**HIPAA 101 – Tip Sheet**

**University of Colorado Denver | Anschutz Medical Campus**

**HIPAA (Health Insurance Portability and Accountability Act).** HIPAA, as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH), is a United States law designed to improve the portability and continuity of health care coverage, standardize health care transactions and implement requirements surrounding health information privacy and security. In general, HIPAA addresses Protected Health Information (PHI) that is maintained or transmitted by a covered entity.

**Covered Entity.** Covered Entities are defined in HIPAA as (1) health plans, (2) health care providers and (3) health care clearinghouses (entities that process nonstandard information they receive from another entity into a standard format or data content, or vice versa) who electronically transmit any health information in connection with transactions for which HHS has adopted standards. HIPAA applies to Covered Entities.

**Hybrid Entity.** A single legal entity that conducts both covered and non-covered functions and designates certain health care components as covered functions – resulting in those functions of the entity being subject to HIPAA. *University of Colorado Denver | Anschutz Medical Campus is a Hybrid Entity.*

**PHI (Protected Health Information).** A patient’s information related to…

* Past, Present, Future
* Mental or Physical Health (or related billing information)
* Which can be connected to the individual by one of 18 identifiers (listed below)
* And which can come in all forms – including oral, written, electronic, etc.

*Excludes employment records and education records (HR/FERPA)*

PHI can be shared without a patient’s authorization for purposes of:

 **T**-reatment

 **P**-ayment

Healthcare **O**-perations

**18 Identifiers which can connect an individual to their PHI, making it identifiable.**

*First, important reminders –*

* *Remember, per the definition above, PHI is not limited to these 18 identifiers*

1. Names;

2. 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;

3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and 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;

4. Telephone numbers;

5. Fax numbers;

6. E-mail addresses;

7. Social Security numbers;

8. Medical records numbers;

9. Health plan beneficiary numbers;

10. Account numbers;

11. Certificate/license numbers;

12. Vehicle identifiers and serial numbers, including license plates;

13. Device identifiers and serial numbers;

14. Web Universal Resource Locators (URLs);

15. Internet Protocol (IP) address numbers;

16. Biometric identifiers (including finger and voice prints);

17. Full face photographic images and any comparable images; and,

18. Any other unique identifying number, characteristic, or code (with some exceptions and requirements).

**Deidentified Information.** Information from which all of the 18 Identifiers have been removed. Note that number 18 can sometimes be subjective and has some implications with respect to research. Deidentified information is not subject to HIPAA.

**Business Associate (BA).** A Business Associate is a person or entity who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the BA to protected health information. A “business associate” must protect the ePHI that it creates, receives, maintains, or transmits on behalf of the CE. A CE may be a BA of another CE if it performs such services for the other CE.

**Business Associate Agreement (BAA).** The HIPAA Rules generally require that CEs and BAs enter into contracts with their BAs to ensure that the BAs will appropriately safeguard PHI. The BAA also serves to clarify and limit, as appropriate, the permissible uses and disclosures of PHI by the BA, based on the relationship between the parties and the activities or services being performed by the BA. A BA is directly liable under the HIPAA Rules for making uses or disclosures of PHI not authorized by the BAA or required by law. The following items must be addressed in the BAA to ensure compliance with current regulation:

1. Safeguards for protecting PHI
2. Reporting mechanism for inappropriate use/disclosure of PHI
3. Pass-through of provisions to any agent/subcontractor
4. Access to PHI for amendment and mechanism for Accounting of Disclosures (AOD)
5. Provision stating that BA will make available its internal practices, books and records relating to the use and disclosure of PHI for audit by HHS
6. Plan for return/destruction of PHI and termination of underlying agreement

**Limited Data Set (LDS).** A LDS is described as health information that excludes certain, direct identifiers (listed 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. Street addresses (other than town, city, state and zip code);
3. Telephone numbers;
4. Fax numbers;
5. E-mail addresses;
6. Social Security numbers;
7. Medical records numbers;
8. Health plan beneficiary numbers;
9. Account numbers;
10. Certificate license numbers;
11. Vehicle identifiers and serial numbers, including license plates;
12. Device identifiers and serial numbers;
13. URLs;
14. IP address numbers;
15. Biometric identifiers (including finger and voice prints); and
16. Full face photos (or comparable images).

**Data Use Agreement (DUA).** An agreement into which a CE enters with the intended recipient of a LDS that establishes the ways in which the information in the limited data set may be used and how it will be protected. The data use agreement must:

1. Establish the permitted uses and disclosures of the limited data set by the recipient, consistent with the purposes of the research, and which may not include any use or disclosure that would violate the Rule if done by the covered entity;
2. Limit who can use or receive the data; and
3. Require the recipient to agree to the following:
4. Require recipient not to use or disclose the information other than as permitted by the data use agreement or as otherwise required by law;
5. Use appropriate safeguards to prevent the use or disclosure of the information other than as provided for in the data use agreement;
6. Report to the covered entity any use or disclosure of the information not provided for by the data use agreement of which the recipient becomes aware;
7. Ensure that any agents, including a subcontractor, to whom the recipient provides the limited data set agrees to the same restrictions and conditions that apply to the recipient with respect to the limited data set; and
8. Require recipient not to identify the information or contact the individual.

It is important to note that this information ***is*** **PHI** under HIPAA. *It is* ***not de-identified*** *information* and is still subject to the requirements of HIPAA.

**Useful Links:**

Internal –

[Office of Regulatory Compliance](https://research.cuanschutz.edu/regulatory-compliance#ft-hipaa-privacy-and-compliance-2) website

[HIPAA Policies](https://research.cuanschutz.edu/regulatory-compliance/home/hipaa/university-hipaa-policy) (you can also get to these via the Office of Regulatory Compliance website above; Policies include references to relevant sections in the Code of Federal Regulations)

[APS 5055 – HIPAA Hybrid Entity Designation](http://www.cu.edu/ope/aps/5055)

External –

[HIPAA FAQs for Professionals | HHS.gov](https://www.hhs.gov/hipaa/for-professionals/faq/index.html) website

[Summary of the HIPAA Privacy Rule](https://www.hhs.gov/sites/default/files/privacysummary.pdf) HHS – Office for Civil Rights Summary HIPAA Privacy document (this link is to a PDF document that includes references to specific sections of the Code of Federal Regulations)

[Guidance Regarding Methods for De-Identification of PHI in accordance with HIPAA](http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html)

[Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule (NIH)](https://privacyruleandresearch.nih.gov/pdf/HIPAA_Booklet_4-14-2003.pdf)