Understanding the Interaction Between EPSDT and Federal Health Information Privacy and Confidentiality Laws*

Jane Hyatt Thorpe[a] and Sara Rosenbaum[b,c]

September 2013

Table of Contents

Executive Summary

Access to patient health information across providers and settings of care is increasingly recognized as a critical element in improving the quality and value of health care delivery. Without access to patient health information, tests may be unnecessarily repeated, access to care and benefits may be withheld or delayed, and care may not be optimally coordinated across a team of providers or settings of care. This is particularly true for Medicaid-eligible children whose health care needs may be met across health care, social, and educational settings. Medicaid entitles children to Early and Periodic Screening Diagnostic and Treatment (EPSDT), the Medicaid benefit for children and adolescents, that begins at birth and extends to age 21. EPSDT offers broad preventive, diagnostic and treatment benefits that can keep children healthy and advance healthy child and adolescent development.

Under EPSDT, as is the case with health care generally, a complex federal and state regulatory framework governs access to health information across treatment and care settings. This

---

* This paper was funded by the Centers for Medicare & Medicaid Services (CMS), under Task Order HHSM-500-T0002, National Early and Periodic Screening, Diagnostic, and Treatment (EPSDT) Improvement Workgroup, under subcontract from NORC at the University of Chicago. Any opinions are those of the authors and do not represent the positions of CMS, NORC or George Washington University.
[a] Associate Professor of Health Policy, The George Washington University School of Public Health and Health Services
[b] Harold and Jane Hirsh Professor, Health Law and Policy, The George Washington University School of Public Health and Health Services
[c] The authors wish to thank Teresa Cascio, JD, for her research supporting this work.

framework protects the privacy and confidentiality of patient health information; in some cases, it can restrict, rather than enable, information sharing.

This analysis focuses on privacy and confidentiality in a federal legal context, but state law is foundational to health information privacy and confidentiality.

Overarching Considerations

In approaching the subject of health information privacy and confidentiality in the context of health care for Medicaid-enrolled children, two sets of relationships stand at the forefront: First, the relationships that exist among health care professionals, minor patients, and parents or caretakers; and second, the necessary relationships that must be forged among health care, educational, and social service providers. These two sets of relationships have complex interactions with one another and heavily influence federal and state laws related to health information exchange and disclosure.

The special relationship between health care professionals and patients creates legal obligations. The first is to furnish clinically appropriate care, which may involve the sharing of information with other health care professionals. The second is to provide patients (and where minor children are concerned in most cases, their families) sufficient information about care and treatment to enable informed choice about care. The third is to protect the confidentiality and privacy of health information, particularly information that could cause harm.

These duties must be carried out in ways that recognize the many types of health and social service settings whose activities influence child health (e.g., traditional clinical care settings, school-based health care settings, child care programs, and the like). Furthermore, health care providers must be able to communicate effectively across health care delivery arrangements that may operate independently of one another (e.g., between a Medicaid managed care organization and a school-based health program) in order to ensure appropriate care and management.

Where children are concerned, the relationship between parents/legal caretakers effectively acts as an overlay on this set of system interactions. The relationship between parents and children is unique in law. With few exceptions, parents have a right to gain access to health information about their children, as well as the right to control the use or disclosure of information about their children's health or health care that could cause harm.

Relevant Laws and Regulations

Several federal laws govern the privacy and confidentiality of health information for Medicaid-eligible children across health care and school settings.

A. *The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*

HIPAA sets a national framework for the management, transmission, and disclosure of health information. At HIPAA's core lies an effort to balance the right of individuals to control third party access to information about health and health care against the need of providers and payers for a flow of information for treatment, payment, and health care operations. Despite common misperceptions, the Privacy Rule vests fairly broad discretion in health care providers and insurers. HIPAA empowers them to prudently exchange protected health information related to treatment, payment, and operations and to do so without written patient authorization. However, beyond these three purposes – treatment, payment, and health care operations – HIPAA sets important exceptions. Some of these exceptions require written patient authorization, or at a minimum, the opportunity for a patient to object to the disclosure of information.

HIPAA does not preempt (i.e., displace or overrule) more stringent state law protections. State laws may establish additional or stricter protections than those afforded by HIPAA (e.g., a requirement of patient authorization even when HIPAA itself does not).

The HIPAA framework contains added dimensions when the issue is disclosure of information regarding the treatment of minors. The Privacy Rule generally treats a minor's parent, guardian, or other person acting *in loco parentis* as the minor's *personal representative* for purposes of handling all required or permitted disclosures as well as those disclosures requiring written authorization, as long as the parent or other person is recognized by law as having the authority to act on behalf of the minor. But in the event a state or other law requires otherwise (e.g., a state law that recognizes minors as emancipated for certain types of care, such as family planning or pregnancy-related care) state law will control. Thus, when minors are involved, it is absolutely critical to consult state law in addition to the HIPAA Privacy Rule.

Finally, and perhaps most importantly where school health is concerned, HIPAA does not apply to medical or health information in education records (e.g., school-based records such as those maintained by a school nurse). Student health information maintained in education records is governed by the Family Educational Rights and Privacy Act (FERPA).

B. *The Family Educational Rights and Privacy Act (FERPA)*

Unlike HIPAA, FERPA is a law that turns on specific patient consent to the release of information that exists in what the law classifies as an education record. Importantly, for purposes of this analysis, FERPA treats elementary and secondary student health records, including immunization records, as education records. FERPA allows parents to access health information contained in their child's education records and requires parents to consent in writing to most other disclosures including disclosures to providers and insurers. While exceptions do exist to the general rule requiring written parental consent to the release of information contained in education records, such exceptions are limited. Thus, for example, access to education records can exist without parental consent in emergency situations and situations involving immunization records.

C. *42 C.F.R. Part 2 (Part 2)*

Long-standing federal regulations, codified at Part Two of Title 42 of the Code of Regulations (CFR), and frequently referred to as the "Part Two" regulations, protect the confidentiality of alcohol and drug use patient records. Part 2 provides additional protections for health information that relates to patient substance use diagnosis or treatment information. Information covered by Part 2 may be disclosed only with written patient authorization with limited exceptions (e.g., emergency situations).

In addition to the laws and regulations discussed above, separate privacy and confidentiality protections also exist under a variety of federal programs, such as family planning programs funded by Title X, community health centers, Head Start programs, Child Welfare programs, and the Individuals with Disabilities Education Act (IDEA). In general, IDEA requirements align with FERPA requirements.

HIPAA requirements apply to programs that are considered to be providers of health services (e.g., community health centers, family planning programs, public health agencies funded through a combination of CDC grants). These providers, and other participating providers, also would be subject to Medicaid's own long-standing privacy statute, which requires state agencies to safeguard the use and disclosure of information about applicants and beneficiaries to purposes related to program administration. Because delivering health care is integral to program administration, the Medicaid privacy statute comes into play as well. Thus, Medicaid providers would be expected to be both HIPAA compliant as well as in compliance with any specific requirements that a state Medicaid agency might impose under state or federal law.

What This Means in an EPSDT Context: Creating an Environment For Responsible Information Exchange and Thinking about Treatment Teams as a Possible Solution

Medicaid-eligible children receiving EPSDT health care benefits across systems will have information contained in various records: health records governed by HIPAA or the Medicaid privacy statute; education records governed by FERPA; records maintained by child welfare agencies; records maintained by Head Start agencies; treatment records for substance abuse programs; and Title X family planning clinic or health center records. As described above, HIPAA allows providers significant discretion to share patient health information for treatment and payment related purposes, in a secure and appropriate fashion, without patient authorization. As such, a provider may share health information with a Medicaid agency for payment purposes, as well as a school-based provider (e.g., instructions for medications taken during school hours). However, certain federal laws, such as FERPA and Part 2, may set special rules for health information contained in educational records or for special types of health information, such as substance abuse information. State laws also may set stricter disclosure standards for certain types of information, such as mental health conditions. State laws also may be more liberal in addressing the relationship between parents and children in a health care context, for example, enabling minors to make independent decisions about certain types of health information as "emancipated minors."

The common denominator for laws that are stricter than HIPAA about disclosure of personal health information is the issue of written patient consent. The key, therefore, may lie in the ability of various treating providers to come together to create "treatment team" consent forms, and engage families (and where relevant, adolescents) in order to enable information exchange among team members without specific consent for each exchange. For example, parents of children receiving care for emotional disorders in both a school and a children's hospital treatment setting could agree to permit the entire treatment team – the school clinic, the children's hospital, consulting specialists, the pharmacy – to share information needed to assure the child's appropriate care in school. This approach does not authorize the treating team to share information with third parties (such as summer camps) who may want it, but it would bring team members under a common information umbrella and into a unified confidential relationship with the child and family. This approach might be considered by Medicaid agencies, Medicaid managed care organizations, and health care providers involved in the treatment of children.

Introduction

This analysis explores the interaction between the special Medicaid benefit for children and adolescents, known as Early and Periodic Screening Diagnostic and Treatment (EPSDT), and certain federal laws pertaining to the privacy and confidentiality of health information. It is designed to provide greater clarity regarding the federal legal framework that surrounds the use and disclosure of health information across health care, educational, and social service settings for Medicaid-eligible children.

This analysis focuses on privacy and confidentiality in a federal legal context. But a full overview of EPSDT and its interaction with health information privacy and confidentiality law would consider state law as well. Indeed, where the privacy and confidentiality of health information is concerned, state law is foundational and continues to apply in many different treatment settings. Special state laws may apply to health information exchange related to mental health and HIV/AIDS, as well as disclosure of health information in the case of sexually active adolescents who use family planning services. As such, health care providers and state Medicaid agencies will need to consult their own state law experts in order to understand the additional state law considerations that may arise in situations involving health information exchange and disclosure for children and adolescents.

The analysis begins by discussing overarching considerations that apply to the various federal laws governing health information privacy. It then summarizes the principal privacy-related elements of the following laws:

A. Medicaid and EPSDT (Title XIX)
B. The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule
C. The Family Educational Rights and Privacy Act (FERPA)
D. 42 C.F.R. Part 2 (special privacy rules applicable to substance abuse treatment)
E. The Title X Family Planning Program
F. Medicaid Privacy Statute
G. Individuals with Disabilities Education Act (IDEA)
H. Head Start Act
I. The Child Welfare Program

The analysis concludes with a series of questions and answers addressing situations that arise regarding health information exchange and information disclosures in the case of Medicaid-enrolled children.

Overarching Considerations

In approaching the subject of health information privacy and confidentiality in the context of pediatric and adolescent health care for Medicaid-eligible children, certain considerations are important to bear in mind. The first is the key relationships that guide principles related to the use and disclosure of health information. A second relates to special issues that may arise when children are treated across multiple care settings (e.g., provider-based clinical care settings, schools, and child care programs).

Health Care Relationships

At its heart, the law is all about the rights and obligations created by various health care relationships. In the case of pediatric and adolescent health, many relationships come into play. In an information exchange and disclosure context, the task becomes how to reconcile and balance these relationships. Where pediatric health care is concerned, two relationships become relevant:

A. *Patients and health care professionals.* The special relationship between health care professionals and their patients gives rise to a legal obligation on the part of providers to both furnish clinically appropriate care (which may involve the sharing of information with other health care professionals) and provide patients (and their families) sufficient information about care and treatment options to assure their ability to make informed choices about care. A key dimension of the provider/patient relationship is to protect the confidentiality and privacy of health information, especially information that could cause harm.
B. *Parents/legally responsible caretakers and children*. The relationship between parents/legal caretakers and their children is unique in law. This relationship in turn gives rise to parents' right of access to health information about their children as well as the right to control the use or disclosure of information about their children's health or health care that could cause harm. In certain situations the law may override this right of access and control, in situations in which children's privacy concerns may outweigh the interests of parents. This issue may arise under state law in the case of certain types of information (such as about receipt of family planning or pregnancy care or treatment for a sexually transmitted infection (STI)) or in cases in which a child is considered an emancipated minor. State laws that establish independent legal rights in certain children for certain types of information can vary widely. For example all 50 states and the District of Columbia give adolescents confidentiality rights where information about treatments for STIs is concerned, but at varying ages.[1]

Treatment Across Multiple Patient Care Settings

In order to appropriately manage care, pediatric treatment may be necessary across multiple health care settings. In modern society, numerous factors feed into the need for multi-location health care: parental employment that precludes the ability to take a child out of school or child

[1] Guttmacher Institute, An Overview of Minors' Consent Law, *State Policies in Brief* (as of February 1, 2013) 2013, http://www.guttmacher.org/datacenter/profiles/US.jsp, accessed February 17, 2013.

care for a medical or dental appointment; educational mainstreaming of children and adolescents with disabilities, which in turn necessitates in-school health management; and the strategic location of medical and dental providers in community-based locations such as schools, teen social and employment centers, or mobile vans serving homeless shelters, especially in the case of children living in communities with elevated poverty and rates of medical and dental underservice. Strong communication among providers – and between providers and payers in the types of networked health care arrangements that employ more rigorous utilization management and that are far more common in the case of Medicaid managed care – becomes an essential aspect of appropriate health care itself in these situations.

Program oversight that recognizes these various considerations emerges as an important aspect of state Medicaid administration. State agencies have multiple duties, all of which can be thought of as part of their overall duty to administer the Medicaid program in the best interest of program beneficiaries: a duty to assure the overall quality of care; in the case of EPSDT, a duty to assure access to covered services, which dates back to the program's 1967 enactment; and a duty to protect the privacy of health information. Taken together, these duties create a significant interest in Medicaid programs in ensuring that necessary and appropriate information is exchanged across multiple treatment settings, while assuring that as part of information exchange, participating providers comply with various federal laws related to health information privacy.

Overview of Key Laws

A. *Medicaid and EPSDT*

The Early and Periodic Screening Diagnostic and Treatment or EPSDT benefit was added to Medicaid in 1967 in the wake of government studies documenting extensive, preventable physical, mental, and dental health conditions among both impoverished preschool children and adolescent military draftees.[2] EPSDT is the Medicaid benefit for children and adolescents, that begins at birth and extend to age 21. [3] EPSDT is a required benefit for "categorically needy" beneficiaries and optional for medically needy children and adolescents (i.e., those who "spend down" to eligibility by incurring high medical costs).[4]

A crucial term in EPSDT is "early," which modifies not only the word "screening" but also "diagnosis" and "treatment," signaling EPSDT's role in promoting child health. Its purpose is to prevent the development of serious conditions and correct or ameliorate diagnosed conditions that, if left untreated, ultimately could emerge as serious adulthood illness and disability.

Because EPSDT represents required coverage for children, its terms apply regardless of the type of coverage arrangement used: the traditional Medicaid fee-for-service program; through

[2] ROSENBAUM S., MAUERY D., SHIN P.ET AL., NATIONAL SECURITY AND U.S. CHILD HEALTH POLICY: THE ORIGINS AND CONTINUING ROLE OF MEDICAID AND EPSDT (2005), http://sphhs.gwu.edu/departments/healthpolicy/dhp_publications/index.cfm?mdl=pubSearch&evt=view&PublicationID=35A8D671-5056-9D20-3DEFF238AEFA7071

[3] Social Security Act, 42 U.S.C. §1396d(a)(4)(B) (2012).

[4] 42 U.S.C. § 1396a(a)(10)(A)(i)-(C).

managed care arrangements; or under "alternative benefit plans"[5] for newly eligible adults under the Affordable Care Act's Medicaid expansion as well as certain other individuals and families.[6]

EPSDT benefits consist of the following coverage:

1. Periodic and "as needed" comprehensive assessments of physical, mental, and developmental health that begin at birth and last through adolescence;
2. Childhood immunizations recommended by the Advisory Committee on Immunization Practice (ACIP);
3. Periodic and "as-needed" vision, hearing and dental services including preventive restorative, and emergency dental care, eyeglasses, and hearing aids and other hearing devices; and
4. Medically necessary diagnostic and treatment services needed to "correct or ameliorate defects and physical and mental illnesses and conditions" that fall within Medicaid's definition of "medical assistance," regardless of whether such treatments would be covered under the state Medicaid plan in the case of beneficiaries ages 21 and older.[7]

Beyond coverage, EPSDT is designed to assure access to care. EPSDT thus provides for:

1. Informing EPSDT-eligible beneficiaries and their families about covered services including screening assessments, diagnosis and treatment, and all age-appropriate immunizations; and
2. Providing or arranging (either directly or through referrals to agencies, organizations, and individuals) corrective or ameliorative treatment whose need is disclosed by a screen.[8]

As with other Medicaid benefits, the EPSDT provisions are governed by general program standards related to access, quality, and health information privacy. Because EPSDT can be thought of as the pediatric and adolescent coverage component of the Medicaid program, all providers furnishing care for children effectively offer some dimension of the EPSDT benefit. Children receiving dental exams and routine care are receiving EPSDT dental benefits. Children receiving periodic or as needed health exams and treatment for various health needs and conditions are receiving a periodic or "as needed" screen along with diagnosis and treatment. Children diagnosed at birth or in infancy with serious developmental disabilities are, by virtue of the care they receive, using EPSDT-covered services. As such, virtually all health care furnished to children and adolescents under age 21 can be thought of as falling within EPSDT. Therefore, when one considers how federal health information laws apply to EPSDT, one is really assessing how federal health information laws apply to health care furnished to Medicaid enrolled children and adolescents generally.

---

[5] CMS created the term "alternative benefit plans" in a January 2013 notice of proposed rulemaking. Medicaid, Children's Health Insurance Programs, and Exchanges: Essential Health Benefits in Alternative Benefit Plans, Eligibility Notices, Fair Hearing and Appeal Processes for Medicaid and Exchange Eligibility Appeals and Other Provisions Related to Eligibility and Enrollment for Exchanges, Medicaid and CHIP, and Medicaid Premiums and Cost Sharing, 78 Fed. Reg. 4594 (proposed Jan. 22, 2013).
[6] 42 U.S.C. § 1396u-7.
[7] 42 U.S.C. § 1396d(r).
[8] 42 U.S.C. §1396a(a)(43).

B. *HIPAA Rules*

HIPAA sets a national framework for the management, transmission, and disclosure of health information. At HIPAA's core lies an effort to balance the right of individuals to control access by third parties to information about health and health care against providers' and payers' need to be able to exchange and manage information needed for treatment, payment, and health care operations. As a result, HIPAA gives health care providers considerable flexibility over information management and exchange, if done prudently, while at the same time giving individuals the ability to control information flow.
Patients typically sign forms with their providers acknowledging that they have been informed of their general HIPAA rights. This acknowledgement of one's rights however, should not be confused with the right to control the release of certain types of information through express consent.

Collectively there are 4 separate HIPAA Rules:

1. The Privacy Rule,[9] issued in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA);[10]
2. The Security Rule,[11] which also stems from HIPAA;
3. The Enforcement Rule,[12] which also stems from HIPAA and sets out the enforcement system for the HIPAA Rules; and
4. The Breach Notification Rule,[13] required under the Health Information Technology for Economic and Clinical Health Act (HITECH), enacted as part of the American Recovery and Reinvestment Act of 2009.[14]

In January 2013, the United States Department of Health and Human Services (HHS) released a major set of regulations updating the various HIPAA Rules.[15] These changes will be discussed where relevant.

1. The Privacy Rule

Although the HIPAA Privacy Rule establishes important safeguards over health information privacy, the rule also can be thought of as "provider-centered." That is, HIPAA is designed to essentially create a privacy "operating system" for health care providers, an approach to health information management that protects information while still enabling providers to engage in the types of information exchange that are vital to health care and to the overall operation of the

---

[9] 45 C.F.R. §§ 160.101- 552 (2012); 45 C.F.R. §§ 164.102-106; 45 C.F.R. §§ 164.500-534.
[10] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 139 (1996) (codified as amended in scattered sections of 42 U.S.C.).
[11] 45 C.F.R. §§ 160.101- 552; 45 C.F.R. §§164.102-106; 45 C.F.R. §§ 160.302-318.
[12] 45 C.F.R. §§ 160.300-552.
[13] 45 C.F.R. §§ 164.400-414.
[14] Health Information Technology for Economic and Clinical Health Act (HITECH), Pub. L. No. 111-5, 123 Stat. 115 (2009) (codified in scattered sections of 42 U.S.C.).
[15] Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566 (Jan. 25, 2013).

health care system, especially the relationship among providers of clinical care and between providers and insurers.

Purpose. The purpose of the Privacy Rule is to protect the privacy of individually identifiable health information (referred to under the Rule as protected health information (PHI)).[16] The Privacy Rule was initially published in 2000 and then later updated in 2003 and 2013.

Scope of the Rule. The purpose of the Privacy Rule is to regulate *the use, maintenance, management, and transmission of electronic health information* among *covered entities.* The rule is broad, although in school settings it has definite limits; indeed, as discussed below, certain health information about children and adolescents may be maintained in records that are considered to be outside the HIPAA umbrella. As a result, these records are not covered by HIPAA's relatively permissive approach to information sharing among treating providers and between providers and insurers.

What entities are covered by the Privacy Rule? Under HIPAA, health plans and health insurers, health care clearinghouses, and all health care providers regardless of size who electronically transmit health information in connection with certain transactions (e.g., benefit eligibility inquiries, claims, and referral authorization requests)[17] are Covered Entities. The Privacy Rule also applies to Business Associates who work on behalf of Covered Entities and use or maintain PHI.[18] A Business Associate is defined as a person or organization, other than a member of a Covered Entity's workforce, that performs certain functions or services on the Covered Entity's behalf that involve the use or disclosure of PHI. Relevant functions or activities include claims processing, data analysis, utilization review, and billing; while services are limited to legal, actuarial, accounting, consultation, data aggregation, management, administrative, accreditation, or financial.[19] Together these Covered Entities and their Business Associates are referred to as "Regulated Entities."[20]

What is Protected Health Information (PHI)? The term "'protected health information" or PHI applies to all "individually identifiable health information" that is held or transmitted by a Regulated Entity.[21] PHI can be in any form (e.g., electronic, paper, or oral). The concept of "individually identifiable health information" means information, including demographic data, that relates to:

1. an individual's past, present or future physical or mental health condition;
2. the provision of health care; and
3. payment for care, whether in the past, present, or future.

To be PHI, the information must allow identification of an individual patient or member or must itself contain enough information to "reasonably lead to" individual identification. Examples of these types of information are name, address, birth date, and Social Security Number.[22]

---

[16] 45 C.F.R. § 160.103.
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] *See* 78 Fed. Reg. at 5566.
[21] 45 C.F.R. § 160.103.
[22] *Id.*

What PHI does NOT include: The FERPA exception. PHI explicitly does *not* include: 1) a Regulated Entity's employment records; 2) education records; or 3) certain other records subject to the Family Educational Rights and Privacy Act (FERPA).[23] ***In other words, health information about a child that is stored in records that are governed by FERPA are subject to FERPA's special standards, not the general Privacy Rule standards.*** Thus, FERPA trumps the Privacy Rule. Indeed, even where HIPAA might allow one health care provider to disclose certain information to another provider without having to obtain written authorization or express permission, it is FERPA's more stringent requirements – not the Privacy Rule – that would govern the transmission of information if the provider doing the disclosing holds the information in records governed by FERPA.

Permissive disclosures and required disclosures; when authorization is required for a Regulated Entity to disclose PHI. The Privacy Rule sets forth the situations under which a Regulated Entity *must* disclose PHI without obtaining an individual's authorization as well as those situations under which a Regulated Entity *must* obtain authorization prior to disclosure. A Regulated Entity must (i.e., is required to) disclose PHI to an individual (or a personal representative) upon his or her specific request for access. The Entity also must disclose PHI to HHS for HHS to assess compliance with HIPAA.[24]

At the same time, HIPAA identifies situations in which the Regulated Entity *must obtain* an individual's authorization prior to releasing PHI. In general, a Regulated Entity must obtain an individual's written authorization for any use or disclosure of PHI that is not otherwise required or permitted by the Privacy Rule.[25] The HIPAA Privacy Rule also specifically identifies the following circumstances in which prior written authorization from the individual is required: disclosure of psychotherapy notes with few exceptions (e.g., for defense in a legal proceeding brought by the individual who is the subject of the PHI); disclosure for marketing purposes; and disclosure for the sale of PHI.[26]

Notably, the Privacy Rule leaves considerable room for health care providers to engage in *permissive disclosures,*[27] that is, to exchange information according to their own customs and practices without written authorization or permission.

When a Regulated Entity may disclose PHI without written authorization or express permission of an individual. As a threshold matter, the Privacy Rule prohibits Regulated Entities from disclosing PHI unless authorized in writing or permitted by the individual whose information is involved. [28] *But there is a range of crucial exceptions to this basic principle*, and the Rule *permits* Regulated Entities to disclose PHI in a number of situations without written authorization or permission.

Regardless of whether the information being disclosed does – or does not require – the written authorization or permission of the individual, Regulated Entities are expected to make reasonable efforts to limit their disclosures to the "minimum necessary" to achieve the purpose for which

[23] Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.
[24] 45 C.F.R. §§ 160.300-316.
[25] 45 C.F.R. § 164.508.
[26] *Id.*
[27] 45 C.F.R. § 164.502(a).
[28] *Id.*

the information was released or requested.[29]

The Rule *permits* Regulated Entities to use and disclose PHI without authorization for certain purposes:[30]

1. For treatment, payment, and health care operations,[31] defined in the Rule as including the following types of activities: direct patient care, obtaining premiums and reimbursement for furnished health care services, and administrative, financial, and quality improvement activities essential to maintaining the Regulated Entity's business;[32]
2. In situations where disclosure is required by law or where it is in the public interest to disclose because of a serious and imminent threat to health or safety *and* (in the reasonable belief of the Regulated Entity) the disclosure is to an entity that is in a reasonable position to be able to prevent the threat (e.g., to the police);[33]
3. For public health practice, health research and health care quality improvement purposes. Under these circumstances, a Regulated Entity may disclose a *limited data set* (LDS) without authorization provided it enters into a data use agreement with the recipient setting forth the agreed upon use(s) of the LDS and related privacy requirements.[34] The Rule defines a *limited data set* as PHI that excludes 19 identifiers of the individual or of the individual's relatives, employers, or household members, such as names, address, telephone and fax numbers, email addresses, social security numbers, medical record numbers and health plan beneficiary numbers;[35] OR
4. When an individual expressly authorizes disclosure of PHI.

Thus, the Rule allows PHI disclosure *without authorization* by Regulated Entities of information that is covered by the Rule, as long as the disclosure is for treatment, payment, or health care operations, and in other situations, and as long as the information disclosed is kept to the minimum necessary (*in the opinion of the disclosing entity*) to accomplish the purpose for which the disclosure is being made with few exceptions. For example, the minimum necessary standard does not apply to disclosures made for treatment purposes where it may be difficult to fully understand a patient's medical condition without their entire medical history. In treatment situations, much provider-to-provider exchange of treating information is governed by provider custom. For example, a health center may provide a specialist with a child's entire medical record if requested by the specialist to ensure appropriate treatment. Of course, if the health center and specialist's custom or practice is *always to* secure patient authorization before exchanging any information, then the health center staff would maintain such a practice. In other words, under the Privacy Rule, much provider-to-provider exchange of treating information is to be governed by provider custom.

When Regulated Entities may not follow their own custom and disclose information for treatment, payment, and health care operation purposes without written authorization or express

[29] 45 C.F.R. § 164.502(b).
[30] For a complete list of permissive disclosures see 45 C.F.R. § 164.512.
[31] 45 C.F.R. § 164.506.
[32]45 C.F.R § 164.501.
[33] 45 C.F.R. § 164.512.
[34] 45 C.F.R. § 164.514.
[35] *Id.*

permission. The Privacy Rule, as noted, gives providers the flexibility to follow their own customs when the PHI being disclosed is related to treatment or payment and when safeguards to protect such disclosures are followed. But there are certain situations in which providers' own customs must give way to more stringent standards:

1. When a patient expressly refuses to allow the disclosure of any – or certain -- information for purposes of treatment, payment or health care operations or other purposes to which an individual may object.[36] Note, however, a Regulated Entity is not required to agree to an individual's request to restrict disclosures unless the restriction involves disclosure of information to a health plan for payment purposes and the individual has paid for the services in full.[37]
2. When a "more stringent"[38] state law prevents certain disclosures without express authorization (e.g., information related to HIV/AIDS, or mental illness, or confidential family planning information).
3. When the information involves addiction, governed by 42 C.F.R. Part 2;[39] or
4. When the information is held in a record covered by FERPA, which lacks HIPAA's permissive disclosure standard.

Disclosure of a minor's health information. The HIPAA Privacy Rule generally treats a minor's parent, guardian, or other person acting in loco parentis as the minor's *personal representative* for purposes of handling all required or permitted disclosures as well as those disclosures requiring written authorization so long as the parent or other person is recognized by law as having the authority to act on behalf of the minor. There are three circumstances in which a minor has the authority to act on his or her behalf: (1) when the minor consents to the health care service and no other consent is required by law; (2) in cases in which a minor may lawfully obtain the health care service without parental consent (e.g., contraceptive services); and (3) in situations where the parent agrees that the health care provider and the minor may keep the information confidential.[40] However, in the event a state or other law requires otherwise, the state or other law will control.[41] Thus, when minors are involved, it is absolutely critical to consult state law in addition to the HIPAA Privacy Rule.

In sum, the Privacy Rule vests fairly broad flexibility in health care providers and insurers to exchange prudent amounts of PHI related to treatment and payment and to do so without written authorization. At the same time, it should be emphasized that there are important written authorization exceptions, as noted, which mean that ultimately, health care providers want to think about securing express patient consent not only to treatment but to the sharing of information that is related to their treatment and that needs to be shared with another health care provider in order to assure that treatment is appropriate. In other words, HIPAA creates discretion to share information in a secure and appropriate fashion. But there are enough exceptions, as well as enough cases in which the information is governed by a much more stringent law such as FERPA or Part 2 so that health care providers might be far better off

[36] 45 C.F.R. § 164.522.
[37] *Id.*
[38] 45 C.F.R. § 160.203.
[39] 42 C.F.R. Part 2.
[40] 45 C.F.R. § 164.502.
[41] *Id.*

focusing on carefully developing information release authorizations that allow them to share most information with children's treatment teams as well as with their state Medicaid program as well as with managed care entities administering the program on a state agency's behalf.

2. The Security Rule

The Security Rule[42] requires Regulated Entities to establish and maintain reasonable and appropriate administrative, physical, technical, and organizational safeguards for protecting electronic PHI (not paper-based records).[43] Specifically, Regulated Entities must: 1) ensure the confidentiality, integrity, and availability of all e-PHI that the Regulated Entity creates, receives, maintains, or transmits; 2) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; 3) protect against any reasonably anticipated uses or disclosures; and 4) ensure workforce compliance.

3. The Enforcement Rule

The Enforcement Rule[44] governs the enforcement process, including HHS investigations, requirements for setting the amount of a civil monetary penalty if a violation occurs, and requirements for hearings and appeals if a Regulated Entity challenges a violation. The Rule does not allow individuals to sue Regulated Entities whom they believe have violated the provisions of the Rule. Instead, the Rule allows aggrieved individuals to file a complaint with the HHS Office for Civil Rights (OCR) or the State Attorney General, which may enforce HIPAA on their behalf. Regulated Entities that violate the HIPAA Privacy, Security, and Breach Notification Rules may be liable for penalties up to $1.5 million depending on the level of their culpability.[45]

4. The Breach Notification Rule

The Breach Notification Rule[46] requires Regulated Entities to disclose breaches of certain unsecured PHI to the individuals affected, the HHS Secretary, and in certain circumstances, the media. Generally, a breach is defined as an impermissible use or disclosure under the Privacy Rule that "compromises the security or privacy of the protected health information" such that the use or disclosure "poses a significant risk of financial, reputational, or other harm to the individual."[47]

C. *The Family Educational Rights and Privacy Act (FERPA)*

Purpose. The purpose of the Family Educational Rights and Privacy Act (FERPA) is to protect the privacy of student education records.[48] Unlike HIPAA, FERPA is all about the shielding of information contained in records to which the law applies. There is no emphasis on provider

[42] 45 C.F.R. §§ 160.101- 552; 45 C.F.R. §§164.102-106; 45 C.F.R. §§ 160.302-318.
[43] 45 C.F.R. § 164.306.
[44] 45 C.F.R. §§ 160.300-552.
[45] HITECH § 13410(d).
[46] 45 C.F.R. §§ 164.400-414.
[47] 45 C.F.R. § 164.402.
[48] 20 U.S.C. § 1232g; 34 CFR Part 99.

flexibility and custom to manage health information in the context of treatment, payment, or health care operations. Instead the issue is parental and student control.

Scope. FERPA applies to all educational agencies and institutions that receive federal education funding, which means not only public schools and school districts but also private and public colleges, universities, and other postsecondary institutions, including medical and other professional schools. Typically FERPA exempts private and religious elementary and secondary schools.

What types of records are covered by FERPA? Under FERPA, the term "education records" refers to "records, files documents, and other materials" that "contain information directly related to a student" and that "are maintained by an education agency or institution" or an entity acting as the agent of an institution.[49] Who is considered to be an agent of the institution is a matter of federal law, but generally includes employees, contractors, and others working on behalf of or at the direction of the institution.

What types of records does FERPA exclude? The term "education records" does *not* include the following: 1) records created by instructors, teachers, or administrators that are accessible only by the teacher or a substitute; 2) records created for law enforcement purposes by a law enforcement unit of an education agency; 3) records regarding educational agency or institution employees that are made in the normal course of business and only pertain to their employment; and 4) records regarding a *postsecondary student or student over the age of 18* created by a physician, psychologist, psychiatrist, or other health care professional for treatment purposes *if* such records are only accessible by the treating professional or another "appropriate professional" specified by the student.[50]

Are school clinic records "education" records? ***Importantly, for purposes of this analysis, FERPA treats elementary and secondary student health records, including immunization records, as education records.*** Records maintained by a school nurse are considered "education records" if they are maintained by an educational agency or institution subject to FERPA. In addition, records maintained by a school on special education students, such as records of services provided to students under the Individuals with Disabilities Education Act (IDEA), are considered "education records" if they are maintained by an educational agency or institution subject to FERPA. Where a clinic is operating in a school (e.g., a community health center offering satellite clinics in schools managing an array of primary and specialized health needs in collaboration with other treating providers who come to the school clinic site to furnish care), FERPA would apply if the clinic is considered to be an agent of the school, that is, if, under its agreement with a school, the clinic is carrying out responsibilities of the school and is subject to school direction.

How about postsecondary records? As noted, at the postsecondary level, medical and psychological treatment records are *not* considered "education records" if they are made, maintained, and used only for treatment of the student and disclosed only to treating providers.

[49] 20 U.S.C. § 1232g(a)(4).
[50] *Id.*

Commonly referred to as "treatment records," these records may be disclosed for purposes other than treatment, but only if the disclosure meets one of FERPA's recognized exceptions (see list below) or only with a student's written consent.[51]

The role of written consent. Unlike HIPAA, FERPA contains no general authority to health care providers to act without written consent and disclose or exchange information for treatment and payment or health care operation purposes. The entire FERPA model can be thought of as parent-centered rather than provider-centered, as is the case with HIPAA. *Unless one of the FERPA exceptions applies, an educational agency or institution (or its agent) may disclose "education records" only with written parental consent or the consent of a student age 18 or older or enrolled in a postsecondary institution.*

The main and most common exception to the FERPA written consent requirement is disclosure by an educational agency to the parents of any child who is considered a dependent of the parents for tax purposes. An educational agency or institution may always disclose information contained in an education record to the parent(s) of dependent children. FERPA also contains other exceptions to the written consent requirement:[52]

1. When a disclosure is required by law;
2. When the disclosure is to accrediting organizations to perform accrediting functions;
3. When disclosure is needed in an emergency to protect the health and safety of the student or others; and
4. When the disclosure involves registered sex offenders or the disclosure of drug and alcohol violations to a parent, as long as the student is under 21 and the student's use or possession constitutes a disciplinary violation. (But this type of disclosure may be limited by Part 2, discussed below.)

D. *42 C.F.R. Part 2*

Purpose. Part Two of Title 42 of the Code of Regulations establishes rules protecting the confidentiality of alcohol and drug abuse patient records.[53] Like FERPA, Part 2 is designed to completely protect certain types of health information from disclosure as a matter of federal law, unless written consent is given. Put simply, Part 2 sets a written consent standard for the disclosure of information contained in virtually all patient drug and alcohol health records maintained by federally funded programs.

Scope of Part 2. Under Part 2, whose origins date back several decades, the term "records" refers to "any information, whether recorded or not, relating to a patient received or acquired by a federally assisted alcohol or drug program."[54] The term "federally assisted alcohol or drug program" encompasses *programs*. A "program" encompasses federally assisted clinics providing alcohol or drug abuse diagnosis, treatment or referrals or units within general medical facilities that are identified as providing programs for alcohol or drug diagnosis, treatment, or

[51] 34 C.F.R. § 99.30.
[52] 20 U.S.C. § 1232g(b)(1).
[53] 42 C.F.R. Part 2.
[54] 42 C.F.R. § 2.11.

referrals. A program also would include general medical facilities and their staff that treat alcohol or drug abuse as a primary function of the facility.[55]

The term “federally assisted” spans all forms of federal financial assistance: grants and contracts; Medicaid and CHIP payments.[56] Potentially (although there has been no ruling yet to the best of our knowledge) the term includes health plan coverage furnished through Qualified Health Plans sold in Health Insurance Marketplaces (also known as Exchanges), whose costs are subsidized through federal premium subsidies and cost-sharing assistance.

Written consent. Part 2 bars the disclosure of information contained in any “patient record” maintained by a “federally assisted program” without written consent by patients or personal representatives.[57] Part 2 permits disclosure without written consent if the disclosure is made to medical personnel who need the information to immediately treat a health threat to the patient.[58] No written consent is needed for certain disclosures to the Food and Drug Administration (FDA).

When minors may consent. Part 2 allows minors to consent to the release of information if they have the capacity to seek treatment independently and without parental consent. There is no payment exception to the consent rule. That is, a provider must obtain the written consent of families or minors before disclosing information to an insurer or managed care organization. (Programs may refuse to treat minors if they or their families refuse to consent for purposes of payment, unless such a refusal is barred by state law). If a minor must obtain parental consent before receiving alcohol or drug abuse treatment, then both the minor and the parent or guardian must give written consent to disclosure. (Special rules apply when a minor lacks the capacity to make a rational choice, in the opinion of a program director; this determination also allows a program to make certain disclosures to parents).

Requirements for records and disclosures. Written records that are protected by these regulations must be held under lock and key when not in use (e.g. secure room, safe, locked file cabinet). Programs must have written procedures for regulating access and use of these written records. Programs may allow patients to access, inspect, and copy their own records. Information accessed by patients may not be used for criminal investigations or prosecutions. Any disclosures made pursuant to a patient’s written consent must contain the following statement: “This information has been disclosed to you from records protected by Federal confidentiality rules (42 CFR Part 2). The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient.”[59]

[55] *Id.*
[56] 42 C.F.R. § 2.12.
[57] 42 C.F.R. § 2.13.
[58] 42 C.F.R. § 2.51.
[59] 42 C.F.R. § 2.32.

E. *The Title X Family Planning Program and Community Health Centers*

Scope. Title X of the Public Health Service Act provides grants for the development and operation of comprehensive programs of family planning services. Title X services include family planning and related preventive health services such as immunizations against sexually transmitted disease and cancer screenings. Title X program services can be provided through state, county, and local health departments, community health centers, Planned Parenthood centers, and hospital-based, school-based, faith-based, and other private nonprofit organizations. Title X grantees operate under federal confidentiality requirements and must maintain the confidentiality of patient information, including information involving adolescent patients. Information may be disclosed with patient consent.[60] Certain information may be disclosed if required by law as long as grantees use appropriate safeguards. Information may be disclosed in "summary, statistical, or other form" as long as it does not contain identifying information.[61]

Community health centers (known as Federally Qualified Health Centers under Medicaid law) are nonprofit clinics that provide comprehensive primary health services to medically underserved communities and populations. In 2011 health centers operating in more than 8,000 locations around the country furnished care to over 20 million patients, one-quarter of whom were children. Because they must, by law, be located in communities designated as medically underserved as a result of elevated health risks and a shortage of primary health care, health centers are one of the country's most important sources of primary health care for low-income children. Their services are comprehensive and frequently include both medical and dental care. As with Title X grantees, health centers that receive federal grant funding under §330 of the Public Health Service Act are required to maintain the confidentiality of all identifiable personal facts and circumstances obtained from patients. As with Title X, health centers may disclose such information only with a patient's consent. Similar to other programs, exceptions to this confidentiality rule do exist. Information may be disclosed when it is necessary to provide services to individual patients or when the HHS Secretary conducts medical audits.[62] In addition, community health centers must comply with state law standards related to the confidentiality of information about treatment provided to children and adolescents.

Of course, both Title X grantees and community health centers are considered Regulated Entities under HIPAA. Therefore, both providers could prudently exchange information as needed for treatment, payment, and health care operations. At the same time, both providers are required to comply with applicable confidentiality laws such as HIPAA and 42 CFR Part 2 discussed above (federal in the case of Title X and state laws in the case of health centers).

F. *The Medicaid Privacy Statute*

The Medicaid program contains its own privacy statute that binds state agencies as well as providers and entities that participate in Medicaid.

Scope. The privacy statute requires state Medicaid agencies to maintain safeguards that restrict the use and disclosure of applicant and recipient information to "purposes directly connected

[60] 42 C.F.R. § 59.11.
[61] *Id.*
[62] 42 C.F.R. §51c.110.

with" administration of the state plan and the exchange of information related to Child Nutrition Programs.[63] The term "purposes directly related to State plan administration" is relatively broad, encompassing several types of activities: [64]

1. Establishing eligibility;
2. Determining medical assistance amounts;
3. Providing or arranging for services to beneficiaries; and
4. Investigating, prosecuting, or conducting a civil or criminal procedure related to the administration of the plan.

Safeguards must be established and maintained for economic, social, and medical information.

Informed consent requirement. Federal standards establish a requirement of informed consent. Under this standard, "if possible," agencies must obtain consent prior to releasing information to third parties.[65] Federal standards also specify that consent is not necessary if the request pertains to verification of income, eligibility, or medical assistance payments and permit agencies to release information without individual consent in emergency circumstances, followed by notice to individuals.[66]

Required policies and procedures. Under federal requirements, state agencies must maintain policies governing outside requests for information and must execute data use agreements with other agencies before obtaining or releasing information related to eligibility verification or third party liability.[67] State Medicaid agencies are prohibited from publishing the names of applicants and beneficiaries.[68]

G. *<u>Individuals with Disabilities Education Act (IDEA)</u>*

Alignment with FERPA. The Individuals with Disabilities Education Act (IDEA)[69] finances both educational services and early intervention (EI) services for infants, toddlers, and pre-school aged children. The IDEA contains express provisions that align IDEA administration with the terms of FERPA; indeed, in order to receive IDEA funding, states must comply with FERPA.[70] Thus, health records maintained by schools or their agents such as a school nurse or other health practitioner working for or under contract with a school would be subject to the FERPA standard and shielded from disclosure to third parties (including insurers or other providers) without written consent, except in narrow circumstances. Similar standards apply to EI services; safeguards must be in place to insure the confidentiality of personally identifiable information.[71] Furthermore, parents must receive notice of and consent to the exchange of their child's information in accordance with federal and state law (e.g., HIPAA, FERPA, and applicable state

[63] 42 U.S.C. § 1396a(a)(7).
[64] 42 C.F.R. § 431.302.
[65] 42 C.F.R. § 431.306.
[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] Individuals with Disabilities Education Act, Pub. L. No. 108-446, 118 Stat. 2647, 20 U.S.C. § 1417 (2012).
[70] 20 U.S.C. § 1417(c).
[71] 20 U.S.C. § 1439(a)(2).

laws such as those addressing mental health or HIV/AIDS). In addition, states that receive federal funds must annually report data regarding the children receiving assistance to the federal Education Secretary. The required data elements include race, gender, ethnicity, and types of disabilities. States may not include personally identifiable information in their reports.[72]

H. *Head Start*

Alignment with FERPA. As with education programs, the Head Start program rests on the assumption of privacy and confidentiality with respect to records maintained by Head Start agencies. The Head Start Act requires the HHS Secretary to establish regulations to protect the confidentiality of "personally identifiable data, information, and records collected or maintained" in administering the program.[73] The regulations must provide protection equivalent to that provided by the FERPA.[74]

I. *Child Welfare Programs*

As with education programs and Head Start, the various child welfare programs provide for the confidentiality of information created by public agencies and grantees funded under the Social Security Act.[75] The requirements are fairly general. For example, State Plans for Child Welfare Services (Stephanie Tubbs Jones Child Welfare Services Program) must address, among other items, "how medical information for children in care will be updated and appropriately shared, which may include the development of an electronic health record."[76] Similarly, under the Child Abuse Prevention and Treatment Act (CAPTA) acute care hospitals, which join with a health-care provider organization, child welfare organization, disability organization, and a state child protection agency, and receive CAPTA grants must agree to protect the "confidentiality of medical, social, and personal information" regarding parents of children with disabilities, abused children, and the parents of abused children. Such information may only be released to provide specified services (e.g., providing information about community services, providing follow-up services, etc.).[77] In addition, all providers delivering health care services through these programs must comply with the HIPAA requirements. Given the greater specificity of the HIPAA requirements, those requirements are also foundational for providers delivering services through these programs (meaning compliance with HIPAA exceeds the confidentiality requirements of the Child Welfare programs).

Summing it Up: The Key Role of Written Consent in Cross-System Situations

This review of numerous laws governing the provision of health, educational, and social services to children underscores several basic points.

[72] 20 U.S.C. § 1418(a)-(b).
[73] 42 U.S.C. 9844(k)(5).
[74] *Id.*
[75] *See* 42 U.S.C. § 622(b)(15)(A)(iii); 42 U.S.C. § 5106(b).
[76] 42 U.S.C. 622(b)(15)(A)(iii).
[77] 42 U.S.C. 5106(b)(4)(D)(iv).

First, in the case of health care services, HIPAA offers the basic framework for thinking about the communication or disclosure of patient health information between and among providers, payers and other authorized parties. Because the communication of health information is so basic to the appropriate provision of medical care, health system operations, and third party financing, HIPAA gives providers the flexibility to share information.

Second, certain federal health care laws place limits on certain types of information that can be exchanged (through disclosure to other providers) for treatment, payment, and health care operation purposes. Under these laws, these limits can be overcome by obtaining the written consent of patients. Specifically, Part 2 places strict limits on the exchange of information related to alcohol or substance abuse treatment. Title X limits information exchange related to the services furnished by grantees. State laws governing privacy and confidentiality also may impose limits on the information that can be exchanged.

Third, education, child welfare, and Head Start programs have very different purposes. They are not health care programs; instead they are programs whose purpose is to furnish other services, and their rules regarding records developed by program grantees again presume written informed consent to the release of information, except in emergencies. FERPA contains a broad definition of what is an education record and extends this definition not only to schools and school districts but also to their agents, which may include school clinics.

Fourth, Medicaid agencies are expected to maintain systems to ensure that information exchanged about patients for medical care reasons is covered by safeguards. Nothing explicit in the Medicaid statute, however, would override the basic HIPAA rule, which permits the prudent exchange of health information for treatment, payment, and health care operation purposes without written informed consent unless such exchange is limited by a separate law.

Fifth, HIPAA has its limits. The authority to disclose information without written consent is related to treatment, payment, and health care operations. Were a school to simply request health information on a child for educational purposes, HIPAA would not allow a disclosure without written consent. (The 2013 HIPAA Privacy Rule makes an exception for immunization information.)[78]

Finally, children receiving health care across systems will have information contained in various records: health records governed by HIPAA or the Medicaid privacy statute; education records governed by FERPA; records maintained by child welfare agencies; records maintained by Head Start agencies; treatment records for substance abuse programs; and Title X or health center records. Depending on what law applies to the record, the need for written consent to disclosure will vary. The key, therefore, may lie in the ability of various treating providers to come together, create “treatment team” consent forms, and engage families (and where relevant, adolescents) around certain levels of consent. For example, a Title X family planning clinic and a health center furnishing general health care could enter into an agreement with an adolescent under which the adolescent allows the Title X family planning clinic to disclose family planning information contained in the Title X record to her health center treating clinician. Similarly, parents of children receiving care for emotional disorders in school and at a children’s hospital could agree to permit the entire treatment team – the school clinic, the children’s hospital,

[78] 45 C.F.R. § 164.512(b)(1).

consulting specialists, the pharmacy – to share information needed to assure the child's appropriate care in school. This does not authorize the treating team to share information to third parties who want it, but it would bring them all under a disclosure umbrella by extending a unified confidential relationship with the child to all team members.

We attach to this analysis a special document prepared by the Departments of Health and Human Services and Education, which provides joint guidance on the application of HIPAA and FERPA to student health records. The document explains, in accessible FAQ format, the circumstances under which education agencies can provide access to student health information contained in education records. The document also explains situations in which student health information will not be considered to be held in education records for FERPA purposes and how information can be exchanged without written consent. The joint guidance explains the breadth of FERPA's education records exemptions under HIPAA, noting that certain health care providers are not considered to be acting as agents of the school and therefore, that such records would be subject to HIPAA rather than FERPA.[79] However, the guidance is specific to the application of HIPAA and FERPA and does not address the privacy and confidentiality requirements of other relevant laws and regulations described above, including Part 2 or Title X, or their application to Medicaid-eligible children receiving EPSDT benefits.

Questions and Answers

As part of this analysis, we collected questions from Medicaid agencies and health care programs that might illustrate the types of information management and exchange issues that arise in the case of providers that practice in different systems but that all are engaged in the treatment of Medicaid-enrolled children.

1. **How do HIPAA and FERPA requirements apply when a provider is billing Medicaid and/or another payer (e.g., form of insurance)? (Note: In the event another form of insurance is available, Medicaid is considered the payer of last resort).**

   Either HIPAA or FERPA will apply when a provider submits claim(s) for reimbursement as the provider will need patient identifiable information (e.g., patient name, payer or health plan name, diagnosis codes, etc.) to submit the claim(s). Whether HIPAA or FERPA applies depends on the location of the identifiable health information needed for billing purposes. Is the information located in a patient record held by a Regulated Entity and protected by HIPAA (e.g., a provider)? Or is the information located in an education record held by an educational agency or institution and protected by FERPA? And lastly, regardless of whether the information is held in a record by a Regulated Entity or an educational agency or institution, does the record contain information about alcohol or substance abuse treatment or other types of care that are subject to special disclosure protections?

[79] Joint Guidance on the Application of the FERPA and HIPAA to Student Health Records, pgs. 4-5 (November 2008) available at www.ed.gov/policy/gen/guid/fpco/doc/**ferpa-hippa-guidance**.pdf *(accessed on February 17, 2013).*

HIPAA allows a Regulated Entity such as a provider to send payment information to Medicaid and other insurers without written consent. If, however, the treatment is delivered in a school setting and the health provider is acting on the behalf of the school, such as a school nurse, then written consent would be required, since the information would be considered to be held in a FERPA-protected record and not covered by HIPAA's more liberal disclosure standards. If the health information needed for billing purposes is included in a patient record and held by a Regulated Entity subject to HIPAA, then the information may be disclosed for purposes of obtaining payment for services rendered. For example, if a public elementary school employs a health care provider that bills Medicaid electronically for services provided to a student under the IDEA, the school (and the health care provider) would be considered a Regulated Entity for purposes of HIPAA and would be permitted information needed for billing purposes without written consent under HIPAA. If, however, a public elementary school employs a health care provider that bills Medicaid electronically for services provided under the IDEA and records of those services are maintained only in the student's education record, FERPA would apply and the school must obtain written parental consent to disclose information necessary to bill Medicaid.

Even where the record is considered to be governed by HIPAA, the 2013 HIPAA Privacy Rule allows patients to restrict disclosure to third party payers where the service is paid for out-of-pocket.[80] In other words, a patient may instruct his or her provider not to release information (and the provider must comply) to a third party payer, including Medicaid, about services the patient pays for personally. This situation probably would not arise frequently in the case of Medicaid-eligible children and adolescents. If the information were held in a FERPA-protected education record, FERPA's written consent rules would apply to Medicaid billings. Similarly, if the service were furnished by a Part 2-covered federally assisted treatment program, written consent would be required.

2. How do HIPAA, FERPA, and Part 2 apply to school emergency health forms? Is there a model form for securing parental consent, if needed, that would satisfy the requirements of all three statutes?

Emergency health forms are used to obtain written parental consent to allow a school to consent to emergency medical treatment for an enrolled child in the event of an emergency. They also may authorize a school to share patient health information with medical providers needed to treat the patient in the event of an emergency even though such disclosures are permitted by HIPAA, FERPA, and Part 2. HIPAA permits a Regulated Entity to disclose PHI if the Regulated Entity believes that it is necessary to prevent a serious and imminent threat to the health or safety of a person or the public and the recipient of the information is reasonably able to prevent the threat. Similarly, FERPA allows disclosure without student or parental consent to persons that need the information in an emergency to protect the health and safety of the student or others. The Part 2 Regulations allow for disclosure without patient consent to medical personnel that require the information to immediately treat a health threat to the patient.

[80] 45 C.F.R. § 164.522.

Even though these laws allow disclosure of patient health information in emergency situations, it is often simpler and more direct for schools to obtain both written parental consent for the school to consent to treatment and to disclose needed health information in the event of an emergency so that parents are on notice of how the school will handle student information in the event of an emergency and allow parents to object prior to an emergency.

We are not aware of a single model form for valid parental consent to disclosures for emergency medical treatment. In addition, state law may impose additional requirements that would need to be addressed in a consent form.

3. **Does either HIPAA or FERPA require written parental consent before a school can place a child's protected personal information (e.g., name, address, parent's name, student's date of birth and SSN, participation in school lunch) on a Medicaid or CHIP application to be shared with state or local agency staff conducting application reviews?**

Written consent would be required under both FERPA and Part 2 to disclose information on a Medicaid or CHIP application. It is unlikely that HIPAA would apply to a school's submission of information on a Medicaid or CHIP application so its more permissive disclosure provisions could not be relied upon in this situation.

Under FERPA, if the information noted above were maintained in an education record, written parental consent would be required to release the information to state or local authorities conducting application reviews. Schools may give parents information about the Medicaid and CHIP programs, and help them understand the benefits provided by the programs, as long as no identifiable student information is disclosed by the school directly to the Medicaid and/or CHIP program without written parental consent. However, FERPA does include an exception that allows a school to release information included in an education record if required by law. The Affordable Care Act (ACA) provisions going into effect on January 1, 2014 could have an impact on the answer to this question because of this exception. The ACA's requirement for individuals to obtain health insurance may be interpreted such that a disclosure of information for purposes of application reviews is considered to be required by law.

If the requested information includes any information related to alcohol or substance abuse treatment, disclosure would be prohibited without patient or parental consent under Part 2.

Because elementary and secondary schools generally are not considered Regulated Entities for purposes of HIPAA, information included in an "education record" is considered outside the regulatory authority of HIPAA. In the event an elementary or secondary school is considered a Regulated Entity for purposes of HIPAA (i.e., the school employs a health care provider and the provider electronically submits health care claims to a health plan for payment), it is still unlikely that HIPAA's more liberal disclosure rules would apply to this circumstance because the information noted above would be maintained in student health records that are considered education records under FERPA and not PHI under HIPAA.

4. **How do HIPAA and FERPA affect a school-based health care provider's ability to share health information contained in a child's school record with another health care provider, such as the child's primary care provider or a school-based clinic provider? How might HIPAA or FERPA affect the ability of schools to establish formal health information exchange systems between school health providers and primary care providers?**

   At the elementary and secondary school level, student health records, including immunization records, that are maintained by a school, school district, or school-operated health clinic that receives funding from the U.S. Department of Education, are considered education records and subject to FERPA, not HIPAA. The same is true of records maintained by a school nurse or any other health care provider employed by or under contract with a school or school district to provide services to students such as immunization, vision, dental, and/or hearing services. Because the health information is contained in the student's education record, a school-based health care provider must have written parental consent before sharing that health information with another provider. However, a non-school based provider that is a HIPAA Regulated Entity (such as a student's primary care provider) may share information with a school nurse, 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 provider may discuss a student's health care needs, such as medication, with a school nurse who will provide care to the student while at school. Thus, the rules governing sharing of information are not bi-directional. Outside providers (HIPAA Regulated Entities) MAY share information with school-based providers for treatment purposes without consent, but school-based providers MAY NOT share information with outside providers without written parental consent.

   It is also common for schools and school-based or contracted health care providers to obtain parental consent prior to providing screening and/or preventive services to students. Such consent forms also may address with whom health information generated from the visit may be shared regardless of whether it becomes part of a HIPAA protected medical record or a FERPA protected education record.

   FERPA also applies to most public and private postsecondary institutions and student records, including those maintained by campus health clinics. At the postsecondary level, records maintained by a campus health clinic will be considered to be either "education records" or "treatment records" and protected by FERPA, not HIPAA, even if the school is considered a Regulated Entity. Generally, information contained in education records may only be disclosed with written student consent (if the student is above the age of 18 or enrolled in a postsecondary institution) unless an exception applies (e.g., disclosure required by law or in the event of an emergency to protect the safety and health of the student or others). However, treatment records also may be disclosed to external health care providers (e.g., a specialist) who are providing treatment to the student or upon student request to an external provider for review. In the event FERPA protected treatment records are disclosed for review to an external provider that is a HIPAA Regulated Entity, the records then become subject to the HIPAA rules.

Otherwise, they remain treatment records subject to FERPA so long as the records are only disclosed for treatment purposes.

If a school subject to FERPA (most schools other than private and religious elementary and secondary schools) wishes to establish formal health information exchange systems between school health providers and external primary care providers, written parental consent would be required to release information from school-based providers to external providers. However, external providers, who are governed by HIPAA, may, without parental consent, release PHI about a student to a school-based provider for treatment purposes. HIPAA also allows non-school based health care providers to release immunization records directly to a school without parent authorization.

5. a. Do special considerations arise under HIPAA or FERPA when the data exchange between school health providers and other providers is carried out electronically (e.g., via fax, internet portal, or electronic mail)?

There are no special considerations that arise based on the medium through which information is maintained or disclosed under FERPA. If information is included in an education record and maintained by an educational agency or institution (as well as contractors working on their behalf), whether that record is paper-based or electronic, it may only be disclosed (no matter the means of disclosure) with written parental consent or without consent if an exception applies (e.g., disclosure required by law or in the event of an emergency to protect the safety and health of the student or others).

Under HIPAA, PHI that is exchanged electronically is subject to the requirements of the HIPAA Security Rule. If a HIPAA Regulated Entity (or contractors acting on their behalf) is exchanging information for a permissible purpose with a Medicaid agency (e.g., payment), the Regulated Entity must meet certain administrative, physical, technical, and organizational safeguards for protecting PHI that is maintained electronically.

b. How do these laws apply to third parties, such as contractors, acting on behalf of the school or state Medicaid agency and that carry out and store the electronic information that is exchanged?

FERPA requirements apply directly to an educational agency or institution. Such an educational agency or institution must ensure that their contractors or other parties working on their behalf also meet FERPA requirements. The responsibilities of contractors and other third parties working on behalf of an educational agency or institution are likely included in the terms of a contract or other agreement. In the event a contractor or other third party violates FERPA in the course of their work for the educational agency or institution, the educational agency or institution is responsible for and can be penalized for the violation.

The same is true under HIPAA. A HIPAA Regulated Entity is responsible for meeting the requirements of HIPAA and ensuring that their contractors or other third parties working on their behalf also meet those requirements. In the event of a violation of HIPAA, the HIPAA Regulated Entity is responsible for the violation whether the HIPAA Regulated Entity violated HIPAA or one of its contractors or other third parties working on its behalf did so. Furthermore, under the 2013 modifications to the HIPAA Privacy and Security Rule, contractors and other third parties working on behalf of a Covered Entity and accessing protected health information (referred to as Business Associates) are directly liable under HIPAA as well meaning that the federal government can penalize the Business Associate directly for violations of HIPAA.

c. Under what circumstances may the health information stored in such systems be used by a Medicaid agency or school system to carry out an assessment of the quality of the program?

Whether the information is stored electronically or paper-based, the same requirements for disclosure apply under both HIPAA and FERPA. In addition, FERPA allows an educational agency or institution to disclose information maintained in an education record to accrediting organizations to perform accrediting functions. It is arguable that an accrediting organization responsible for assessing the quality of a program as part of its accreditation process would need access to identifiable student information in which case a school would be able to release information without parental consent (e.g., to verify immunization requirements met). Under this circumstance, an educational agency or institution would be able to release, without parental consent, health care information stored in education records to an accrediting organization to assess the quality of a program. Alternatively, if a quality assessment was required by law an educational agency or institution would be able to release health care information stored in education records without parental consent according to the terms of the authorizing law.

Under HIPAA, a HIPAA Regulated Entity may use and disclose PHI electronically for its own health care operations, including internal quality improvement activities. HIPAA also allows disclosures for public health, oversight, and law enforcement purposes. Depending on the nature of the request from a Medicaid agency, a HIPAA Regulated Entity may be permitted to release the data for quality assessment activities without written consent for one of these purposes.

6. Where a school requires evidence of completion of substance abuse treatment before a child referred for treatment by the school can be readmitted to school, how do HIPAA, FERPA, the Medicaid Privacy Statute, and 42 C.F.R. Part 2 affect the treating provider's ability to provide the school with information? What state law considerations might apply?

In this situation involving information related to a child's substance abuse treatment, the Part 2 Regulations are the controlling authority, not HIPAA, FERPA, or the Medicaid privacy statute. The Part 2 Regulations protect the confidentiality of alcohol and drug abuse patient records. "Records" refers to "any information, whether recorded or not, relating to treatment a patient received or acquired by a federally assisted alcohol or drug program." Patient records protected by these regulations may only be disclosed if a patient or personal representative provides written consent for the disclosure or the disclosure is made to medical personnel that require the information to immediately treat a health threat to the patient or to FDA medical personnel to facilitate patient or physician notification of errors with any product under FDA regulation. Minors may consent to the release of their information so long as they have the capacity under state law to obtain drug or alcohol treatment. Consent is necessary even if the minor's parent or guardian is disclosing information for financial reimbursement.

In all situations involving minors, state laws may be relevant as well. State laws may provide stricter protection for this type of information or limit the ability of a minor or parent of a minor to consent to disclosure (e.g, state law typically governs at what age a minor may consent to certain types of treatment such as substance abuse or mental health and/or to disclosure of related information).

7. a. How do HIPAA, FERPA, and Part 2 apply in situations in which a school nurse or a provider in a school-based clinic provides or refers a child for confidential treatment for reproductive health, mental health, or substance abuse and the referral or treatment information is entered into the child's school record?

HIPAA: Under HIPAA, the school nurse or a provider in a school-based clinic may refer a child for confidential treatment for reproductive health, mental health, or substance abuse treatment as a permissive disclosure for treatment purposes. However, once the health care information related to the referral is entered into the child's school record it is no longer governed by HIPAA, but rather FERPA (see below).

FERPA: Once any student-related information (treatment or otherwise) is entered into an education record maintained by an educational agency or institution subject to FERPA, disclosure of such information may only occur pursuant to written parent consent or if an exception applies (e.g., required by law or in an emergency to protect the health or safety of the student or others).

Part 2: Any Part 2 protected substance abuse information included either in a student's medical or education record may only be disclosed if the patient/student or personal representative provides written consent for the disclosure or the disclosure is made to medical personnel that require the information to immediately treat a health threat to the patient or to FDA medical personnel to facilitate patient or physician notification of errors with any product under FDA regulation. Minors may consent to the release of their information so long as they have the capacity under state law to obtain drug or alcohol treatment.

b. What might be the relevance of state laws under this situation? Since the information has been entered into the school record, can parents gain access to it, even where federal or state law might provide for confidentiality of care even for minors?

Health care providers, schools, and state Medicaid agencies should always consult state law experts in order to understand the additional considerations that come into play where the exchange of health information involving children and adolescents is concerned. This need for additional consultation is particularly important where the information that is the subject of focus is highly sensitive in nature, such as information regarding mental illness and emotional disorders (substance abuse and addiction related information is protected by 42 CFR Part 2), reproductive health and family planning, and diagnosis, treatment, or management of sexually transmitted diseases (STDs) or HIV.

c. What if the child receives a referral for treatment to a Title X funded clinic? What are the confidentiality rules for federally qualified health centers?

All Title X Family Planning Program staff and federally qualified health center staff must maintain the confidentiality of information they receive while providing services to individuals. Project staff may disclose the information with the individual's consent or in order to provide services which would include sharing information with other health care providers or as required by law so long as they utilize appropriate safeguards. In the case of a minor receiving care from a Title X Family Planning Program, a review of state law is critical, since (in one way or another) all state laws address the question of whether a minor's consent is required to disclose health information to a parent or guardian, as well as whether exceptions exist to a bar against the direct release of information to a parent or guardian without the minor's consent.

8. Does parental consent for two providers to exchange a child's health or school information between them automatically carry over into other treatment settings involving additional providers?

HIPAA always permits disclosure of patient information between providers for treatment purposes without patient or parental authorization. FERPA does not and new written parental consent would be required each time information is disclosed to an additional provider not included in the original consent.

Under FERPA, in the event a parent consents to the disclosure of his or her child's information contained in an education record maintained by an educational agency or institution subject to FERPA to a particular provider or multiple providers, that consent to disclose only applies to the specified providers. If the parent or the school determines that disclosures to additional individuals are necessary, the parent must provide written consent for disclosure to the additional individuals.

If the information is released to an external, non-school based health care provider regulated by HIPAA and subsequently entered into a medical record maintained by the health care provider, the information becomes PHI subject to HIPAA. In the event the information becomes PHI subject to HIPAA (e.g., entered into the medical record maintained by the provider) and the external health care provider is a HIPAA Regulated Entity, the health care provider may disclose the information to other health care providers for treatment and other HIPAA-permissible purposes without patient or parent authorization.

9. Is it possible to create a single medical record that spans school, health care, child care, and juvenile justice settings and is accessible by providers working in all settings? If so, is it possible to create a parallel consent form that would span access

by all relevant providers? In this vein, can schools create separate health information records that are not part of the education documents and therefore not subject to FERPA's special confidentiality and parental access rules?

With parental or student (if 18 or above or enrolled in a postsecondary program) consent, it would be possible to create a unified medical record in accordance with the requirements of FERPA and HIPAA as applicable. Such consent would need to authorize release of relevant and needed information to and among a set of identified individuals or organizations that would be responsible for ensuring the privacy and security of the information as applicable under FERPA and HIPAA. In that vein, it also would be possible to create a unified consent form provided the form meets the requirements of a written authorization specified by HIPAA and written consent requirements specified by FERPA. However, to the extent the record(s) would include information about alcohol and substance abuse treatment or other sensitive information potentially protected by state law, any relevant requirements also would need to be considered and in some cases information segregated to prevent unauthorized disclosure. As the health care delivery system moves towards electronic exchange and storage of information, the technology supporting the concept of a unified medical record is becoming more of a reality provided appropriate safeguards and protections can be maintained and enforced in accordance with HIPAA, FERPA, and other relevant laws and regulations including state laws.

Concluding Thoughts

Two key issues affect exchange of information across systems of care that span schools and communities. The first is where health information is stored. Is it in what would be considered the record of a HIPAA Regulated Entity? Or is it in an education record covered by FERPA? The second key question is whether written consent is required. HIPAA actually does not require consent if disclosures are for treatment, payment, and health care operations. As a result, a HIPAA Regulated Entity has more running room to disclose without consent, although, as can be seen in the case of disclosures to schools, this running room is not infinite. Disclosure without written consent is generally limited to treatment, payment, and health care operations. Where two providers are treating a child, the HIPAA Regulated Entity may be able to disclose to the school health nurse. But the HIPAA Regulated Entity could not simply disclose to the school's registration office. On the other hand, the school nurse presumably would not be able to disclose to the HIPAA Regulated Entity (e.g., a separate community health center) without parental consent.

Neither the regulations nor the Joint Guidance address what happens when a health center or other clinic operates in school satellite locations. Is the provider a single provider for purposes of being able to share the information across service sites and to Medicaid and other insurers? Or is the school-located satellite considered an agent of the school for purposes of records governance, so that parental consent would be required? One would presume that the health center would have a general consent on file for the family in any event, thereby obviating the need for further consent. But the question does not appear to be answered definitively.

What is also evident is the value of thinking about this problem in a manner that emphasizes patient engagement on the part of families and adolescents. To this end, a model Guide addressing patient engagement in creating "treatment team" consent arrangements that span different care settings would go a long way, in our view, to addressing the HIPAA/FERPA tension, since it would put a consent system in place for multi-setting, multi-jurisdictional care arrangements.

Of course a multi-site consent form might not address all issues. Patients might continue to resist most information exchange related to certain information linked to the most sensitive health conditions (e.g., mental illness, reproductive health, substance abuse). In our view, the need to develop models for allowing treating teams to share even the most sensitive information involving child and adolescent health represents fertile territory for innovative patient engagement research and evaluation because of the complexities involved in balancing the need for information flow against concerns of privacy and confidentiality.