1 HIPAA Privacy and Security

By David B. Nelson, CHPC, CHRC, CIPP/G, CIPP/US, CISSP

Author’s Note

This chapter outlines what is probably the single most important set of regulations to impact the health care privacy professional. Every discipline, whether accounting, journalism or candle making, has one tool that forms the basis for all activities. The Health Insurance Portability and Accountability Act (HIPAA), among its information exchange benefits, created a national baseline for health care privacy and security. As our nation continues to move toward the expanded sharing of information through electronic health care records (locally, regionally and nationally), it is incumbent on all health care privacy professionals to speak the same language. A privacy professional must grasp HIPAA as the core academic discipline.

This edition of the HCCA Health Care Privacy Compliance Handbook incorporates the provisions of the Health Information Technology for Economic and Clinical Health Act (HITECH), enacted through the American Recovery Reinvestment Act (ARRA) of 2009, Public Law 111–5 as well as the modifications issued January 25, 2013 by the Department of Health and Human Services (HHS), commonly known as the Omnibus Rule. Some of the outstanding changes brought by those provisions require the health care industry to:

- Modify the individual authorization form, and other requirements, to facilitate research and disclosure of child immunization proof to schools,
and to enable access to decedent information by family members or others;

- Adopt the Enforcement Rule
- Adopt the additional HITECH Act enhancements to the Enforcement Rule not previously adopted in the interim final rule of October 30, 2009, such as the provisions addressing enforcement of noncompliance with the HIPAA Rules due to willful neglect
- Adopt and implement the Breach Notification Rule
- Prohibit most health plans from using or disclosing genetic information for underwriting purposes.

Other emendations have also been made and incorporated into this text.

**Contents and Organization**

Those new to privacy should note that the Code of Federal Regulations (CFR) holds the HIPAA Rules, but the Federal Register contains the comments on regulations. Rules are the letter of the law and the intent is the Federal Register. The latter is very informative in gleaning “intent” and is written conversationally with examples and resides at page 82462 Federal Register/Vol. 65, No. 250/Thursday, December 28, 2000/Rules and Regulations.

Traditionally HIPAA has been taught, presented and/or explained by reading down through the Code of Federal Regulations (CFR) point by point. This can be tedious as there are nearly one thousand lines to digest in subsets that can run six layers deep, which do not necessarily connect logically in the same order. This chapter pulls together privacy concepts and discusses implementation from a practical perspective by integrating topics. If it does not seem to apply to your situation, or appears to skip important pieces, go to the Federal Register to read the comments Health and Human Services made on the proposed and adopted regulation.

This chapter is divided into the following segments for ease of understanding:

- **Section One: HIPAA the ACT**
This chapter does not incorporate state, local laws and/or cross reference to other legal mandates and the relationship to HIPAA. However, the privacy professional should know conflict may exist between state and federal mandates so documentation of how privacy, security or breach reporting will be administered is critical.

Section One: HIPAA the Act

HIPAA was passed by Congress and signed into law in 1996. HIPAA has three predominant purposes:

- To make health insurance portable under ERISA;
- To move health care onto a nationally standardized electronic billing platform; and
- To prevent fraud, waste and abuse (Administrative Simplification)

Only by knowing what Congress intended though, can the privacy professional attach importance in relation to all HIPAA mandates.

Intent

“It is the purpose of this subtitle to improve the Medicare program under title XVIII of the Social Security Act, the medicaid program under title XIX of such Act, and the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information.” (1996 Public Law 104-191)

Between 1 and 1.5 percent of all private insurance dollars, and between 10 and 15 percent of public insurance dollars are lost to fraud, waste or abuse of the
health care system. No one knows exactly how much money is lost but it is clear that this contributes to the rising cost of health care.

The intent of HIPAA, to improve health care programs and the delivery of services thorough the two largest health plans in the United States, is accomplished by improved data flows. Improved data will lead to better outcomes by increasing accuracy if done consistently, using national standards for formats, specific transactions and an agreed upon vocabulary.

The improved data flows also support a rapid way to review, cross reference and data mine for fraudulent behavior. Easier to spot 991 dental services performed by one provider on a single day, or the use of a higher paying billing code that requires three surgical packs when only one pack was used.

The standards and implementation specifications ensure that participatory entities are speaking the same language in the same electronic way. The specifics of data flow are outlined in the Transaction and Code Set rule (45 CFR 162.100 – 162.1900) which includes Unique Identifiers.

Intent Barriers

“Until people are more confident about the security of electronic medical records it is vitally important that we err on the side of privacy;” Senator Sheldon Whitehouse (D-RI). Congress, knowing they wanted to improve the health care industry via the HIPAA vehicle, predicted accurately that the goals could not be accomplished unless privacy and security provisions were integral elements. Many states had no privacy rights or individual access rights to health care records. The lack of individual access and the intent to move to national standards contributed to a sense of foreboding in the privacy sector and by individuals, so the Privacy and Security rules were promulgated to make health care interstate commerce equal, thus creating a national health care privacy and security baseline or “floor.”

Congress did not predict in 1996 how the Internet would affect health care, though, and according to Dr. David Brailer, “HIPAA was never intended for the digital age.” Privacy professionals will face this issue as the regulations continue to evolve and catch up with the changing environment.

Section Two: Organization
To determine what is required of an organization and its business partners, an entity must determine if they are a covered entity, what kind of covered entity, what data is covered, what do they use the data for, where do they disclose the data, who do they receive data from, and what are all the purposes of the data. Organizationally these decisions and documentations lead to a framework which guides development of policies and procedures to support HIPAA compliance.

First it is necessary to determine if an entity is subject to HIPAA. To accomplish this, an understanding of several definitions is required. An entity must meet the definition of at least one of the three types of “covered entities” (CE) but other definitions must be considered as they clarify relationships.

**Definitions**

**Applicability.** (a) Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to the following entities:

1. A health plan;
2. A health care clearinghouse;
3. A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

(b) Where provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to a business associate. *(45 CFR §160.102)*

**Health Plan.** Means an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg–91(a)(2)).

(1) *Health plan* includes the following, singly or in combination:

   i. A group health plan, as defined in this section.
   ii. A health insurance issuer, as defined in this section.
   iii. An HMO, as defined in this section.
iv. Part A or Part B of the Medicare program under title XVIII of the Act.

v. The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, et seq.


vii. An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)).

viii. An issuer of a long-term care policy, excluding a nursing home fixed indemnity policy.

ix. An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.

x. The health care program for uniformed services under title 10 of the United States Code.

xi. The veteran’s health care program under 38 U.S.C. Chapter 17.

xii. The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq.


xiv. An approved state child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, et seq.


xvi. A high risk pool that is a mechanism established under state law to provide health insurance coverage or comparable coverage to eligible individuals.

xvii. Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg–91(a)(2)).

(2) Health plan excludes:
i. Any policy, plan, or program to the extent that it provides, or pays for the
cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS
Act, 42 U.S.C. 300gg-91(c)(1); and

ii. A government-funded program (other than one listed in paragraph (1)(i)–
(xvi) of this definition):

A. Whose principal purpose is other than providing, or paying the cost of,
health care; or
B. Whose principal activity is:

1. The direct provision of health care to persons; or
2. The making of grants to fund the direct provision of health care
to persons. (45 CFR §160.103)

Note: Health Plan exclusions set aside Medicaid enrollment as a traditional
welfare program, a government funded program whose principle purpose is
NOT providing or paying for health care. It should be noted that if the same
government program performs enrollment (either directly or through a
centralized process), but then provides or pays the cost of health care, the
exclusion provision would not apply. Documentation of what constitutes the
“principal” activity guides the business relationship.

Subhealth Plan (SHP). Means a health plan whose business activities, actions,
or policies are directed by a controlling health plan. (45 CFR 162.103)

Controlling health plan (CHP) means a health plan that—

1. Controls its own business activities, actions, or policies; or
2. i. Is controlled by an entity that is not a health plan; and
   ii. If it has a subhealth plan(s) (as defined in this section), exercises
   sufficient control over the subhealth plan(s) to direct its/their
   business activities, actions, or policies. (45 CFR 162.103)

Note: The relationship between a CHP and SHP is a recent revision to the
regulations. This would apply to the state Medicaid plans and the
administration, if part of the administration takes place at the local level. The
relationship between the state (CHP) and the local administration (SHP) is not a
BA, as it meets the Business Associate definition exclusion at (4)(iii). This is particularly relevant where the local level also provides the health care service or contracts out for the services, which meets the exclusion provision of 45CFR §160.103 “Business Associate (2)(ii)(B)(1 and 2)”. These relationships should use “other arrangements” to meet the mandate at 45 CFR §164.314(a).

**Health Care Clearinghouse.** Means a public or private entity, including a billing service, re-pricing company, community health management information system or community health information system, and “value-added” networks and switches that does either of the following functions:

1. Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

2. Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity. (45 CFR 160.103)

**Health Care Provider.** Means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business. (45 CFR 160.103)

And...

**Transaction.** Means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

1. Health care claims or equivalent encounter information.

2. Health care payment and remittance advice.

3. Coordination of benefits.

4. Health care claim status.

5. Enrollment and disenrollment in a health plan.

6. Eligibility for a health plan.
7. Health plan premium payments.

8. Referral certification and authorization.


10. Health claims attachments.

11. Health care electronic funds transfers (EFT) and remittance advice.

12. Other transactions that the Secretary may prescribe by regulation. *(45 CFR 160.103)*

The provider definition is very broad and includes non-traditional services such as acupuncture or case management, so a general rule of thumb usually works: if it looks like some kind of health care, it probably meets the definition.

To obtain the named specific providers, the privacy professional must go to the Social Security Act. This is a long list. The 1395x(s) referenced above includes seventeen specified services with dozens of subsets and clarifications, while the 1395x(u) says “hospital, critical access hospital, skilled nursing facility, comprehensive outpatient rehabilitation facility, home health agency, hospice program….”

Secondly HIPAA, the Act, defined the “transactions” in general terms, so to be qualified as a covered “provider” under HIPAA, it is not required that they meet the Transaction and Code Set criteria (content, terminology, transmission criteria…) to be “transmitting”, just the general descriptions listed above.

**Documentation**

Once an entity has determined they are a CE, they should document (policy) what type of CE they have determined applies to them. The standards, implementation specifications, and organizational requirements for a provider are different than a health plan or clearing house. Only by documenting the determination can the privacy professional create the baseline compliance tools to develop an appropriate privacy program including auditing or monitoring daily activities.

**Other HIPAA Entity Designations**
Some business arrangements do not clearly fall into the three definitions, but are intimately related to HIPAA-covered functions. To account for this, HHS included some definitions for complex business relationships.

Hybrid Entity. Means a single legal entity:

1. That is a covered entity;
2. Whose business activities include both covered and non-covered functions; and
3. That designates health care components in accordance with paragraph §164.105(a)(2)(iii)(D). (45 CFR §103)

An example might be a university that runs a community clinic. The clinic information could easily be covered by HIPAA, yet the educational records are not. The entity can self-declare itself a Hybrid CE and then document which parts perform covered functions and which ones do not.

Documentation

Another element to be documented for the Hybrid designation is if PHI or IIHI flows out of the covered division into a non-covered division for a support activity such as General Counsel or Auditing. These divisions, while still part of the same legal entity may, like a business associate discussed below, perform functions on behalf of the covered division. They are part of the same legal entity so any data that flows from the covered division to the non-covered division must meet the “disclosure” provisions such as Minimum Necessary. While not a Business Associate relationship because they are part of the same workforce, the CE division must get “assurances” that meet the specifications at 45 CFR §164.314(a).

Business Associates (BA). The BA is probably the most familiar arrangement that an external party would participate in with a HIPAA CE. However the privacy professional should note that the BA describes a particular type of relationship and should not be used if the relationship does not meet the definition. Additionally BAs are directly liable for compliance with certain of the HIPAA Privacy and Security Rules’ requirements.

Business Associate:
1. Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:

   i. On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing, or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or:

   ii. Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

2. A covered entity may be a business associate of another covered entity.

3. Business associate includes:

   i. A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.

   ii. A person that offers a personal health record to one or more individuals on behalf of a covered entity.

   iii. A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

4. Business associate does not include:
i. A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

ii. A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met.

iii. A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.

iv. A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services. (45 CFR 160.103)

Note: To ensure that HIPAA CEs extend the privacy and security standards to contractors (downhill data flow), the concept of the BA was added to the HIPAA Security and Privacy Rules. A mandate is placed on the CE to either get “assurances” for privacy and security standards from their business partners or to include BA language to a contract.

The BA relationship is defined where a separate legal entity uses or discloses PHI on behalf of the CE. Usually, the BA relationship looks like claims processing, data analysis, billing, benefit management, quality assurance, quality improvement, practice management, legal, actuarial, accounting, accreditation or other administrative services. This is not an exhaustive list of functions and the relationship should be reviewed from the standpoint of the information handled: if it is individually identifiable information going outside of your legal boundary, you are half way to the BA relationship.

In general, if the other entity is:

- Part of the same legal entity (hybrid)—get assurances—not a BA, as per 45 CFR 164.314(a).
Not part of the same legal entity and is using/disclosing on the CEs behalf it is BA.

A BA, it should specifically spell out the permitted uses and disclosures.

Be wary if a state/fed or fed/fed mandate on the CE data would make a particular use or disclosure “illegal” for the CE, is still illegal for the BA to perform (other party’s research, sharing or giving of PHI to BA...).

Not part of the same legal entity, *neither* using nor disclosing on the CEs behalf, but providing services, a service contract with privacy/security clauses will meet the 164.314(a) provision of “assurances.”

**Note:** There was a perceived weakness of BA contract enforcement, which was addressed by the language in the Health Information Technology for Economic and Clinical Health (HITECH) Act. The BA is now responsible for their own violations of an Administration Simplification provision (45 CFR §160.402(a)). The mandate on a CE to establish assurances or institute the BA language still exists, but the legal liability for violations, and possible penalties, flow directly via the contract tool to the entity that violates the rule.

Although there is no mandate, there is still much debate on how to perform due diligence to detect if a BA is abiding by Administration Simplification. One thing the privacy professionals should be aware of is the requirement that a BA pass down the identical requirements to any subcontractor they utilize.

The author’s opinion is that the BA language/contract/amendments have probably been over used. In the maturation of the industry, the early stages were fraught with inserting BA language in everything. This was not unreasonable to reduce perceived risk, as the industry had no clear idea of how penalties would work. Everyone was over cautious and leapt into BA language “just in case.” Legal debates over whose BA language to use and which party was the BA were wide spread. Many institutions still do not fully grasp the intent of the 164.314(a) mandate.

**Organized Health Care Arrangement.** Means—

1. A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;

2. An organized system of health care in which more than one covered entity
participates and in which the participating covered entities:

i. Hold themselves out to the public as participating in a joint arrangement; and

ii. Participate in joint activities that include at least one of the following:

   A. Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

   B. Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

   C. Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

3. A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;

4. A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or

5. The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans. (45 CFR 160.103)

Note: Typically an OHCA is a clinically integrated care setting where individuals
receive health care from more than one health care provider. The definition also applies when more than one CE who participate in care but hold themselves out to the public as participating in a joint arrangement. An OHCA must also participate in joint activities and do one of the following: utilization review; quality assessment and improvement activities; or payment activities.

An OHCA could be a group health plan, a health insurance issuer or health maintenance organization (HMO) with respect to such a group health plan. But that classification is only in terms of PHI created or received that relates to individuals who are or who have been participants or beneficiaries in such a group health plan.

An OHCA could be a group health plan and one or more other group health plans that are maintained by the same plan sponsor, but only where PHI is created or received by insurance issuers that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

**Affiliated Covered Entities.** Are “Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of this part.” ([45 CFR §164.105(b)(1)](https://www.gpo.gov/fdsys/content/getdoc.pdf?pdfurl=https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/codeset/index.html))

**Note:** These are legally distinct entities that share common control or common ownership and choose to designate themselves as one affiliated CE for the purposes of complying with the HIPAA Privacy standard. Affiliated entities must meet the same requirements as a single CE, but this designation allows for things like the Notice of Privacy Practices and Privacy Policies and Procedures to be held in common as long as they all agree to abide by them. There is a similarity to the long standing Qualified Service Organization (QSO) for federally supported Alcohol Drug program subject to [42 CFR Part 2, the key being separate legal entities.](https://www.gpo.gov/fdsys/content/getdoc.pdf?pdfurl=https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/codeset/index.html)

**HIPAA Covered Data**

Once it is determined that an entity meets the HIPAA CE criteria and some of the relationships are defined, the entity must identify what information is covered, where it resides, and how it utilizes the information. It is important that a privacy program be based on the information use and data flow so that the program can support elements such as where an authorization is required or detect violations such as unauthorized disclosure.
Definitions

The following definitions describe parts of a diagram (below), followed by other data definitions that affect the determination of HIPAA covered data.

Health Information. Means any information, including genetic information, whether oral or recorded in any form or medium, that:

1. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. (45 CFR 160.103)

Individually Identifiable Health Information (IIHI). Is information that is a subset of health information, including demographic information collected from an individual, and:

1. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
   
   i. That identifies the individual; or

   ii. With respect to which there is a reasonable basis to believe the information can be used to identify the individual. (45 CFR 160.103)

Protected Health Information (PHI). Means individually identifiable health information:

1. Except as provided in paragraph (2) of this definition, that is:
   
   i. Transmitted by electronic media;

   ii. Maintained in electronic media; or
iii. Transmitted or maintained in any other form or medium.

2. Protected health information excludes individually identifiable health information:

   i. In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

   ii. In records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and

   iii. In employment records held by a covered entity in its role as employer;

   iv. Regarding a person who has been deceased for more than 50 years. (45 CFR 160.103)

**Electronic Protected Health Information (EPHI).** Means information that comes within paragraphs (1)(i) or (1)(ii) of the definition of protected health information as specified in this section. (45 CFR 160.103)

**Note:** The following two definitions reside in the middle of the regulation and not in one of the sections reserved for definitions.

**De-identified Information.** This means information that does not identify an individual and which there is no reasonable basis to believe that the information can be used to identify an individual.

Health information is not individually identifiable health information only if either a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable who:

1. Applies such principles and methods and determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and documents the methods and results of the analysis that justify such determination; or

2. (i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

   **A. Names;**
B. All geographic 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: The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

C. 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;

D. Telephone numbers;

E. Fax numbers;

F. Electronic mail addresses;

G. Social security numbers;

H. Medical record numbers;

I. Health plan beneficiary numbers;

J. Account numbers;

K. Certificate/license numbers;

L. Vehicle identifiers and serial numbers, including license plate numbers;

M. Device identifiers and serial numbers;

N. Web Universal Resource Locators (URLs);

O. Internet Protocol (IP) address numbers;

P. Biometric identifiers, including finger and voice prints;
Q. Full face photographic images and any comparable images; and

R. Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and

(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is subject of the information. (45 CFR 164.514 (a) (b))

**Limited Data Set.** A CE may use or disclose a limited data set if the CE enters into a data use agreement with the following direct identifiers of the individual or of relatives, employers, or household members of the individual removed:

- Names;
- Postal address information, other than town or city, state, and zip code;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers/serial numbers or 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; and
• Full face photographic images and any comparable images. *(45 CFR 164.514(e)(3)(i))*

**Note:** One of the proposed uses of De-Identified and Limited Data Sets is to make them available for research purposes. However, combined with publicly available information, especially in small population centers, it may be possible to re-identify the individual. This is of concern for the privacy professional as, while using the data is a permissive, it may not be foolproof from re-identification.

**Unsecured Protected Health Information.** Means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5. *(45 CFR 164.402)*

**Note:** To put HIPAA covered information in context, think of the HIPAA Rules as looking at increasingly smaller sets, or classifications, of information.

**All Information;** Literally every piece of information your entity has in its possession or has access too.

• **Health Information;** Every piece of health, and health related information.

• **Individually Identifiable Health Information (IIHI);** Health information that identifies an individual or can be used in combination with other information to identify an individual.

• **Protected Health Information (PHI);** Health information that is transmitted in one of the covered HIPAA transactions.

• **Electronically Protected Health Information (EPHI):** this is a subset that is covered by some specialized standards in the HIPAA Security Rule.
In the lower right corner of the graphic is the EPHI.

One thing to consider is that if the EPHI cannot be segmented from the universe of information, the entity may have to protect all information to the same degree as the HIPAA data—or provide greater protections if state or federal law demands it. Further, it is the author’s opinion that the electronic health records will not be able to provide segmentation by specific definitions or regulation for some time to come. The privacy professional should know what elements within an electronic record constitute: the legal record, the medical record, the Designated Record Set, or any other mandated definition that creates a subset from the record. The latter is important in meeting some state’s regulations.

Once information has been determined to be covered by HIPAA, the privacy professional must ferret out where the information resides and what the use of the information is. This identification process plays a part in doing the Risk Analysis (RA). The RA is required by the HIPAA Security Rule and should not be skipped by the privacy professional, just because the RA is a “security thing.”

**Note:** The Security Rule at 45 CFR §164.306(a)(3) says “Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.” Part E is the Privacy Rule. To implement the Security Rule, the privacy professional must be able to communicate to the security professional exactly what the uses and disclosures will be, any mandates such as a required authorization and predict what failures would look like so that electronic detection mechanism may be utilized. In this way the Risk Analysis fulfills its intent by capturing all risks,
not just risks to the system 45 CFR §164.306(a)(1) or data 164.306(a)(2).