. For example, a subject's initials cannot be used to code their data because the initials are derived from their name. Additionally, the researcher must not have actual knowledge that the research subject could be re-identified from the remaining identifiers in the PHI used in the research study. In other words, the information would still be considered identifiable is there was a way to identify the individual even though all of the 18 identifiers were removed.

5. When is health information considered de-identified?

   Health Information that does not identify an individual and that there is no reasonable basis to believe that the information can identify an individual is not individually identifiable health information.

   Health information is considered de-identified if:
   - It has been determined by the appropriate person that the risk is very small that the information could be used to identify an individual.
   - It meets the safe harbor method which is the removal of all of the individual identifiers from the health information.
   - Children's may de-identify information and use codes or other similar means of marking records so they may be later re-identified.

6. What is a Limited Data Set (LDS)?

   A limited data set refers to PHI that excludes 16 categories of direct identifiers and may be used or disclosed, for purposes of research, public health, or health care operations, without obtaining either an individual's authorization or a waiver or an alteration of authorization for its use and disclosure, with a data use agreement.

A limited data set is described as health information that excludes certain, listed direct identifiers (see below) but that may include city; state; ZIP Code; elements of date; and other numbers, characteristics, or codes not listed as direct identifiers. The direct identifiers listed in the Privacy Rule's limited data set provisions apply both to information about the individual and to information about the individual's relatives, employers, or household members. The following identifiers must be removed from health information if the data are to qualify as a limited data set:

1. Names.
2. Postal address information, other than town or city, state, and ZIP Code.
3. Telephone numbers.
4. Fax numbers.
5. Electronic mail addresses.
6. Social security numbers.
7. Medical record numbers.
8. Health plan beneficiary numbers.
10. Certificate/license numbers.
11. Vehicle identifiers and serial numbers, including license plate numbers.
12. Device identifiers and serial numbers.
13. Web universal resource locators (URLs).
14. Internet protocol (IP) address numbers.
15. Biometric identifiers, including fingerprints and voiceprints.
16. Full-face photographic images and any

9. Account numbers. comparable images.

7. What is the difference between HIPAA Authorization and Informed Consent?

   A HIPAA Authorization is an individual's signed permission to allow a covered entity to use or disclose the individual's PHI that is described in the authorization for the purpose(s) and to the recipient(s) stated in the authorization. In contrast, an informed consent document is an individual's agreement to participate in the research study and includes a description of the study, anticipated risks and/or benefits, and how the confidentiality of records will be protected, among other things. A HIPAA Authorization can be combined with an informed consent document or other permission to participate in research. If a covered entity obtains or receives a valid HIAA Authorization for its use or disclosure of PHI for research, it may use or disclose the PHI for the research, but the use or disclosure must be consistent with the authorization.

8. What is the difference between HIPAA Authorization, Partial HIPAA Waiver and Full HIPAA Waiver?

   A Full HIPAA Waiver allows an investigator to use and disclose PHI for a particular research trial or activity without obtaining either a verbal or written authorization from the participants. The criteria for a Waiver or Alteration are as follows:

   - The use or disclosure (not necessarily the research study) involves no more than minimal risk; AND
   - The research could not practicably be conducted with the waiver or alteration; AND
   - The research could not practicably be conducted without access to and use of the PHI.

   A Partial HIPAA Waiver allows an investigator to obtain, use, and/or disclose PHI for one specified portion of a research trial or activity (e.g., in the course of recruitment) without first obtaining a verbal or written authorization.

   Authorization is an individual's signed permission to allow a covered entity to use the individual's PHI. Anytime subjects will sign a HIPAA Authorization, this selection should be checked. Anytime a Partial HIPAA Waiver is requested, this option should also be checked.

9. What is an Alteration of HIPAA Authorization?

   The IRB may approve an alteration of the requirements of a written HIPAA Authorization provided the research meets the criteria for waiver or alteration (see above). The most frequent alteration is for verbal HIPAA Authorization when the IRB has also waived the requirement for written consent.

10. At what point in recruitment is HIPAA Authorization needed?

If the IRB has granted partial waiver of HIPAA Authorization to permit access to or collection of PHI for screening without written authorization, contact and screening information may be used.

If you are in contact (verbal, written, or electronic) with the subject for screening, you should indicate to the potential subject that in order to determine whether he or she is eligible for the research, you may need to share information with other study staff. If a person is not eligible, the information should be destroyed and not used for any other purpose, unless you are required to retain the data for the sponsor or for FDA-regulated studies.