Health Insurance Portability and Accountability Act (HIPAA) Frequently Asked Questions

May 2016

DaSy Center

DaSy The Center for IDEA Early Childhood Data Systems

The contents of this report were developed under a grant from the U.S. Department of Education, #H373Z120002. The contents do not necessarily represent the policy of the U.S. Department of Education, and you should not assume endorsement by the Federal Government. This document is for information purposes only, and is not legal advice or a substitute for legal counsel. Readers should refer to their own legal counsel to ensure adherence to HIPAA and related regulations applicable to their specific circumstances. The information contained in this document is intended to be current as of April 1, 2016, and may not reflect the most current legal developments.

May 2016

Suggested citation:
Center for IDEA Early Childhood Data Systems (2016). *Health Insurance Portability and Accountability (HIPAA) Frequently Asked Questions*. Menlo Park, CA: SRI International.

Contents

Introduction

The purposes of this document are to provide an orientation to the Health Insurance Portability and Accountability Act (HIPAA)[1] for IDEA Part C early intervention and IDEA Part B preschool special education agencies, programs, and service providers, and to highlight the aspects of HIPAA that may be most relevant for these early childhood programs under IDEA. DaSy has received many questions regarding when and whether HIPAA data privacy requirements apply to IDEA Part C early intervention and Part B 619 preschool. Like many topics in the public policy world, there is not always a simple answer. Given the different organization of early intervention and preschool special education from state to state and the variability in the structure and responsibility for service delivery, the response to many questions about HIPAA requirements is, "It depends."

Determining whether HIPAA requirements apply depends largely on where the information in question resides, what type of information is in question, and who maintains the information. Sorting out these key factors, in many cases, will simplify and clarify this task. This FAQ provides the basic information needed to begin to sort through the relevant factors needed to determine whether HIPAA or FERPA apply, but it is always important to check your local resources and Federal Resource Centers.

This document of Frequently Asked Questions (FAQs) is organized in two sections.

- The first section provides some working knowledge of what HIPAA is and what it is not. The answers to the FAQs in this section provide context and reference points for the wide range of HIPAA regulations and requirements.
- The second section focuses on ways HIPAA and the Family Educational Rights and Privacy Act (FERPA) may overlap or interact. The information in these FAQs is offered as a tool to help sort through the particulars of your early intervention and preschool special education system and determine areas where HIPAA requirements might apply. The FAQs will likely not provide "the answer" but should help you focus your questions on the relevant and specific circumstances needed to get the answer.

Finally, here are some cautionary notes on the use of these FAQs.

- The information provided should be used as a guide or starting point, not as a substitute for careful analysis of the particular circumstances of a state or local agency or program.
- The information does not constitute legal advice. We urge states, local agencies, programs, and providers to consult with their attorneys when making determinations on when individually identifiable information is or is not covered by HIPAA requirements.
- The questions and answers provided in this document reference the intersection of HIPAA and FERPA[2] but should not be considered a definitive reference on FERPA requirements. The Privacy Technical Assistance Center and the U.S. Department of Education Family Policy Compliance Office (FPCO) both provide a wide range of resources and information about FERPA.

[1] See: http://www.hhs.gov/ocr/privacy/

[2] The Family Educational Rights and Privacy Act (FERPA) establishes requirements for the protection of information held in education records.

Section I: HIPAA FAQs

1. What is HIPAA and why does it matter to me?

We hear references to "HIPAA" all the time. Typically we assume that the term is synonymous with "privacy." In most everyday settings, "HIPAA" likely does refer to "HIPAA privacy." However, within the operating framework of Part B 619 and Part C, it is important to remember that HIPAA is multi-faceted and that HIPAA regulations encompass more than just privacy.

IDEA Part C early intervention and IDEA Part B preschool special education agencies, programs, and service providers frequently interact with HIPAA "covered "entities," which are typically health care providers (see question 4, below). Children in these programs may receive services from these covered entities and you may need to exchange and share information with them.

In the course of business, covered entities may reference "HIPAA requirements," but the requirements they reference may or may not be privacy requirements. As mentioned above, there are several parts to HIPAA. Some deal with how a health care provider sends bills to insurers and receives payment from them. Some have to do with when and how to report incidents that compromise the integrity of the Information Technology (IT) system. Other requirements specify security measures for health IT systems and set penalties for failure to comply with HIPAA provisions.

The information below is meant to provide a basic framework for understanding the different HIPAA requirements and to provide a basis for asking the right questions when you encounter them.

1.1 HIPAA Background

In order to improve the efficiency and effectiveness of health care transactions, Congress enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This Act (1) created certain new health insurance protections and requirements and extended some existing provisions; and (2) established the requirement for health care entities to use certain standards when exchanging information electronically. The Act also established the process by which those standards would be set.

Congress recognized that it was important to protect information stored and transmitted electronically. As a consequence, HIPAA also included mandates that privacy protections be established within a specified timeframe.

Provisions of the law are implemented through a series of regulations collectively known as "HIPAA Administrative Simplification Regulations." These can be found in 45 CFR Parts 160, 162, and 164.

1.2 HIPAA Requirements[3]

Table 1. HIPAA Requirements and Descriptions of Requirements

HIPAA Requirement	Description
HIPAA Transactions and Code Sets	The Department of Health and Human Services establishes, through rule making, specific requirements for how health care diagnoses and procedures are described and for how this information is formatted and transmitted electronically.
HIPAA Privacy	45 CFR Part 160 and Subparts A and E of Part 164 The Privacy Rule establishes national standards for the use and disclosure of personally identifiable health information and for the protection of that information.
HIPAA Security	45 CFR Part 160 and Subparts A and C of Part 164 The Security Rule establishes national standards for technical and non-technical safeguards necessary to protect personally identifiable health information held in an electronic format. In general, if agencies or providers are in compliance with HIPAA security requirements, they would also be considered compliant with FERPA's "reasonable methods" requirements.
HIPAA Breach Notification	45 CFR §§ 164.400-414 The Breach Notification Rule sets requirements for notification of individuals, the public, and the U.S. Department of Health and Human Services (DHHS) when an impermissible use or disclosure of unsecured protected health information occurs.
HIPAA Enforcement	45 CFR Part 160, Subparts C, D, and E The Enforcement Rule lays out requirements relating to compliance with HIPAA regulations and the conduct of investigations, and establishes civil money penalties for violations and the procedures for hearings. These provisions apply to HIPAA Privacy and Security Rules as well as to other HIPAA Administrative Simplification regulations.

2. I've heard about "new" HIPAA requirements and something called the "Omnibus Rule." What are those about?

The "Omnibus Rule" has to do with the Health Information Technology for Economic and Clinical Health (HITECH) Act. In 2009 Congress passed the Health Information Technology for Economic and Clinical Health (HITECH) Act, as part of the American Recovery and Reinvestment Act. The law modified some provisions of the original HIPAA statute, established additional requirements, and provided more specific legislative direction in some areas. The HIPAA "Omnibus Rule," published in January 2013, modifies provisions in the Privacy Rule, the Security Rule, and the Enforcement Rule to incorporate relevant requirements of the HITECH Act.

[3] Additional information is included in the Appendix.

3. My state has enacted health privacy laws. Some of the provisions are different from HIPAA privacy provisions. How do I know what applies?

In general, HIPAA provisions are considered a "floor" of federal privacy protections. If state laws provide greater privacy protections, the state law applies.

A state law provision is preempted if it is contrary to HIPAA provisions. A provision is considered contrary if it is impossible to comply with both the HIPAA requirements and with state requirements, or if the state law "stands as an obstacle to the accomplishment and execution of the full purposes and objectives" of HIPAA provisions.

The HIPAA rule provides a number of exceptions to the general applicability of the preemption provision. The rule specifies certain conditions under which preemption might not apply to a state law provision and establishes a process for states to apply to the U.S. Department of Health and Human Services (DHHS) for an exception for that provision of law. The Secretary of the DHHS is the deciding authority for exception determinations. (Part 160 Subpart B § 160.202)

Questions about specific state privacy requirements and how they relate to, or are affected by, HIPAA requirements should be addressed in consultation with legal counsel.

4. Who has to comply with HIPAA?

HIPAA legislation established groups designated as "covered entities." This is an important definition for state and local agencies and programs to understand and a critical question for programs and service providers under IDEA Part C and Part B 619. Determination of whether or not a state or local agency, program, or service provider is a "covered entity" should be made in consultation with the agency's or provider's attorney.

It is also important to know that an entity might be a "covered entity" under one—but not all—HIPAA requirements. (See Question 11)

Covered entities are defined as:

- Health plan: individual or group plan that provides or pays for health care
- Health care clearinghouse: entities that convert nonstandard information into the standard format required for electronic transmission
- Health care provider: any individual or group who provides health care services and who transmits health care information electronically for HIPAA covered services

5. What is a "Business Associate"?

Business associates are entities that provide services involving the use of protected health information on behalf of or to a covered entity. (Definition at 45 CFR 160.103) HIPAA rules require that contracts between the covered entity and business associate include certain elements, including "the permitted and required uses and disclosures of protected health information by the business associate." 45 CFR 164.504 (e)(2)(i)

While they are not defined as covered entities, under the 2001 HITECH Act business associates are required to comply with some HIPAA requirements and are subject to enforcement actions and penalties for violations of those requirements.

Examples of business associates include:

- An external entity that helps the agency with claims processing and billing third party reimbursement such as Medicaid or private insurance
- A private legal firm that has access to Protected Health Information (PHI) in the course of its work for the agency
- A technology company that has access to PHI while working on fixes to a state data system

These companies or individuals performing these services are considered HIPAA business associates only if they are performing them for a HIPAA covered entity.[4]

6. Does HIPAA apply to entities that do not receive federal funding?

Yes. None of the HIPAA requirements is conditioned on receipt of federal funding. Entities are "covered entities" based on specifications included in the HIPAA Rules. (See Question 4)

7. What kind of information is protected under HIPAA?

HIPAA regulations refer to "protected health information" or PHI. Protected health information is defined in the rule as "individually identifiable health information." (Part 160 Subpart A § 160.103)

HIPAA privacy protections do not extend to individually identifiable information contained in education records (See Section II for more information on this topic.)

PHI includes any individually identifiable information about physical or mental health conditions, any health care (services, treatments, diagnostic tests, etc.), and payments made for or on behalf of an individual if it can be directly or indirectly linked to the individual.

PHI also includes demographic information and common identifiers, such as name, address, and birth date, if those identifiers can be associated with the individual's health information. The relationship of individual identifiers with health information is deemed "fundamental" by the Office for Civil Rights because absent that linkage, the identifiers would not be considered protected health information. For instance, the inclusion of a child's name in a hospital directory is not a HIPAA privacy violation because the child's name is not linked to any protected information about his or her health condition or treatment.

8. Does the HIPAA Privacy Rule require authorization from individuals before their information can be shared?

The HIPAA Privacy Rule defines and limits how an individual's health information may be used. In general, the use or disclosure of an individual's protected health information is prohibited without prior authorization from that individual. (See exceptions in Question 9, below.)

Prior authorization must be written in plain English and be specific about what information will be disclosed, the entity that will receive the information, and the purpose for which the information is disclosed. It must include an expiration date for the authorization.

A covered entity may not require an individual to grant an authorization as a condition for receiving services. For example, a physician conducting research on a particular condition or treatment may ask an individual for authorization to include PHI in that research. But the doctor may not require such authorization for the individual to receive the doctor's health care services.

[4] Additional information is included in the Appendix.

9. When can HIPAA-protected information be used without an individual's authorization?

The HIPAA Privacy Rule establishes categories of information use that do not require prior authorization from an individual. These categories are called "required disclosures" and "permitted disclosures."[5]

"Required disclosures" are those that a covered entity must provide. They include:

Disclosure, upon request, to an individual or their personal representative for access to their own information, or for an accounting of any entity who has received their PHI (accounting for disclosure)

- Disclosure to DHHS when it is engaged in a compliance investigation or review of enforcement action

"Permitted uses and disclosures" are those that a covered entity is allowed to make without prior written authorization. There are five general categories of permitted uses. The permitted uses most likely relevant to IDEA Part C early intervention and IDEA Part B preschool special education agencies, programs, and service providers are those in the category "treatment, payment, and health care operations."

In general, the "treatment, payment, and health care operations" category involves uses necessary for a covered entity:

- To treat patients (e.g. consult with a specialist on appropriate procedures to use on a patient)
- To get paid for services (e.g. send information to an insurance company to support a bill for services provided to a patient)
- To perform a range of activities necessary to operate and manage a business (e.g. quality improvement activities, performance evaluation, credentialing and accreditation, medical reviews, audits, etc.)

Additional information about the other four permitted categories is provided in the appendix (See Question 9). They are:

- Opportunity to agree or object
- Incident to an otherwise permitted use and disclosure
- Public interest and benefit activities
- Limited data set

[5] Additional information is included in the Appendix.

Section II: HIPAA/FERPA FAQs

10. Is PHI contained in education records subject to HIPAA privacy requirements?

In almost all cases the answer is no; personally identifiable health information contained in education records covered by FERPA is not covered by HIPAA privacy requirements. That information is covered by FERPA privacy requirements.

The HIPAA rule specifically excludes information held in education records from the definition of PHI:

> "(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)"

In 2008, the Departments of Education and Health and Human Services published joint guidance entitled: "Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records."

This guidance expands on the intersection of FERPA and HIPAA rules, stating:

> "When a school provides health care to students in the normal course of business, such as through its health clinic, it is also a "health care provider" as defined by HIPAA. If a school also conducts any covered transactions electronically in connection with that health care, it is then a covered entity under HIPAA. As a covered entity, the school must comply with the HIPAA Administrative Simplification Rules for Transactions and Code Sets and Identifiers with respect to its transactions. However, many schools, even those that are HIPAA covered entities, are not required to comply with the HIPAA Privacy Rule because the only health records maintained by the school are "education records" or "treatment records" of eligible students under FERPA, both of which are excluded from coverage under the HIPAA Privacy Rule. See the exception at paragraph (2)(i) and (2)(ii) to what is considered "protected health information" (PHI) at 45 CFR § 160.103. In addition, the exception for records covered by FERPA applies both to the HIPAA Privacy Rule, as well as to the HIPAA Security Rule, because the Security Rule applies to a subset of information covered by the Privacy Rule (i.e., electronic PHI)." (p. 3)

This guidance provides additional information in the form of FAQs addressing particular situations and providing additional information about the applicability of FERPA and/or HIPAA requirements. Some of these FAQs of relevance to IDEA Part C early intervention and IDEA Part B preschool special education agencies, programs, and service providers are included in Question 14.

11. How do I know if the information I have is covered by HIPAA or FERPA?

The HIPAA Privacy Rule specifically excludes records "subject to, or defined in" the Family Educational Rights and Privacy Act, 20 U.S.C. section 1232g.

In general, as long as the individually identifiable health information is maintained only in an education record, and not combined for other purposes with other health records for that child, then that

information would be subject to the requirements contained in IDEA Part C, IDEA Part B 619, and FERPA, but not in HIPAA.

It is important to know that while HIPAA privacy provisions may not be applicable, other HIPAA requirements may apply. For instance, HIPAA electronic transactions standards would probably apply if the information contained in the education record is transmitted electronically for billing purposes.

Two questions can serve as a starting point for determining what information is covered and by which HIPAA requirements. It is important to remember that an entity may be subject to some, but not all, HIPAA requirements.

- First, ask whether the agency or provider that holds the information is a HIPAA-covered entity. For example, a local therapy provider delivers physical and occupational therapy services to Part C children. The provider bills private insurers, Medicaid, and/or the state lead agency electronically (depending on various reimbursement circumstances). This provider *would* be considered a HIPAA-covered entity under the Transactions and Code Sets requirements. In other words, the provider would have to submit bills and receive payment using the electronic standards set out in HIPAA Transactions and Code Sets regulations.
- Second, ask where the patient/client information resides. What kind of record contains the information about the services being billed? Continuing with the example of the local therapy provider referenced above, this provider maintains all of the children's early intervention information in an education record. In this case the provider *would not* be considered a covered entity under the HIPAA Privacy Rule and would not have to meet HIPAA privacy requirements.

12. What about early intervention counseling or psychotherapy records and HIPAA rules? What rules apply? Is there a difference between official progress notes and personal notes?

If the counseling records are part of an education record, they would be covered by FERPA protections and not by HIPAA.

There is generally no distinction among types of information in terms of HIPAA Privacy Rule protections. There is one exception, however. The Privacy Rule provides special protections to "psychotherapy notes."

Applying this provision will probably be rare in the Part C and Part B 619 contexts. But it is worth noting that the HIPAA regulation defines psychotherapy notes in fairly broad terms:

> "Psychotherapy notes means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record." (Part 164 Subpart E § 164.501)

Under HIPAA, disclosure of information contained in psychotherapy notes can only be made with a HIPAA compliant authorization for disclosure. (This authorization must be in writing and specify what information is being released as well as the purpose for release and permitted use of the information.) The HIPAA "permitted" uses do not apply to this category of protected health information.

13. Some states require proof of immunization before a child can be enrolled in a preschool, child care, and/or kindergarten. Do HIPAA requirements apply to a child's immunization record?

Yes, immunization information included in a covered entity's health records is included under HIPAA privacy protections. However, once the immunization information is in an education record, it is no longer covered by HIPAA. The information is then covered under FERPA.

However, the U.S. Department of Health and Human Services recently revised relevant HIPAA regulatory provisions to make it easier for parents to give their permission to share immunization information. Health care providers must still obtain parental consent to share the child's immunization record, but the consent does not have to be a formal HIPAA compliant authorization for disclosure.

Parents can give their permission less formally, for instance in a note or e-mail to the doctor or clinic holding the record, or in a voice message left on office answering system. The health care provider must then document receipt of this parental consent, but the rule does not specify any particular format for that documentation.

HIPAA does not specify how the entity receiving the immunization records handles that information. The rule allows the state or local agency or program to determine where that information should reside.

14. What do I most need to know about the FAQs from "Joint Guidance on the Applicability of Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records"?

As previously mentioned, the Joint Guidance provides a set of Frequently Asked Questions about HIPAA and FERPA requirements and applicability. The link to the Joint Guidance is: http://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hipaa-guidance.pdf. Included below are four of these FAQs, which are likely to be of interest to IDEA Part C early intervention and IDEA Part B preschool special education agencies, programs, and service providers. All of 14.1 - 3 is a direct quote from Joint Guidance cited above:

14.1 Does the HIPAA Privacy Rule apply to an elementary or secondary school? (Joint Guidance Question 1)

Generally, no. In most cases, the HIPAA Privacy Rule does not apply to an elementary or secondary school because the school either: (1) is not a HIPAA covered entity, or (2) is a HIPAA covered entity but maintains health information only on students in records that are by definition "education records" under FERPA and, therefore, is not subject to the HIPAA Privacy Rule.

- The school is not a HIPAA covered entity. The HIPAA Privacy Rule only applies to health plans, health care clearinghouses, and those health care providers that transmit health information electronically in connection with certain administrative and financial transactions ("covered transactions"). See 45 CFR § 160.102. Covered transactions are those for which the U.S. Department of Health and Human Services has adopted a standard, such as health care claims submitted to a health plan. See the definition of "transaction" at 45 CFR § 160.103 and 45 CFR Part 162, Subparts K–R. Thus, even though a school employs school nurses, physicians, psychologists, or other health care providers, the school is not generally a HIPAA covered entity because the providers do not engage in any of the covered transactions, such as billing a health

plan electronically for their services. It is expected that most elementary and secondary schools fall into this category.

- The school is a HIPAA covered entity but does not have "protected health information." Where a school does employ a health care provider that conducts one or more covered transactions electronically, such as electronically transmitting health care claims to a health plan for payment, the school is a HIPAA covered entity and must comply with the HIPAA Transactions and Code Sets and Identifier Rules with respect to such transactions. However, even in this case, many schools would not be required to comply with the HIPAA Privacy Rule because the school maintains health information only in student health records that are "education records" under FERPA and, thus, not "protected health information" under HIPAA. Because student health information in education records is protected by FERPA, the HIPAA Privacy Rule excludes such information from its coverage. See the exception at paragraph (2)(i) to the definition of "protected health information" in the HIPAA Privacy Rule at 45 CFR § 160.103. For example, if a public high school employs a health care provider that bills Medicaid electronically for services provided to a student under the IDEA, the school is a HIPAA covered entity and would be subject to the HIPAA requirements concerning transactions. However, if the school's provider maintains health information only in what are education records under FERPA, the school is not required to comply with the HIPAA Privacy Rule. Rather, the school would have to comply with FERPA's privacy requirements with respect to its education records, including the requirement to obtain parental consent (34 CFR § 99.30) in order to disclose to Medicaid billing information about a service provided to a student.

14.2 Does FERPA or HIPAA apply to elementary or secondary school student health records maintained by a health care provider that is not employed by a school? (Joint Guidance Question 3)

If a person or entity acting on behalf of a school subject to FERPA, such as a school nurse that provides services to students under contract with or otherwise under the direct control of the school, maintains student health records, these records are education records under FERPA, just as they would be if the school maintained the records directly. This is the case regardless of whether the health care is provided to students on school grounds or off-site. As education records, the information is protected under FERPA and not HIPAA.

Some outside parties provide services directly to students and are not employed by, under contract to, or otherwise acting on behalf of the school. In these circumstances, these records are not "education records" subject to FERPA, even if the services are provided on school grounds, because the party creating and maintaining the records is not acting on behalf of the school. For example, the records created by a public health nurse who provides immunization or other health services to students on school grounds or otherwise in connection with school activities but who is not acting on behalf of the school would not be "education records" under FERPA. In such situations, a school that wishes to disclose to this outside party health care provider any personally identifiable information from education records would have to comply with FERPA and obtain parental consent. See 34 CFR § 99.30.

With respect to HIPAA, even where student health records maintained by a health care provider are not education records protected by FERPA, the HIPAA Privacy Rule would apply to such records only if the provider conducts one or more of the HIPAA transactions electronically, e.g., billing a health plan electronically for his or her services, making the provider a HIPAA covered entity.

14.3 Where the HIPAA Privacy Rule applies, does it allow a health care provider to disclose protected health information (PHI) about a student to a school nurse or physician? (Joint Guidance Question 5)

Yes. The HIPAA Privacy Rule allows covered health care providers to disclose PHI about students to school nurses, physicians, or other health care providers **for treatment purposes**, without the authorization of the student or student's parent. For example, a student's primary care physician may discuss the student's medication and other health care needs with a school nurse who will administer the student's medication and provide care to the student while the student is at school.

Appendix: Supplemental HIPAA Information

1. HIPAA Regulations (FAQ 1)

HIPAA Transactions and Code Sets

"Transactions" refer to the exchange of electronic information for specified purposes, for instance when a physician submits a claim for payment to an insurance company.

"Code sets" are specified terms used to describe health care diagnoses and procedures.

These standards are established through rulemaking by the Department of Health and Human Services. These rules also include specific requirements, called "implementation specifications" that facilitate the smooth flow of electronic transactions.

HIPAA Privacy

45 CFR Part 160 and Subparts A and E of Part 164
Congress recognized that the protection of personal information is an important consideration and directed the U.S. Department of Health and Human Services to make recommendations to Congress about the appropriate use of personally identifiable information and the rights an individual should have regarding his or her own health information.

The statute established a timeframe for Congress to act on those recommendations. Since Congress did not pass legislation within that timeframe, the U.S. Department of Health and Human Services established HIPAA privacy requirements through notice and comment rulemaking. The final HIPAA privacy regulation was published in August 2002.

The Privacy Rule establishes national standards for the use and disclosure of personally identifiable health information and for the protection of that information. The Office for Civil Rights (in the U.S. Department of Health and Human Services) is responsible for the administration and enforcement of HIPAA privacy provisions.

HIPAA Security

45 CFR Part 160 and Subparts A and C of Part 164
The law also required the U.S. Department of Health and Human Services to establish standards to ensure the security of protected health information. The HIPAA Security Rule essentially "operationalizes" the protections provided under the Privacy Rule. It establishes national standards for technical and non-technical safeguards necessary to protect electronic health information. Individuals and entities that hold and exchange electronic health information must comply with the provisions of this regulation.

The final Security Rule was published in February 2003 and further amended by the Omnibus Rule of 2013. The Office for Civil Rights is responsible for overseeing and enforcing provisions of the Security Rule.

In general, if agencies or providers are in compliance with HIPAA security requirements, they would also be considered compliant with FERPA's "reasonable methods" requirement.

HIPAA Breach Notification

45 CFR §§ 164.400-414
A "breach" is defined as the impermissible use or disclosure of unsecured protected health information (information that has not been made unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology). The Breach Notification Rule sets requirements for notification of individuals, the public, and the U.S. Department of Health and Human Services should a breach occur.

Requirements were set out in a series of guidance documents and an interim final regulation in 2009 and finalized in the 2013 HIPAA Omnibus Rule.

HIPAA Enforcement

45 CFR Part 160, Subparts C, D, and E
The HIPAA Enforcement Rule lays out requirements relating to compliance and the conduct of investigations, and establishes civil money penalties for violations and the procedures for hearings. These provisions apply to the HIPAA Privacy and Security Rules as well as to other HIPAA Administrative Simplification regulations.

Enforcement activities were governed by a series of Interim Final Rules from 2003 until February 2006 when the final Enforcement Rule was published.

Enforcement requirements were modified by the 2009 Health Information Technology for Economic and Clinical Health Act (HITECH). These requirements were incorporated into the Enforcement Interim Final Rule and finalized in the 2013 Omnibus Rule.

2. "Business Associate" (FAQ 5)

The Privacy Rule lists a number of functions, activities, and services typically performed by business associates. Functions include:

- Claims processing or administration
- Data analysis
- Processing or administration
- Utilization review
- Quality assurance
- Billing
- Benefit management
- Practice management
- Repricing

Services listed are:

- Legal
- Actuarial
- Accounting
- Consulting
- Data aggregation
- Management
- Administrative
- Accreditation
- Financial

3. "Permitted" Use and Disclosure without Prior Authorization (FAQ 9)

There are five general categories of permitted use:

Treatment, Payment, and Health Care Operations

(See FAQ 9)

Opportunity to agree or object

This is a category of uses where a covered entity may obtain informal approval (rather than HIPAA-compliant authorization) from an individual. Examples of uses in this category are inclusion of an individual's name in a hospital directory and permission to discuss treatment with a family member.

Incident to an otherwise permitted use and disclosure

A covered entity must adopt reasonable safeguards, but is not required to anticipate and eliminate any possible circumstance where disclosure might occur in the course of permitted activities. For instance, in an emergency room where patients are separated only by curtains, a health care provider may discuss an individual's treatment, even though a patient on the other side of the curtain might hear that discussion.

Public interest and benefit activities

There are 12 "national priority purpose" categories for which disclosure is permitted, but not required. While some of these may sound broad and open ended, each has specific conditions required for use of the category and/or limitations on types and use of PHI disclosed.

Required by law

- Public Health Activities
- Victims of Abuse, Neglect or Domestic Violence
- Health Oversight Activities
- Judicial and Administrative Proceedings
- Law Enforcement Purposes
- Decedents
- Cadaveric Organ, Eye, or Tissue Donation
- Research
- Serious Threat to Health or Safety
- Essential Government Functions
- Workers' Compensation

Limited data set

Data in what is called a 'limited data set' may be shared. The HIPAA rule defines a limited data set as "protected health information that excludes…direct identifiers of the individual or of relatives, employers, or household members of the individual." The rule specifies data elements that must be removed in order to qualify as a limited data set. The Privacy Rule also requires data use agreements between the covered entity and the recipient of the data set specifying uses of the information and safeguards for the data.

For more information, please see: http://www.hhs.gov/ocr/privacy/index.html