Do HIPAA Privacy and Security Laws Apply to College & University Student Health Clinics?

By Elizabeth Swinton Schoen, JD[1]

SUMMARY

Dramatic changes in our national and local health care systems and insurance markets have raised a key question for nearly all colleges and universities (collectively 'Universities' in this paper): **Do the "HIPAA Rules"[2] apply to student health clinics?**

Universities vary in their legal opinions on whether the Health Care Portability and Accountability Act of 1996 (HIPAA), including the new privacy and security rules in effect September, 2013,[i] applies to student health clinics. One common position is that the Family Education Rights and Privacy Act (FERPA) applies and HIPAA does not. A second perspective takes the position that HIPAA does apply, though the rest of the campus, as a 'Hybrid' entity, may continue under FERPA. A third, less common, conclusion is that neither HIPAA nor FERPA apply due to an exemption given to student "treatment records," a position which we argue creates potential liability for the University.

Why is this question important? If HIPAA Rules do apply to student health clinics, there are extensive administrative, physical and technical policies and safeguards required to protect the privacy interests of its students and, to the extent applicable, other patients. Failure to meet these requirements, even in a single instance, could result in significant financial penalties against the University. Universities operating under HIPAA are also responsible for affirming that "business associates", including EMR vendors, insurance companies, labs, etc. are compliant with HIPAA requirements. Additionally, as of September, 2013, business associates are independently liable for failure to maintain HIPAA Rules.[ii]

---

[1] **Liz Schoen, JD** specializes in HIPPA, Medicare, Medicaid and regulatory compliance issues. She is a graduate of Emory University School of Law and Connecticut College.

Medicat LLC, an EHR vendor serving the college health market, engaged E.S. Schoen & Affiliates to explore these important issues and present our findings in a whitepaper that could be of benefit to decision makers considering this important question. You can find contact information at medicat.com

[2] HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164

Remaining Conundrums: Because the application of these regulations is relatively new, especially those in effect as of September, 2013, there are a number of grey areas regarding the application of HIPAA or FERPA that remain untested by regulatory agencies. To sort through these widely contrasting perspectives and conundrums, one needs a basic understanding of the HIPAA and FERPA laws. This paper will review those basics and then address practical questions that have been raised by student health center staff or University counsel who are struggling with the HIPAA vs. FERPA dilemma.

Lastly, given the major changes in our health care clinics and insurance marketplace, we consider whether applying HIPAA to student health clinics as a long-term objective may ultimately be a good practice for Universities and their business associates, even if current regulations clearly permit compliance under FERPA.

Disclaimer: This Paper was drafted for non-attorneys and is not intended as legal advice. It provides the reader with an overview of the HIPAA and FERPA regulations with respect to questions raised regarding student health clinics. It is recommended that the reader seek appropriate legal advice regarding the specific facts of their organization. This paper was prepared in September 2013. Future laws, regulations and policies may change. While some citations are made, others have been intentionally left out of the paper. Please send questions or comments to whitepapers@medicat.com.

Table of Contents

I. THE HIPAA BASICS

Since 1996, the enactment of HIPAA and its subsequent federal regulations, "covered entities" (e.g. hospitals, outpatient clinics, insurance companies, physician offices) have had to comply with the privacy and security requirements under HIPAA. Here are some basic HIPAA facts. [3]

a. What Do the HIPAA Rules Regulate?

The HIPAA Rules regulate privacy and security of "protected health information" (PHI) that is created, maintained and transmitted by "covered entities" or "business associates" as part of their healthcare operations. It is essential to understand that the privacy regulations apply to both non-electronic and electronic PHI which includes individually identifiable information such as names, social security numbers, diagnostic codes, demographic information). For example, the privacy regulations can apply to paper copies of medical records and billing information as well as electronic copies. In contrast, the HIPAA security regulations only apply to electronic health information (e-PHI). This is important since the security regulations are much more stringent than the privacy regulations.

b. How are PHI and e-PHI Defined?

HIPAA defines PHI as "individually identifiable health information" which is transmitted

- By electronic media;
- Maintained in electronic media; or
- Transmitted or maintained in any other form or medium.[iii]

Electronic PHI (e-PHI) is information that falls within the first two bullets above. Under HIPAA, "individually identifiable health information" is defined as information that relates to the past, present, or future health of an individual, or to the payment for the provision of health care to that individual, that either directly identifies the individual or provides reason to believe the information can be used to identify the individual.[iv]

c. What does HIPAA Apply to?

The HIPAA Rules apply to "covered entities" and "business associates." Covered entities include health care providers such as hospitals, outpatient clinics, physician practices, psychiatric clinics) as well as insurance companies like HMOs, Medicaid, Medicare, TriCare, Managed Care organizations.

The HIPAA Rules also apply to "business associates" of covered entities who are vendors of covered entities that provide a service to the covered entity and have access to the covered entity's PHI. Examples of business associates include:

- software companies that provide maintenance services for electronic health records;
- e-prescribing gateway companies or other entities that provides the transmission of data services involving PHI;
- attorneys, consultants and accountants who have access to their clients protected health information;
- shredding companies, transcription services, billing services;
- health information exchange organizations.

Entities not considered business associates. Entities that act as mere conduits for the transmission of PHI may not be considered business associates.[v] The government has provided the following example: data transmission organizations that act as mere conduits for the transport of PHI but do not access the information other than on a random or infrequent basis are not business associates.[vi]

The 2013 HIPAA Rules require that there be a written contract between a covered entity and their business associates[vii] and mandate that certain provisions be in the contract and that business associates are directly liable for non-compliance with HIPAA under the law of agency. [viii]

d. What are the Penalties for not Complying with HIPAA?

The penalties for not complying with HIPAA can be significant. The government has specifically stated that a covered entity or their business associate who "willfully neglect" to comply with HIPAA can be liable for as much as 1.5 million dollars.[ix] Liability can result not only from a specific breach of a patient's privacy and security but also for failing to comply with the administrative and technical safeguards of the HIPAA rules.[x] For example, failing to have required policies and procedures and train staff on the HIPAA rules could violate HIPAA laws.

Business associates and their subcontractors are now directly liable for HIPAA violations.[xi] For example, if a business associate such as an EMR vendor fails to comply with the HIPAA regulations, the covered entity can be directly liable for the business associates breaches as well as the business associate. This is what is termed "downstream" liability.

e. Who Enforces HIPAA?

Under HIPAA, Congress delegated to the U.S. Department of Health and Human Services (HHS) the authority to create regulations and enforce them. In 2009, HHS gave the regulatory and enforcement authority to the Office of Civil Rights (OCR) which has the authority to impose civil monetary penalties (CMPs) against a covered entity or business associate that fails to comply with the regulations.

This is significant since OCR does not have to file a lawsuit in federal court to impose fines against an individual or entity that breaches HIPAA.[xii] Rather, OCR only has to go through an administrative enforcement process. If a covered entity or a provider fails to appeal an adverse determination by OCR for HIPAA violations, the decision becomes final.[xiii]

f. Examples of What Covered Entities and Their Business Associates Must do to Comply with HIPAA?

Covered entities and their business associates must have appropriate administrative, physical and technical safeguards to comply with the HIPAA Rules.[xiv] These include having policies and procedures, conducting risk assessments, training staff, complying with the breach notification rules (and conducting internal investigations of each breach), and having written agreements between covered entities and business associates.

g. Encryption and Destruction: Two Exceptions to HIPAA's Breach Notification Rules

The 2009 and 2013 HIPAA regulations created extensive requirements that both covered entities and business associates must undergo if they suspect or are made aware of a potential breach of an individual or group's privacy or security.[xv] These rules further require that if there is a breach, the covered entity must notify the individual(s), the government, and if 500 or more records are involved, the media.[xvi]

There are two important exceptions to these rules: encryption and destruction. In 2009, HHS issued a guidance[xvii]identifying that encryption and destruction are two methods that render PHI "secure". As a result, HHS declared that use of these methods were exempt from the breach notification obligations, a practice that every covered entity or business associate should strive towards.

***Practice Tip for Covered Entities and Business Associates**: To avoid having to undergo the burdensome and potentially damaging process of notifying individuals and others of a breach, use of encryption is recommended in all transmissions of data (at rest and in motion) that would involve PHI. For example, all PHI for hosted Medicat clients are encrypted not only during transmission, but also within the database itself (at rest).*

h. What is a Hybrid Entity Under HIPAA?

The term "hybrid entity" refers to an entity that has both "covered" and "non-covered" entities in its business organization.[xviii] Under HIPAA, "covered functions" means a function that makes the entity a HIPAA covered entity (i.e., the entity is a health plan, a health care clearinghouse or a health care provider).[xix] A "health care component" is an operational component of a covered entity that uses or discloses protected health information. For example: a University may perform business activities that include both covered functions (e.g., owning and operating hospitals and student health clinics), and other non-covered health functions (e.g., university academic administration and residential halls.)[xx]

The 2013 HIPAA regulations now mandate that the healthcare component of a hybrid entity must include all relevant business associate functions within the entity (e.g. a university IT department supporting the health center's EMR system, including access to the health record database), who must also comply with HIPAA.[xxi]

THE FERPA BASICS

a. What is Regulated under FERPA and Who Regulates FERPA

The purpose of FERPA is to protect the privacy of student "education" records.[xxii] FERPA applies to educational agencies and institutions that receive funds under any program administered by the Department of Education (DOE), including loans and grants to students.[xxiii] By this definition, nearly all private and public post-secondary institutions; including medical and other professional schools, fall under FERPA regulation.

b. "Education" Records under FERPA

FERPA regulates "education records" which is defined broadly. Education records include, but are not limited to, records that are:

- Directly related to the student;
- Maintained by an educational agency or institution or party acting for the agency or institution;
- Special educational records relating to disabilities under IDEA; and

- Records that do not qualify as "treatment records" since they have been disclosed for purposes other than treatment or shared with non-treating health care workers (this treatment record exception and its implications are addressed in detail below.)[xxiv]

c. What is "Personally Identifiable Information" under FERPA?

Some of FERPA's protections apply to "personally identifiable information" contained within education records. Personally identifiable information under FERPA includes, but is not limited to:

- the student's name;
- the name of the student's parent or other family members;
- the address of the student or student's family
- a personal identifier, such as the student's social security number, student number, or biometric record;
- other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
- other information, that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
- information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.[xxv]

d. What are the Penalties for Violating FERPA?

FERPA violations are complaint driven (e.g. can only be initiated if a complaint is filed by a student or parent).[xxvi] The DOE has the authority to pull funds issued by the DOE from an educational institution that violates FERPA.[xxvii] The termination of funding may only occur if the DOE determines that the University failed to comply with FERPA and that compliance cannot be accomplished voluntarily.[xxviii]

II. FRAMING THE ARGUMENTS AND UNDERSTANDING THE GREY AREAS

To understand the grey areas in the HIPAA vs. FERPA debate, it is necessary to understand how HHS defines "PHI." In defining "PHI", HHS created two exceptions: (1) "Education records" as defined under FERPA and (2) "Treatment records" as defined under FERPA[xxix].

a. "Treatment Records" – An Implausibly Narrow Exception

If a treatment record remains true to its very narrow definition as, "records on a student who is 18 years of age or older (i) made or maintained by a physician, psychiatrist, psychologist, or

other recognized professional or paraprofessional acting in his or her professional capacity or assisting in a professional capacity; (ii) made, maintained or used only in connection with treatment of the student AND (iii) disclosed only to individual providing the treatment."[xxx] they are not subject to either HIPAA or FERPA. Hence, such treatment records become a category unto themselves - a 'no man's land' where there is arguably no regulatory oversight by either HIPAA or FERPA. However, we believe that this definition is implausible to defend in practice.

b. "Treatment Records" in Practice – a Narrow Definition.

If a treatment record is disclosed by a university for reasons other than treatment (such as billing) or to persons not involved in the student's treatment, it becomes an "education" record and subject to FERPA.[xxxi] Even if no insurance billing is involved, we believe that student health records maintained within an EMR do not satisfy the strict definition of "treatment records." In our reading, the only way to truly satisfy the definition of "treatment record", is for each physician to keep the paper medical records of students she treats locked-up in her office and only share it with another physician who is directly involved with the treatment of that particular student and then only with the student's permission[xxxii]. In fact, sharing the paper chart with the student himself may violate the "treatment record" definition.[xxxiii]

An EMR system, by definition, provides general access to multiple, albeit with permission, health center staff to all student health records. Consequently, use of an EMR fails the definition of treatment records under FERPA because it violates the specific provider-to-patient direct treatment requirement.

With an EMR, these are "educational records" under FERPA (unless it is determined that HIPAA applies.). Additionally, providing students access to their own health records through a secure patient portal may further violate the treatment record standard.

As a result, those Universities who take the position that student health records are not subject to either HIPAA or FERPA because their student health records constitute "treatment" records may find themselves in a perilous position since the definition and practical application of treatment records are extremely narrow. Additionally, failure to comply with either HIPAA or FERPA on a technicality that clearly obviates the regulatory intent of both laws could leave that University exposed to potential liability in addition to negative publicity.

III. PRACTICAL QUESTIONS RAISED

We have divided these questions into three different categories.

A. Application of HIPAA vs. FERPA to Student Health Clinics
B. Disclosure of Student Health Records to External Providers and Insurance Companies.

C. An University's Use of Third Party Vendors to Manage or Support EMR Services.

A. Application of HIPAA vs. FERPA to Student Health Clinics.

1. When Does FERPA Apply to Student Health Clinics and When Does HIPAA Apply?

To answer this question, it is important to understand the difference between a health record (medical and billing information of a patient) and the type of entity that provides the medical services.

FERPA governs the type of record involved. In the context of a student health clinic, FERPA typically applies to a student health record since it would fall under the definition of an "education" record. Education records include records, files, documents, and other materials that contain information directly related to a student and are maintained by an educational institution**.**

But for the fact that a student health record qualifies as an "educational" record under FERPA, it would be subject to HIPAA. Additionally, a student health record cannot be subject to HIPAA and FERPA at the same time since the HIPAA law specifically exempts educational records from the definition of PHI.

In contrast, HIPAA governs both the type of record involved (excepting "education" and "treatment" records under FERPA) and the type of entity (e.g. "covered entities"). As a result, if a health record is not exempt under FERPA, HIPAA will apply if it meets the definitions of PHI and covered entities.

2. If not for FERPA, HIPAA Would Apply to a Student Health Clinic

a. Is a Student Health Clinic a Covered Entity Under HIPAA?

In order for HIPAA regulations to apply to it, a student health clinic must be a covered entity. Covered entities include health care providers who **transmit** any health information in electronic form in connection with the following types of transactions (*emphasis added*):

- health care claims or equivalent encounter information;
- health care payment and remittance advice
- coordination of benefits;
- health care claim status;
- enrollment and disenrollment in a health plan;
- eligibility for a health plan;
- health plan premium payments;
- referral certification and authorization;
- first report of injury;

- health claims attachments; and
- other transactions that the Secretary may prescribe by regulation.[xxxiv]

Do Student Health Clinics "Transmit" Health Information? Since the definition of covered entities requires an entity to "transmit" health information in electronic form, it is important to understand how the term "transmit" is defined. The way to understand how "transmission" is defined is by looking at the definition of "transaction."[xxxv] HIPAA defines "transaction" as a "transmission of information between two parties." Note that the definition does not define it as a transmission between two entities, but merely as one between two parties. Additionally, the definition of electronic media[xxxvi], the medium which information is transmitted in electronic format, explicitly includes intranets and private network. Included in this definition as well are other types of electronic media that can be used to move information between entities or within a single organization.

HIPAA does not provide a definition for the term "transmit." Since it is not a term of art, the common definition for the word should be used. The common use definition of the word "transmit" is very broad. By its definition, one may transmit information to another person through spoken word. Thus, student health clinics and their medical personnel likely transmit health information so long as they communicate health information in electronic form, even within the clinic, such as between a doctor and a nurse.

b. Are Student Health Clinics Health Care Providers Under HIPAA?

Under federal law, a health care provider is a provider of services (as defined in section 1861(u) of 42 U.S.C. 1395x(u), a provider of medical or health services (as defined in section 1861 of 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. By this definition, it appears that student health clinics and their employees fall within the definition of health care providers.

c. Is a Postsecondary Educational Institution a Hybrid Entity Under the HIPAA?

On its website under "Frequently Asked Questions," the Office of Civil Rights ("OCR") has addressed the issue of whether a post-secondary educational institution is a hybrid entity.[xxxvii] Specifically, in its answer to the question, OCR provides:

> "Yes. A postsecondary institution that is a *HIPAA* covered entity may have health information to which the Privacy Rule may apply not only in the health records of nonstudents in the health clinic, but also in records maintained by other components of the institution that are not education records or treatment records under *FERPA*, such as in a law enforcement unit or research department. In such cases, **the institution, as a *HIPAA* covered entity, has the option of becoming a "hybrid entity" and, thus, having the *HIPAA* Privacy Rule apply only to its health care unit. The school can achieve**

hybrid entity status by designating the health unit as its "health care component." (*Emphasis added*) As a hybrid entity, any individually identifiable health information maintained by other components of the university (i.e., outside of the health care component), such as a law enforcement unit, or a research department, would not be subject to the *HIPAA* Privacy Rule, notwithstanding that these components of the institution might maintain records that are not "education records" or treatment records under *FERPA*.[xxxviii]

3. HIPAA Implications If Treating Non-Students.

a. What if an Employee of the University receives health services at a Student Health Clinic?

If an employee of a University receives services at a student health clinic, that employee's health records are not subject to FERPA since they would not fall within the definition of "education record." HIPAA would apply to the employee's health record unless it falls under the employment exception to the definition of PHI under HIPAA. Like the education record exception, HIPAA regulations exempt from the definition of PHI, "employment records held by a covered entity in its role as an employer."[xxxix] Hence, if an employee of a University is receiving flu shots at a health clinic as part of a university wide employee safety mandate, HIPAA would not apply. However, if an employee of a University goes to a student health clinic at their discretion for an annual physical, the clinic would be subject to HIPAA since the provision of medical services is usually not a function related to employment.

b. What if a Patient is Both a Student and an Employee of the University?

If a patient is both a student and an employee of a postsecondary educational institution, that person's student health clinic medical records are subject to FERPA.

c. What if a Student Health Clinic Treats Patients Who Are Neither Employees nor Students, such as Family Members of Employees or the Public?

If a patient at a student health clinic is neither a student nor an employee, the protected health information held by the clinic is subject to HIPAA regulations because seeing these types of patients qualifies it as a covered entity. This information is not subject to FERPA since it falls outside the definition of "education" record. If seeing non-students, then the clinic is acting as a covered entity under HIPAA.

B. Disclosure of Student Health Records to External Providers and Insurance Companies, Including Student Health Insurance Plans.

1. What Happens when a Student Health Record is Disclosed to an External Provider as a Referral for Treatment?

For the University, the student health record would be considered an "educational record" under FERPA. If the University discloses the student health information to an external provider (such as another physician, clinic or hospital) then the record in the external provider's possession would be subject to HIPAA regulation since they would be considered a covered entity.

2. What Happens When a Student Health Clinic Bills a Third-Party Insurance Company?

Arguably, billing information in a student health clinic's possession is an education record since it applies directly to the student. Because a third party insurance company is defined as a covered entity,[xl] once the billing records are in the insurance company's possession, the insurance company would be subject to HIPAA. However, this is a grey area subject to future regulatory opinion by OCR. Arguably, the records at the educational institution would still be subject to FERPA.

If all the records being transmitted are education records, the health center is not subject to HIPAA by virtue of the transmission.

3. What Happens if a Student Health Clinic Uses a Third-Party Billing Services Vendor to Manage Insurance Claims?

In this scenario, the answer will depend on the type of records the third party billing company is managing. If the University sends billing records on non-students to process insurance claims, then it would clearly fall within HIPAA and there should be a written business associate agreement between the University and the billing company.

If the University only sends student records to a billing company to process claims, there is a strong argument that FERPA applies since under FERPA, an education institution can delegate the handling of student records. This too is a grey area and may ultimately be found subject to HIPAA in order to ensure that the vendor is protecting the privacy rights of the student.

***Practice Tip**: As a precautionary measure, it may be best to have a business associate agreement with the third party billing insurance company even if the University takes a FERPA position.*

***Sample language**: "Client's execution of the Business Associate Agreement does not constitute an agreement or admission that Client is a Covered Entity for purposes of HIPAA in the services transacted under this Agreement."*

C. A University's Use of Third Party Vendors for EMR

1. Is HIPAA implicated if a University purchases EMR Software and Maintains the Software and Database on the University's Server?

It depends on the type of health services and type of people that are served by the University health center. If the health center only provides health services to students, then the information contained in its EMR would be considered education records under FERPA, and therefore not subject to HIPAA since the HIPAA regulations explicitly provide that "education and treatment records under the FERPA laws are exempt from HIPAA" (Example A). If, however, the education client provides health services in its clinic to non-students, HIPAA would be implicated since records related to such services would not be specifically exempted under HIPAA, and therefore the education client would be considered a covered entity under HIPAA (Example B).

Maintaining the software on its own server implicates HIPAA only if the University provides health services to individuals other than students.

***Practice Tip**: It is important to note that if HIPAA applies, as in Example B, the EMR vendor would be considered a "business associate" subject to HIPAA requirements like a covered entity. Moreover, as a precaution, it would be good to have a business associate agreement with the EMR Vendor in both examples in case it was determined that HIPAA applied to Example A.*

2. What is Encryption and When Should it be Used to Protect Our Institution if the University is Hosting the Software and Databases?

Encryption is the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential key process. HHS has declared that the use of encryption is deemed secure and exempt from the breach notification requirements. It is recommended that covered entities should make efforts to encrypt all forms of its electronic health information, including intranets, compact disks, portable devices, cloud computing services, and emails.

Practice Tip: *As an industry best practice, it is recommended that Universities using e-PHI make encryption a mandatory standard with all of their vendors that host and transmit protected health information. For example, Medicat encrypts its data at rest for every hosted client with no exceptions.*

3. What Happens if a University Purchases EMR Hosted Software and the EMR Vendor Maintains the Database on the EMR Company's Server via the "Cloud"?

This is similar to the previous question in that if the University only uses student health information on its EMR software, then FERPA would apply. However, if they are using more than student data on its EMR system, HIPAA would apply.

If HIPAA applies, the key question is whether the EMR Company uses encryption software for data in motion and data a rest. It is important to note that HHS has deemed encryption as a "secure" method of maintaining and transferring data and therefore not subject to the stringent breach notification requirements under HIPAA. If the EMR Company has encryption software, then hosting it on a cloud would satisfy the HIPAA security requirements since HHS has declared that the information is "secure". However, the vendor is still subject to the other HIPAA requirements with respect to its role as a business associate. Business associates are responsible for complying with the HIPAA regulations and are independently liable to OCR for failing to do so.

4. What are the Implications of e-Prescribing through an EMR Vendor?

FERPA would apply to the University if it only retains and uses students' health information on its EMR software. Therefore, arguably, the EMR Company would not be a business associate of the University under HIPAA (although see recommended Practice Tip below regarding use of a "conditional" business associate agreements.)

However, if the University retains and uses non-student information on its EMR, HIPAA would apply. The 2013 HIPAA regulations specifically define business associates to include e-prescribing services. In this case, the e-Prescribing service company would be a subcontractor of the EMR Company. The EMR vendor is a business associate of the University and the e-Prescribing services would be considered a business associate of the EMR vendor (subcontractor of a business associate) and would be responsible for complying with the administrative and technical safeguards of the HIPAA Privacy and Security Rules. The EMR vendor would also need a business associate contract with the e-prescribing company.

5. What is Required for a University when PHI is Shared Electronically with Outside Vendors such as Laboratories, Radiology Practices, or Pharmacies?

First, if FERPA applies and the University is only sharing student health information, arguably, they would still be subject to FERPA if they share this information electronically with these outside vendors.

However, if the clinic shares non-student information with these outside vendors, the University qualifies as a "covered" entity under HIPAA and thus responsible for complying with all of the HIPAA Rules. Additionally, in this situation, the University must consider whether the outside vendor qualifies as a separate "covered entity" conducting "healthcare operations" on behalf of a patient of the education client or a "business associate" of the education client.

Under HIPAA, a covered entity can share protected health information with another covered entity if they are part of healthcare operations.[xli] In this scenario, a laboratory, a radiology practice and a pharmacy system, all of which are separately licensed to provide their services, and which provides such services on behalf of an education client, would be seen as separate covered entities. While they need to make sure that there are safeguards in place to protect the education client's protected health information, they can share such information between each other without having to get specific authorization from the education client's patient.

These vendors would only be business associates if they are doing something specifically on behalf of the education client and not just providing services that they are qualified to provide under their professional licensure. If the vendor is a business associate that intends to maintain or receive protected health information on the client's behalf, the client must enter into a written business associate agreement and obtain satisfactory assurance that the vendor will appropriately safeguard the information before it discloses such information to the vendor.

In all of these scenarios, it is important to note that HIPAA privacy laws mandate that covered entities and business associates follow the "minimum necessary" standards.[xlii] These standards require that the covered entity and business associates make reasonable efforts to limit the amount of protected health information disclosed only as minimally necessary to accomplish the intended purpose of the use.[xliii]

6. What is an EMR Company's Role if it Provides an Interface to the Outside Vendors in Question 5?

If an EMR Company is providing an interface to the outside vendors like the laboratory, radiology practice, and a pharmacy system, it is doing so as a contractor to its education client. If the University only uses student records in its EMR, then arguably FERPA applies. In this situation, arguably a business associate agreement is not required but we recommend that as a precautionary measure, include conditional language in a BA agreement if it is determined that HIPAA applies (see Practice Tip below).

In contrast, if the University's EMR includes non-student health records, FERPA would not apply and the student health clinic would be considered a covered entity subject to HIPAA. As such, it would be required to enter into a BA Agreement with the EMR company and the EMR company would have to enter into a business associate agreement with the outside vendors as a subcontractor of a business associate.

***Practice Tip**: As a precautionary measure and best practice, it is recommended that the University enter into a "conditional" business associate agreement with the EMR Company in the event HIPAA does apply and the University can make sure that its vendors are complying with HIPAA. For example, standard disclaimer language could be used at the top of the agreement stating that the University takes the position that HIPAA does not apply to the services outlined in the Vendor Agreement, but if it is determined that HIPAA applies, the parties have executed the BA Agreement.*

***Sample language**: "Client's execution of the Business Associate Agreement does not constitute an agreement or admission that Client is a Covered Entity for purposes of HIPAA in the services transacted under this Agreement."*

7. Is there a Difference if a University Directly Contracts with an e-Claims Clearinghouse versus having their EMR Vendor Contract with the e-Claims Clearinghouse as Part of the EMR Company's Bundled Service?

Yes. Using the same rationale as the answer question 6 above, the answer depends on whether the University uses only student information on its EMR and therefore would be subject to FERPA.

If HIPAA applies to the University, when the University contracts directly with an e-claims clearinghouse, the e-claims clearinghouse becomes a business associate of the University. A written business associate agreement will have to be executed between the University and the e-claims clearinghouse that includes all of the mandatory provisions under HIPAA. If the EMR company contracts with e-claims clearinghouse, the e-claims clearinghouse

becomes a subcontractor of the EMR company. In that situation, there would need to be two business associate contracts: (1) between the University and the EMR Company; and (2) a business associate agreement between the EMR company and the e-claims clearinghouse.

IV. CONCLUSION

Medical and health information handled by student health clinics may be subject to FERPA, HIPAA, and in very narrow and implausible circumstances, neither. The manner that such information is regulated depends on what kind of information it is, with whom it is shared, what it is used for, and whether the patient is a student. HIPAA laws require covered entities and their business associates to implement extensive privacy and security safeguards, while FERPA do not have similar requirements, creating a disconnect between the privacy interests under FERPA and under HIPAA.

While the HIPAA regulations clearly appear to have considered the FERPA legislation by exempting "education" records from HIPAA protections, HHS did not go far enough to address the issue of student health clinics and their expanding roles in the health care arena. As student health clinics provide more conventional medical and administrative services such as billing third-party insurance companies and offering more services to people other than students, they become more like typical ambulatory clinics, and therefore more like the covered entities regulated under HIPAA.

For those entities subject to HIPAA, the government is now holding not only the providers, but also the vendors that do business with the providers, directly accountable for complying with the HIPAA privacy and security laws.

Even if a University qualifies for the FERPA exception, we suggest that you begin to consider a long term plan to adopt HIPAA-mandated administrative, physical and technical safeguards as best practices for your student health center. Holding your own organization as well as your business associates (vendors) to HIPAA standards will not only provide a high level of practical and legal protection from liabilities associated with privacy breaches, but would also prepare you in the event that federal or state governments ultimately 'fill in the gaps' and determine that HIPAA[xliv] privacy and security safeguards do apply to student health clinics.

[i] Final Rule, 78 Fed. Reg. 5588 (Jan.25 20-13) (to be codified at 45 CFR 160 and 164)
[ii] Id.
[iii] 45 CFR 160.103 , Definition of electronic protected health information and protected health information.
[iv] 45 CFR 160.103 definition of "Individually Identifiable Health Information."
[v] 78 Fed. Reg. 5571 (Jan. 25, 2013).
[vi] 78 Fed.Reg.5571 (Jan. 25, 2013).
[vii] 78 Fed. Reg. 5560 (January 25, 2013) to be codified in 45 CFR 164.314.
[viii] 78 Fed. Reg. 5560 (January 25, 2013) to be codified in 45 CFR 160.402(2).
[ix] 78 Fed. Reg. 5691 (January 25, 2013) to be codified in 45 CFR 160.404.
[x] Id. 45 CFR 160.401-45 CFR 160.408 (2013 Amendments and 2009 regulations)
[xi] 78 Fed. Reg. 5691 (January 25, 2013) to be codified in 45 CFR 160.402.
[xii] See 45 CFR 160.401-426 (Impositions of Civil Monetary Penalties; 45 CFR 160.500 -522 (Procedures for Hearings).
[xiii] Id.
[xiv] See generally, 45 CFR 160 et. seq. and 45 CFR 164 et. seq.
[xv] 45 CFR 164.402- 164.410
[xvi] Id.
[xvii] *Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*. Go to: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hipaaferpajointguide.pdf
[xviii] 45 CFR 164.103 "hybrid entity."
[xix] 45 CFR 164.103 "covered entity."
[xx] Final Rule, 78 Fed. Reg. 5588 (Jan.25 2013) (to be codified at 45 CFR 160and 164).
[xxi] Id.
[xxii] 34 CFR 99.2 and 34 99.3
[xxiii] 34 CFR 99.1 et. seq.
[xxiv] 34 CFR 99.3, definition of "education records."
[xxv] 34 CFR 99.3, definition of "personally identifiable information."
[xxvi] 34 CFR 99.63.
[xxvii] 34 CFR 99.67.
[xxviii] 34 CFR 99.60 -99.66.
[xxix] There is a third exception regarding employment records but that will not be discussed in detail in this paper.
[xxx] 34 CFR 99.3(4).
[xxxi] 34 CFR 99.3, Definition of "Education records."
[xxxii] 34 CFR 99.10(f).
[xxxiii] Id.
[xxxiv] 34 CFR 99.3, definition of "personally identifiable information."
[xxxv] 45 CFR 160.103 definition of "transaction".
[xxxvi] 45 CFR 160.103 definition of "electronic media."
[xxxvii] The Office of Civil Rights, Frequently Asked Questions, (Nov. 25, 2008), http://www/hhs/gov/ocr/privacy/hipaa/faq/ferpa and hipaa/522.html.
[xxxviii] Id.
[xxxix] 45 CFR 160.103, Exclusions to the Definition of PHI.
[xl] 45 CFR 160.103, Definition of "Health Plan."
[xli] 45 CFR 164.506.
[xlii] 45 CFR 164.502(b).
[xliii] Id.
[xliv] Or "HIPAA like" privacy and security safeguards in the event that States create more stringent legislation than HIPAA to apply to student health clinics.

