

Public Health Access to Student Health Data: Authorities and Limitations in Sharing Information Between Schools and Public Health Agencies

Issue Brief

Introduction

The ability of public health officials to access health and other relevant data from schools and education agencies has been an ongoing challenge. In daily public health responsibilities, as well as in emergencies, federal education privacy requirements have limited or blocked public health agencies' access to data in areas such as immunization, mental health, injury, and absentee records. Public health officials must understand their legal authorities and limitations in acquiring and using data from education entities. This issue brief examines the interplay of federal laws related to privacy and disclosure of student health information, and various approaches for obtaining student health information. The term "school" is used in this issue brief to collectively refer to elementary, secondary (high school), and post-secondary (college) institutions, unless otherwise specified. The term "education agencies" generally refers to state education agencies and local school districts, unless otherwise noted.

I. Public Health Data Needs From Schools

Public health focuses on developing, implementing, and evaluating population-based strategies addressing diseases and other threats to health in the general population and in subgroups of the population. Children and adolescents are important population subgroups; the ability of public health officials to regularly access data about them is a key factor in creating effective public health programs affecting these groups.¹ Schools serve as a centralized location for current and long-term data about school-aged populations.

Data from schools can help public health agencies conduct surveillance, intervention, and prevention activities. Examples of the types of activities public health agencies undertake with school-based data include:¹

- Identifying outbreaks of infectious diseases and other health conditions, such as H1N1, staph infections, or community acquired methicillin-resistant *Staphylococcus aureus* (MRSA) infections.
- Tracking immunization coverage to prevent outbreaks of infectious diseases like mumps or measles.
- Identifying trends in chronic and environmental diseases, including the prevalence of asthma, autism, and developmental disabilities.
- Finding trends in injuries among students and evaluating effectiveness of injury-prevention activities.
- Tracking overall health status, rates of overweight and obesity, and prevalence of diabetes and other diet-related conditions.
- Identifying and analyzing environmental exposures related to health concerns, such as exposure to lead or other toxic substances.
- Monitoring for environmental and infectious disease outbreaks in the aftermath of natural disasters and other emergencies.

School-based data also helps in identifying specific needs, targeting health promotion and disease prevention activities, evaluating the effectiveness of public health programs, and tracking long-term health outcomes.¹

Public health agencies view schools and education agencies as important partners in protecting children and adolescents from health threats. Sharing data between schools and public health agencies may, in some instances, be the only realistic and reliable method for getting the information necessary to conduct public health activities, such as tracking immunization rates.¹ However, as will be discussed below, federal privacy protections for student education records have caused difficulties for public

health efforts to conduct mandated and discretionary federal and state public health activities.

II. Federal Laws Governing Health Information Privacy and Disclosure

Two federal laws figure prominently in the discussion of public health access to school data—the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA). This section describes these laws as they relate to privacy and disclosure of student health and other records. HIPAA's Privacy Rule specifically excludes student education records covered under FERPA from coverage under the Privacy Rule. Thus, FERPA governs student health information that falls within the purview of that act; other health-related records outside of FERPA are governed by HIPAA and any applicable state laws.

Family Educational Rights and Privacy Act

The Family Educational Rights and Privacy Act (FERPA)² is a federal law intended to protect the privacy of student education records while allowing students and parents greater access to the records. FERPA, among other things, prevents the disclosure of a student's education record without the consent of a parent or eligible student unless an exception to the law's general consent requirement applies.⁸ "Eligible students" are students who have turned 18 or attend school beyond the high school level at any age.⁹ Schools must notify parents and eligible students annually of their rights under FERPA; the exact method of this notice (e.g., newsletter, student handbook, etc.) is left to the discretion of each school.⁹

FERPA applies to all educational institutions and agencies that receive any funds for programs administered by the U.S. Department of Education (ED or the Department).⁹ Thus, all public schools and school districts and most public and private post-secondary institutions (e.g., colleges) are covered by FERPA.¹¹ Private and religious elementary and secondary schools are not subject to FERPA because they generally do not receive funding from ED.¹¹ ED has historically interpreted FERPA to exclude "non-school" entities, which are not attended by students, from the scope of entities covered by the act. However, amendments to FERPA regulations in December 2011 reflect ED's changed view; the rule now acknowledges that the Department funds entities that do not have students and authorizes ED to enforce FERPA for programs funded by ED or that

disclose or receive protected information under the act.²⁹ (See [ASTHO Current Issues–Winter 2012: Analysis of Revised FERPA Regulations](#)) for more information about the rules changes.)

Rights Under FERPA

FERPA give parents and eligible students the right to:

- Review the student's education records maintained by the school.
- Request that a school correct records which they believe to be inaccurate or misleading.
- Require nondisclosure of the student's education record or personally identifiable information from the record without prior written consent of a parent or eligible student (known as the "general consent rule"), unless an exception applies.

In a written request for consent to disclose, a school must identify the records to be disclosed, the person or entity to whom the information is to be disclosed, and the purpose of the disclosure.² A parent or eligible student has the right to request and receive a copy of the information disclosed to a third party.²

Education Record Defined

"Education record" is defined as records which are: (1) directly related to a student and (2) maintained by an educational agency or institution or by a person acting on behalf of the agency or institution.¹⁰ A student's health records, including immunization information and other records maintained by a school nurse, are considered part of the student's education record and thus are protected from disclosure under FERPA. Records of medical and psychological treatment of eligible students at post-secondary institutions ("treatment records") are excluded from the definition of education records under FERPA if the records are made, maintained, and used only in the treatment of the student and are disclosed only to persons providing treatment.^{2,10,11} Treatment records can be disclosed for purposes other than treatment, but disclosure must be made with consent or under one of the exceptions to the consent requirement.¹¹ If treatment records are released for purposes other than treatment, then they are considered to be education records and all the FERPA requirements then apply.¹¹ FERPA also generally excludes from the definition of "education records" records that are kept by a school's law enforcement unit, security videos, observations by instructors, or records created after the student no

longer attends the school.¹⁰ Records of special education students receiving services under the Individuals With Disabilities Education Act (IDEA) are covered as education records under FERPA.¹⁰

Personally Identifiable Information Defined

FERPA regulations define “personally identifiable information” (PII) to include name, address, personal identifiers like Social Security number or date of birth, biometric data, or other information that could be used alone or in combination to identify a student.¹⁰ However, schools may disclose without consent “directory information” such as a student’s name, address, telephone number, date and place of birth, honors and awards, and dates of attendance.^{9,29} Schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them.^{9,29}

Exceptions to FERPA

FERPA contains a number of exceptions that allow schools to disclose PII from a student’s education record without consent of a parent or an eligible student. Schools may disclose de-identified information without written consent.¹⁰ In addition to disclosures to parents and eligible students, and for directory information, FERPA regulations identify the parties or circumstances in which disclosure of PII may be made without consent.^{9,10} Historically, these exceptions have been narrowly construed by ED to err on the side of protecting the student’s privacy over making a disclosure. Thus, ED interpretations have resulted in a very narrow scope of circumstances and recipients for the release of education records without prior written consent by a parent or eligible student.

School Officials

Information may be given to school officials, including teachers, with a legitimate educational interest. A contractor, consultant, volunteer, or other party to which the school has outsourced activities may be considered a school official if the contractor, etc. is: (1) performing a function that a school employee would otherwise perform; (2) under the direct control of the school when using or maintaining the education records; and (3) subject to FERPA’s limitations on redisclosure of education records.^{19, 20} Schools must make a record of the requests for disclosure and each disclosure of PII it makes, as well as officials that may redisclose the information.²⁸

Specified Officials and Their Authorized Representatives

Disclosure without prior consent is permitted to the U.S. Comptroller General, the U.S. Attorney General, the ED Secretary, or state and local educational authorities.¹⁹ Disclosures to these officials—or their authorized representatives—must be made in connection with an audit or evaluation of federal or state-supported education programs or to enforce or comply with federal legal requirements related to those programs.²³ Recent amendments to FERPA’s regulations newly defined an “authorized representative” as “any entity or individual designated by a state or local educational authority or agency headed by [the officials listed in the rule].”²⁹ Education records disclosed must be protected so that only the specified officials or their authorized representatives have access to PII, and the records must be destroyed when they are no longer needed for the purposes for which they were disclosed.²³ However, these requirements can be waived if the parent or eligible student consents to the disclosure or if collection of PII is expressly authorized by federal law.²³

The “authorized representative” exception for disclosure without consent for audits, evaluations, or studies have been used in the past as a basis for creating memoranda of agreement (MOA) between state and local health and education agencies to share data. Even ED had an MOA with the Centers for Disease Control and Prevention (CDC) in which ED designated the CDC as its authorized representative for the purposes of collecting information under the Metropolitan Atlanta Developmental Disabilities Surveillance Program.²⁹ However, ED guidance and amendments to FERPA regulations in 2008 ultimately narrowed the Department’s interpretation of the scope of “authorized representatives” to generally exclude other state and federal agencies because they were not under the “direct control” of the state educational authority.^{12,30} Amendments to the FERPA rules in December 2011 have allowed non-education agencies to again serve as authorized representatives under FERPA for audits, evaluations, or studies related to educational programs.²⁹ The revised rules also require that state or local educational authorities use “reasonable methods” to ensure that their authorized representatives comply with FERPA and that education authorities enter into written agreements with their representatives specifying the information disclosed and the handling of the information to protect PII.²⁹ ED has issued guidance

addressing the “reasonable methods” and written agreement requirements.²⁹

Health and Safety Emergencies

A school may disclose PII from education records in connection with an emergency if the “information is necessary to protect the health or safety of the student or other individuals.”^{19,25} Information may be disclosed to “appropriate parties,” which include the parents of an eligible student, as well as parties like law enforcement, public health officials, and trained medical personnel.^{8,25} In determining whether to make a disclosure for a health or safety emergency, a school “may take into account the totality of the circumstances pertaining to a threat to the health or safety of a student or other individuals.”²⁵ If the school determines that there is an “articulable and significant threat” the school may disclose information necessary to protect the health or safety of the student or other individuals.²⁵ ED will defer to the judgment of the school in making a determination that, based on the information available at the time, there was a rational basis for the determination.²⁵ The limitations on the health and safety emergencies exception do not prevent a school from including appropriate information about a student’s disciplinary record in the education record or sharing the disciplinary information with teachers and school officials with a legitimate educational interest in the behavior of the student.²⁵ School officials are required to make a record of the PII disclosed under the health and safety emergency exception that identifies the threat that gave rise to the disclosure, the parties the information was disclosed to, and the information disclosed.²⁸

The health and safety exception has traditionally been narrowly construed by ED. Agency guidance states that an “emergency” under FERPA means “a situation in which there is an articulable and significant threat to the health or safety of students or other individuals.”⁸ However, an “emergency does not include the threat of a possible or eventual emergency for which the likelihood of occurrence is unknown.”⁸ In response to a university regarding potential conflicts between state notifiable diseases and conditions reporting requirements and FERPA, FPCO determined, among other things, that for those conditions the state health regulations require immediate reporting on an emergency basis would fall under the FERPA health and safety emergency exception.³⁴ For conditions that did not require emergency reporting, the disclosure of PII in these

circumstances would not meet the imminent threat requirement, so consent was required.³⁴

Studies on Behalf of the School

Disclosures without consent may be made to organizations conducting certain studies for or on behalf of the school.¹⁹ “Organization” is defined to include “federal, state, and local agencies, and independent organizations.”¹⁹ These studies must relate to: (1) developing, validating, or administering predictive tests; (2) administering student aid programs; or (3) improving instruction.¹⁹ Education records disclosed must be protected so that only representatives of the organization have access to PII and the records must be destroyed when no longer needed for the purposes for which the study was conducted.¹⁹ The school must have a written agreement with the organization conducting the study that specifies the purpose and scope of the study and the information to be disclosed.¹⁹ The agreement must also address the organization’s protection of personally identifiable information and ultimate destruction of PII upon completion of the study.^{19,29} Recent amendments to FERPA regulations clarified that state education agencies are allowed to make nonconsensual disclosures of PII for studies in the same way schools and other education officials are.²⁹ Previous interpretations of the rules did not allow state education agencies to make disclosures for studies without consent.²⁹

Judicial Actions

Schools may disclose education records without consent to comply with a judicial order or lawfully issued subpoena. However, the school must make a reasonable effort to notify the parent or eligible student of the order/subpoena before the school complies with it to allow the parent or eligible student time to seek “protective action.”¹⁹ Schools are not required to give advance notice of a disclosure due to judicial action if the disclosure is being made in compliance with: (1) a federal grand jury subpoena for which the court has ordered that the existence or contents of the subpoena not be disclosed; (2) any other subpoena for which the court has ordered that the existence or contents of the subpoena not be disclosed; or (3) an ex parte court order obtained by the U.S. Attorney General or Assistant Attorney General concerning investigations or prosecutions related to an act of domestic or international terrorism.¹⁹ If a school initiates legal action against a parent or student, or if the school is sued by a parent or student, the school may disclose

education records relevant to the matter to the court without a court order or subpoena.¹⁹

Transferring Schools

A school may disclose a student's education records to another school, school system, or education institution (e.g., college) to which the student is already enrolled or intends to enroll or transfer.¹⁹ Provisions in the No Child Left Behind Act of 2001 require states to assure ED that there are procedures in place to facilitate the transfer of disciplinary records regarding suspension or expulsion of a student enrolling or transferring to a public or private elementary or secondary school.^{19,21} A school must attempt to notify the parents or student of the disclosure, give them a copy of the education record if requested, and give them the opportunity for a hearing if requested.²²

Financial Aid

A school may disclose a student's education record to appropriate parties if the disclosure is made in connection with the student's application for or receipt of financial aid.¹⁹ The disclosure may be made without the student's consent if the information is necessary to determine eligibility, amount, and conditions of financial aid or to enforce the terms and conditions of the aid.¹⁹

Accrediting Organizations

Disclosures may be made without consent to accrediting organizations.¹⁹

Juvenile Justice Authorities

Schools can disclose education records to state and local authorities within a juvenile justice system pursuant to specific state laws.^{19,24}

FERPA Liability and Enforcement

FERPA and its implementing regulations do not address any liability or immunity issues.^{2,10} There is no private cause of action in FERPA; individual parents or students may not bring a lawsuit to enforce the act's provisions or seek redress for violations of the act. Persons who believe their rights under FERPA have been violated may file a complaint with the ED's Family Policy Compliance Office (FPCO), which investigates the complaint.^{8,10} FPCO is authorized to, among other things, revoke funding for institutions found in violation of FERPA and its regulations.^{8,10} FPCO is also authorized to bar education entities or agencies and other recipients of

PII that violate FERPA regulations from receiving PII for five years after a violation.^{10,29}

FERPA and State Laws

Any state law or regulation that conflicts with FERPA and its regulations is preempted by the federal law, and the federal requirements take precedence over the state requirements. However, if an educational agency or institution, a recipient of ED funds, or another party to which PII has been nonconsensually disclosed determines that it cannot comply with FERPA or the regulations because of a conflict with state or local laws, it must notify FPCO within 45 days and provide the text and citation to the conflicting state or local law.^{2,29,31} FPCO reviews the conflicting law and any interpretations of it made by the state and provides guidance to the requesting agency or institution regarding FERPA's applicability to the situation.³² However, ED does not have authority to waive or modify any of FERPA's requirements.³² If an education agency or institution is found to be in conflict with FERPA, ED may withhold further payments under any of its programs, issue a complaint to compel compliance, terminate an institution's eligibility to receive funding, or take any other action authorized by law.^{10,32,33,34}

The Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)³ and subsequent amendments enacted changes in the health insurance market and addressed the electronic transmission of health information and the protection of personal health information, among other things. Title II of HIPAA contained a number of administrative simplification and privacy provisions that instructed the Secretary of Health and Human Services (HHS) to issue standards addressing, among other things, the electronic transmission of health information and the privacy of personally identifiable medical information.⁴ In 2000, HHS promulgated rules, *Standards for Privacy of Individually Identifiable Health Information* (the "Privacy Rule"), which set national standards for the protection of certain health information⁵ and has issued subsequent modifications to the rule. The HIPAA Privacy Rule creates a set of basic consumer protections and a series of regulatory permissions for uses and disclosures of protected health information.⁶

HIPAA Privacy Rule

The HIPAA Privacy Rule prohibits covered entities from disclosing protected health information to any third parties, unless the rule otherwise permits the disclosure.⁶

Covered Entities

The Privacy Rule applies to covered entities and their business associates. “Covered entities” are defined as health plans, healthcare clearinghouses, and any healthcare provider that transmits health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA.⁷ A “business associate” is a person or organization not employed by the covered entity that performs certain activities for a covered entity involving the use or disclosure of individually identifiable health information.⁷ A “hybrid entity” is a single legal entity that conducts both covered and noncovered activities under the Privacy Rule.⁷ State and local health departments, for instance, can be hybrid entities if they provide healthcare services to patients for which the agencies transmit health information electronically in addition to conducting their other public health functions. If a state or local health department does not perform these activities, then it would not be a covered entity under the HIPAA Privacy Rule. A hybrid entity must designate in writing its activities that are covered under the Privacy Rule. Thus, if a health agency qualifies as a hybrid entity and it makes the required list of covered activities, then only its healthcare services would be covered under the Privacy Rule; otherwise, all of the hybrid’s activities would be deemed covered under the rule.

Protected Health Information

The Privacy Rule applies to protected health information (“PHI”). PHI is individually identifiable health information held or transmitted by a covered entity or its business associate in any form or media—electronic, paper, or oral. “Individually identifiable health information” is defined to include the types of data listed below that identify the individual or that could be reasonably used to identify the individual:⁷

- Demographic data.
- Common identifiers (e.g., name, address, birth date, Social Security number).
- Information relating to the individual’s past, present, or future physical or mental health condition and healthcare provided to the person.

- Payment for healthcare.

Employment records maintained by a covered entity for its own employees and education records covered by FERPA are specifically excluded from the definition of PHI in the Privacy Rule.⁵ There are no restrictions on the use or disclosure of de-identified health information.⁷

General Disclosure Rule

The Privacy Rule states that a covered entity may not use or disclose PHI except as permitted by the Privacy Rule or as authorized in writing by the person who is the subject of the PHI (or their personal representative).⁷ The rule also requires disclosure to the person/representative or to HHS as part of an enforcement action.⁷

Permitted Uses and Disclosures

The Privacy Rule identifies a number of circumstances in which use or disclosure of PHI is specifically permitted. A covered entity is permitted, but not required, to use and disclose PHI without an individual’s authorization for the following purposes or situations:

- *To the Individual*—To the person who is the subject of the PHI.⁷
- *Treatment, Payment, and Healthcare Operations*—A covered entity may use PHI for its own treatment, payment, and healthcare activities like quality assessment or evaluations. Obtaining patient consent for disclosure of PHI for treatment, payment, and healthcare operations activities is optional under the Privacy Rule.⁷
- *Uses and Disclosures With Opportunity to Agree or Object*—The Privacy Rule allows covered entities to obtain informal permissions by giving persons opportunities to agree or object to the use and disclosure of PHI. Such instances include providing information for hospital directories or notifications to family members. If a person is incapacitated or unavailable to give permission, the covered entity is allowed to exercise its professional judgment in deciding whether the use or disclosure is in the person’s best interest.⁷
- *Incidental Use and Disclosure*—The Privacy Rule does not require covered entities to guarantee that all incidental disclosures of PHI made during an otherwise permitted use and disclosure are

eliminated. Such incidental disclosures are permitted under the rule so long as the covered entity has taken reasonable steps to safeguard against disclosures and that information shared is the minimum necessary under the rule.⁷

- **Public Interest and Benefit Activities**—The Privacy Rule permits the use and disclosure of PHI without a person’s consent in a number of specific situations identified in the rule as “public purposes.”⁷ (See detailed discussion below.)
- **Limited Data Set**—The Privacy Rule allows the use or disclosure of limited data sets for the purposes of research, public health, or healthcare operations.⁷ Limited data sets are those in which 16 of 18 categories of specific identifiers about persons or their households have been removed. Limited data sets may include identifiers like city, state, ZIP code, and elements of the date.³⁶ Limited data sets may be used for research and public health purposes so long as users of the data have entered into a data use agreement to protect the PHI in the limited data set. A limited data set is different from de-identified data because the limited data set still contains some PHI.

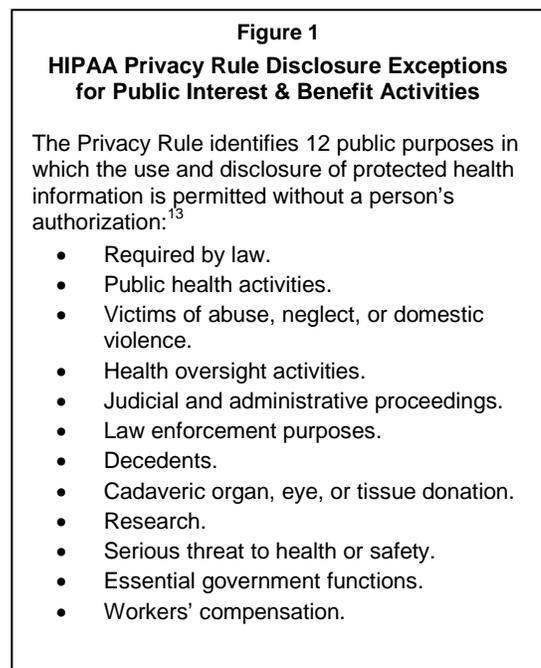
Covered entities may rely on professional ethics and best judgment in deciding which of these permissive uses and disclosures to make.⁷

Disclosures for Public Interest and Benefit Activities

The Privacy Rule permits use and disclosure of PHI without an individual’s authorization for public purposes.⁷ The rule allows, but does not require, these disclosures to recognize the important uses for health information beyond the realm of healthcare.⁷ Several of these exceptions are described below. Figure 1 lists all of the 12 public purposes in the Privacy Rule.

- **Public Health Activities**—Covered entities are allowed to disclose PHI for a variety of public health activities identified in the Privacy Rule. The rule allows disclosure to:¹⁴
 - Public health officials authorized by law to collect or receive PHI for preventing or controlling disease, injury, or disability.
 - Public health or other government officials authorized to receive reports of child abuse and neglect.

- Persons and entities subject to FDA regulation regarding FDA-regulated products or activities for purposes such as adverse event reporting, tracking of products, product recalls, and post-marketing surveillance.
- Persons who may have contracted or been exposed to a communicable disease when notification is authorized by law.
- Employers who request information about their employees’ work-related illnesses or injuries or workplace-related medical surveillance data when this information is needed by the employer to comply with the Occupational Safety and Health Administration (OSHA), the Mine Safety and Health Administration (MSHA), or similar state laws.
- **Serious Threat to Health or Safety**—The Privacy Rule allows covered entities to disclose PHI they believe is necessary to prevent or lessen a serious and imminent threat to a person or the public when such disclosure is made to someone they believe can prevent or lessen the threat (including the target of the threat).⁷ Covered entities may also disclose to law enforcement if the information is needed to identify or apprehend an escapee or violent criminal.⁷



- **Judicial and Administrative Proceedings**—The Privacy Rule permits covered entities to disclose protected health information in a judicial or administrative proceeding if the request for the

information is through an order from a court or administrative tribunal.⁷

Waivers of HIPAA During Emergencies

Federal law provides for the waiver or modification of certain HIPAA requirements during emergencies. Section 1135 of the Social Security Act (SSA) authorizes the HHS Secretary to temporarily modify or waive certain Medicare, Medicaid, State Children's Health Insurance (SCHIP), and HIPAA requirements.¹⁵ The purpose of the 1135 waiver authority is to ensure that sufficient healthcare services are available to meet the needs of individuals enrolled in SSA programs when and where an emergency is experienced. Service providers who in good faith are unable to comply with certain requirements are reimbursed for the services they provide during an emergency and are exempted from sanctions for noncompliance absent fraud or abuse. Section 1135 waivers require both a declaration of national emergency or disaster by the President under the National Emergencies Act or the Stafford Act and a public health emergency determination by the HHS Secretary under Section 319 of the Public Health Service Act (PHSA).

SSA Section 1135 addresses, among other things, the waiver of sanctions arising from noncompliance with HIPAA privacy regulations relating to: (1) obtaining a patient's agreement to speak with family or friends or honoring a patient's request to opt out of the facility directory; (2) distributing a notice of privacy practices; or (3) the patient's right to request confidential communications. The waiver is effective only if actions under the waiver do not discriminate as to the patient's source of payment (e.g., Medicare, Medicaid, private insurance) or ability to pay.

Once the 1135 waiver has been authorized by the HHS Secretary, healthcare service providers' requirements are not automatically waived or modified. The Centers for Medicare and Medicaid Services (CMS) implements the waiver by determining on a case-by-case basis whether and the extent to which sufficient grounds exist for waiving requirements with respect to a particular provider, to a group or class of providers, or to a geographic area.¹⁷ Providers can submit requests to operate under the waiver authority to regional CMS offices and to CMS for other relief beyond the scope of discretion granted to CMS regional offices and state survey agencies. Section 1135 waivers generally expire when the underlying emergency/disaster

declaration terminates; however, waivers related to the HIPAA privacy rule are subject to different requirements and are generally limited to a 72-hour period beginning with implementation of a hospital disaster protocol.¹⁶

HIPAA Liability and Enforcement

The Privacy Rule does not authorize individuals to sue for violations; individuals must direct their complaints to HHS' Office for Civil Rights (OCR), which then investigates the complaint. In cases of noncompliance, the Secretary is directed to resolve the matter by informal means.⁷ If the matter cannot be resolved informally, the Secretary may issue written findings of noncompliance that may be used as a basis for initiating a civil action or a criminal referral.⁷ Covered entities that knowingly and improperly disclose identifiable health information are subject to civil monetary penalties (\$100 per violation up to \$25,000 per year) and criminal penalties (up to \$250,000 and imprisonment up to 10 years).⁷

HIPAA and State Laws

In general, any state laws or regulations that conflict with HIPAA and the Privacy Rule are preempted by federal law, and the federal requirements control over the state requirements. However, the Privacy Rule does contain several exceptions that allow differing state requirements to control:^{7,18}

- The state law relates to privacy of individually identifiable health information and provides greater privacy protections or rights than the Privacy Rule.
- The state law requires the reporting of disease or injury, child abuse, birth, or death and for public health surveillance, investigation, or intervention.
- The state law requires certain reporting by health plans, such as for management or financial audits or evaluations.

States can also request a determination that a conflicting state law will not be preempted by HIPAA regulations if the state can demonstrate one of the conditions enumerated in the rule, including, but not limited to, that the conflicting state provision serves a compelling public health, safety, or welfare interest, and, if the conflicting state requirement relates to a privacy right, that the intrusion into privacy is warranted given the public interest being served.^{7,18}

III. Public Health Access to Student Health Data

Both FERPA and HIPAA contain provisions and exceptions that could be used to facilitate public health agencies' access to student health and other data. The ability to access data under either law requires that the parties seeking access are eligible to receive the data or the circumstances give rise to access. A key distinction in each of the acts is when access to data is permitted with and without consent. This section discusses theories that have been used by health agencies—with varying degrees of success—to allow public health agencies access to student health data.

Obtain Consent

Under FERPA, public health agencies can access education records—including student health data maintained by the school or a person acting on its behalf—if the school has received written consent from a parent or eligible student. The written consent must identify the data to be released, the parties to whom the data will be released, and a description of how the data will be used and it must be signed and dated by the parent or student.²⁶ ED states that such releases are advisable, for instance, for health agencies wishing to use PII to track absences due to H1N1 or other outbreaks before an emergency is recognized; ED has developed sample consent forms for schools and health agencies to use.⁸ Similarly, under HIPAA, health agencies can obtain PHI from covered entities if the agency has received written consent from the patient or their personal representative. If a school's health records are not covered under FERPA—as is generally the case for private elementary and secondary schools—they may be subject to HIPAA as a covered entity if they transmit health information electronically. Health agencies may need written consent to obtain student health data from the school or from students' healthcare providers if no other Privacy Rule exceptions apply.

Use De-Identified Data

Under FERPA, schools can provide public health agencies with access to student health and other relevant data if the information does not contain PII.¹⁹ Thus, ED guidance notes that, in instances like the H1N1 influenza pandemic or other outbreaks, a school may share with a public health agency general information about the number of students absent from the school without prior written consent.⁸

However, if absentee data to be shared with a health agency includes PII and no FERPA exception applies, then the school must obtain written consent before sharing the data with public health officials.⁸

De-identified data must not allow the recipients to identify the students through either a single release or multiple releases of data or to combine the data with other information to identify the students.^{8,19} ED guidance notes that disclosing the absence of all students in a particular activity, class, or grade would result in potential FERPA violations if directory information—which is not considered part of the education record—could be used to identify all the students in that activity, class, or grade.⁸ ED guidance also specifies that while schools are permitted to make nonconsensual disclosures of directory information (e.g., name, address, phone number, grade level, etc.) for students who have not opted out of the directory, FERPA does not permit the disclosure of directory information if it is linked with other non-directory information.⁸ Therefore, a school may not release directory information only for students who have been absent from school.⁸

Under HIPAA, the Privacy Rule does not restrict the use or disclosure of de-identified health information so long as all identifiers have been removed.³⁶

Use Limited Data Sets

HIPAA countenances the release of limited data sets for public health, research, and other purposes.⁷ These data sets have had specific identifiers about the patient or household removed. Users of limited data sets must complete a data use agreement that addresses the use and protection of PHI in the limited data set.⁷ This exception to the privacy rule permits public health agencies to access limited health data about children and adolescents who are not covered under FERPA, such as those who are home schooled or attend private elementary or secondary schools.

Access Data Not Maintained by the School

FERPA applies to education records, including immunization and other student health data, which is maintained by schools or education agencies. Student health data that is maintained by a school nurse who is an employee of the school or acting on behalf of the school is considered to be part of the student's education record. If a person or entity acts on behalf of the school, such as a school nurse providing health services (whether at the school or off site) under contract or otherwise under the "direct control" of a

school, and maintains student health records, then these records are considered education records under FERPA as if the school was maintaining the records directly.¹¹ However, if a person or entity provides health services directly to students and is not employed by, under contract to, or otherwise acting on behalf of a school, then the resulting health records are not deemed to be part of the education record covered by FERPA.¹¹ Even if the services are provided at the school, the resulting health records are not covered by FERPA because the person or entity creating and maintaining the health records is not acting on behalf of the school.¹¹

If a school's education records are not covered under FERPA, as is generally the case for private elementary and secondary schools, they may be subject to HIPAA as a covered entity if they transmit health information electronically. In this scenario, the school is a covered entity and student health records are PHI under the Privacy Rule. One of the rule's permitted exceptions, such as a public health activity, would have to apply before the records are released without consent. If the records are not covered under FERPA or HIPAA, state or local privacy laws may still apply.

Access for Public Health Activities

HIPAA contains a comparatively robust public health exception that allows public health authorities to receive PHI without prior consent of a patient or their representative. However, FERPA does not contain a parallel "public health exception" to the one found in HIPAA. And, because education records covered by FERPA are expressly excluded from the Privacy Rule, public health authorities cannot use HIPAA's public health exception to access school education records without consent.

Access Permitted in Emergencies

Both HIPAA and FERPA contain exceptions that permit disclosure of student data to specified officials in emergencies.

HIPAA Exception for Threats to Health or Safety

HIPAA contains a specific exception for disclosure of protected health information in emergencies, in addition to its broad public health exception. The Privacy Rule allows covered entities to disclose PHI that they believe is necessary to prevent or lessen a serious and imminent threat to a person or the public, when such disclosure is made to someone they believe can prevent or lessen the threat (including the target of the threat).⁷ Covered entities

may also make disclosures to law enforcement officials if the information is needed to identify or apprehend an escapee or violent criminal.⁷ HHS specifically notes that PHI can be released without disclosure to public officials who are reasonably able to respond to, prevent, or lessen a bioterrorism or other public health threat or emergency.³⁵

FERPA Emergency Exception

FERPA contains an exception for nonconsensual disclosure of personally identifiable information in student education records to "appropriate parties" during emergencies if the information is necessary to protect the health and safety of the student or other individuals. ED has identified public health officials as appropriate parties eligible to receive PII during an emergency.⁸ This exception has been narrowly construed by ED to be limited to the period of the emergency; it does not provide for a blanket release of PII from student education records in an emergency.⁸ Each school or education agency is responsible for making a case-by-case determination that the release of PII is necessary to address an "articulable and significant threat."⁸ ED has indicated that it will defer to the judgment of the school or agency in making the determination that there was a "rational basis" for the decision given the nature of the emergency and the appropriate parties to whom the disclosure was made.⁸ FERPA regulations require that within a reasonable period after an emergency disclosure is made, the school or education agency must make a record of the emergency disclosure in the student's education record.²⁸ The record of the emergency disclosure must state the articulable and significant threat that was the basis for the emergency and identify the parties to whom the student's PII was disclosed.²⁸ ED guidance further notes that often, "... threats to health and safety can be fully addressed by sharing appropriate information regarding such threats with parents, the health department, or others in a manner that does not identify particular students."⁸

While more recent guidances issued by ED have generally followed prior interpretations of the emergencies exception, these pronouncements have included more detailed statements related to pandemic influenza (specifically H1N1) and emergency responses to manmade events and natural disasters.^{8,27} Specifically, ED has stated that "... an emergency can exist without a public health authority designation of an emergency."⁸ The FERPA emergency exception may be properly applied if a

public health authority determines that an outbreak (e.g., H1N1 or tuberculosis) poses a significant threat to a community; if so, then schools in that community may also determine that an emergency exists.⁸ ED also noted that an emergency declaration by the HHS Secretary that a public health emergency exists, such as in the case of the October 2009 H1N1 declaration, may serve as a rational basis for a school to determine that an emergency exists, “so long as there is a *current outbreak* of H1N1 in the particular school or school district” (emphasis in original).⁸

Where there is an articulable and significant threat that may be addressed by a “limited release of information to appropriate parties,” and that release is temporally limited to the period of the emergency, the school or education agency may release information “... at any stage of such emergency ...” including “... sharing information where necessary during the early stages of a pandemic.”⁸ In another example from recent guidance, ED notes that school officials would generally be permitted under the emergencies exception to disclose immunization records to public health officials to determine whether or not students have been vaccinated for typhus or other waterborne diseases in the aftermath of flood.²⁷

However, these recent guidances also stress that disclosures made for general emergency preparedness activities are *not* covered under the FERPA emergencies exception.^{8,27} The FERPA emergencies exception would not apply in situations where a threat of a possible or eventual emergency exists but the likelihood of its occurrence is unknown.^{8,27} There must be a temporal linkage to an articulable and significant threat.^{8,27} Yet, ED has indicated that properly designated directory information for students whose parents have not opted out of the disclosure of directory information may be shared with state or local agencies for emergency planning purposes.²⁷ However, if health or emergency management agencies need PII to prepare in advance for the emergency evacuation of special needs children or children on special medications, the school must obtain written consent before making the disclosure.²⁷

Act as an Authorized Representative

Previously, ED interpreted FERPA to allow state/local health agencies to enter into agreements with state/local education agencies to act as the authorized representative of the education agencies

and therefore be eligible to access education records, including student health information, that contain PII without the prior written consent of a parent or eligible student. However, subsequent ED interpretations of FERPA explicitly restricted the release of student education records under the “authorized representative” exception to other entities that are under the control of a school or education agency. The “control of” requirement has been defined as persons who are employees or contractors of the school or education agency. ED has recently amended the FERPA rules to again permit non-education agencies to act as authorized representatives. The “authorized representative” exception is limited to audits and evaluations of federal and state educational programs and the enforcement of federal legal requirements related to those programs. Therefore, despite the expanded scope of entities eligible to serve as authorized representatives, this exception may be of limited or no use for public health agencies seeking to access student health data unrelated to education programs.

Interagency Agreements

In the past, some states have used various forms of interagency agreements between state or local health departments and schools or education agencies as a mechanism to allow for the nonconsensual disclosure of PII in education records. As discussed above, recent guidance by ED has affirmed that such interagency agreements do not supersede FERPA’s consent requirements.^{8,27}

Disclosure Required by Court Order or Subpoena

Both HIPAA and FERPA contain exceptions for disclosure without consent if required by judicial order or subpoena. Under FERPA, a school or education agency must disclose PII from a student’s education record if required by a court order or subpoena; prior written consent of the parent or eligible student is not required.¹⁹ However, the school must make reasonable efforts to notify the parent or eligible student about the impending release before complying with order/subpoena.¹⁹ Similarly, the HIPAA Privacy Rule permits covered entities to disclose PHI in a judicial or administrative proceeding if the request for the information is through an order from a court or administrative tribunal.⁷ The broad public health exception under the Privacy Rule would make it unlikely that a health agency would have to seek a court order or subpoena to access PHI.

Regarding FERPA, a health department could arguably obtain a court order or subpoena to access PII in student education records absent written consent or another exception to the FERPA general consent rule; however, the circumstances giving rise to such judicial action would likely satisfy the requirements for an exception in the first place. ED

notes that “this exception could be used when an emergency no longer exists or the party seeking personally identifiable information from students’ education records would not typically be considered an ‘appropriate party’ under the health or safety emergency exception to general consent.”²⁷

Sources

¹ Association of State and Territorial Health Officials. “Accessing School Health Information for Public Health Purposes” Position Statement. 2006. Available at [www.astho.org/Advocacy/Policy-and-Position-Statements/ under “FERPA and Public Health”](http://www.astho.org/Advocacy/Policy-and-Position-Statements/under%20FERPA%20and%20Public%20Health). Accessed January 31, 2012.

² Family Educational Rights and Privacy Act (FERPA) codified at 20 U.S.C. §1232g.

³ Health Insurance Portability and Accountability Act (HIPAA) of 1996. (P.L. 104-191).

⁴ Chaikind H et al. Congressional Research Service. *The Health Insurance Portability and Accountability Act (HIPAA) of 1996: Overview and Guidance on Frequently Asked Questions* (RL31634). January 24, 2005. Available at www.law.umaryland.edu/marshall/crsreports/crsdocuments/RL3163401242005.pdf. Accessed January 31, 2012.

⁵ U.S. Dept. of Health and Human Services. *Standards for Privacy of Individually Identifiable Health Information*. 45 C.F.R. Parts 160, 164.

⁶ Stevens GM. Congressional Research Service. *A Brief Summary of the HIPAA Medical Privacy Rule* (RS20934). April 30, 2003. Available at www.law.umaryland.edu/marshall/crsreports/crsdocuments/RS20934.pdf. Accessed January 31, 2012.

⁷ U.S. Dept. of Health and Human Services. “Summary of HIPAA Privacy Rule” website. Available at www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html. Accessed January 31, 2012.

⁸ U.S. Dept. of Education. “Family Educational Rights and Privacy Act (FERPA) and H1N1.” October 2009. Available at <http://www2.ed.gov/policy/gen/guid/fpco/pdf/ferpa-h1n1.pdf>. Accessed January 31, 2012.

⁹ U.S. Dept. of Education. “Family Educational Rights and Privacy Act (FERPA)” website. Available at <http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>. Accessed January 31, 2012.

¹⁰ 34 CFR Part 99.

¹¹ U.S. Dept. of Education and U.S. Dept. of Health and Human Services. “Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records.” November 2008. Available at <http://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hipaa-guidance.pdf>. Accessed January 31, 2012.

¹² U.S. Dept. of Education. Notice of Proposed Rulemaking. “Family Educational Rights and Privacy.” 76 F.R. 19726 (April 8, 2011).

¹³ 45 C.F.R. §164.512(a)–(j).

¹⁴ 45 C.F.R. §164.512(b)(i)–(v).

¹⁵ Social Security Act. Pub. L. No. 104-321. Codified at 42 U.S.C. §1320b-5.

¹⁶ U.S. Dept. of Health and Human Services. “Public Health Emergency Declaration Q&As” webpage. Available at www.phe.gov/Preparedness/legal/Pages/phe-qa.aspx. Accessed January 31, 2012.

¹⁷ Center for Medicare and Medicaid Services. “Medicare Fee-For-Service Emergency and Disaster-Related Policies and Procedures That May Be Implemented Only With a § 1135 Waiver.” October 3, 2011. Available at www.cms.gov/Emergency/downloads/MedicareFFS-EmergencyQsAs1135Waiver.pdf. Accessed January 31, 2012.

¹⁸ 45 C.F.R. §160.203, §160.204.

¹⁹ 34 C.F.R. §99.31.

²⁰ 34 C.F.R. §99.33.

²¹ No Child Left Behind Act of 2001. (Pub. L. 107-110). See 20 U.S.C. §7165(b).

²² 34 C.F.R. §99.34.

²³ 34 C.F.R. §99.35.

²⁴ 34 C.F.R. §99.38.

²⁵ 34 C.F.R. §99.36.

²⁶ 34 C.F.R. §99.30.

²⁷ U.S. Dept. of Education. “Family Educational Rights and Privacy Act (FERPA) and the Disclosure of Student Information Related to Emergencies and Disasters.” June 2010. Available at <http://www2.ed.gov/policy/gen/guid/fpco/pdf/ferpa-disaster-guidance.pdf>. Accessed January 31, 2012.

²⁸ 34 C.F.R. §99.32.

²⁹ U.S. Dept. of Education. Final Rulemaking. “Family Educational Rights and Privacy.” 76 F.R. 75604 (December 2, 2011).

³⁰ U.S. Dept. of Education. “Memorandum from William D. Hansen, Deputy Secretary of Education, to State Officials.” January 30, 2003. Available at <http://www2.ed.gov/policy/gen/guid/fpco/pdf/ht031103.pdf>. Accessed January 31, 2012.

³¹ 34 C.F.R. §99.61.

³² U.S. Dept. of Education. Family Policy Compliance Office. “Letter of Technical Assistance to the Regents of the University of California.” September 17, 1999. Available at http://www2.ed.gov/policy/gen/guid/fpco/ferpa/library/oakland_ca.html. Accessed January 31, 2012.

- ³³ U.S. Dept. of Education. Family Policy Compliance Office. "Letter to Grossmont-Cuyamaca Community College District (CA) re: Potential Conflict with State Law." January 16, 2004. Available at <http://www2.ed.gov/policy/gen/guid/fpco/ferpa/library/suarezconflict.html>. Accessed January 31, 2012.
- ³⁴ U.S. Dept. of Education. Family Policy Compliance Office. "Letter to University of New Mexico re: Applicability of FERPA to Health and Other State Reporting Requirements." November 29, 2004. Available at <http://www2.ed.gov/policy/gen/guid/fpco/ferpa/library/baiseunmslc.html>. Accessed January 31, 2012.
- ³⁵ U.S. Dept. of Health and Human Services. Office for Civil Rights. "Frequently Asked Questions" webpage. Available at http://www.hhs.gov/ocr/privacy/hipaa/faq/disclosures_for_law_enforcement_purposes/397.html. Accessed January 31, 2012.
- ³⁶ U.S. Dept. of Health and Human Services. National Institutes of Health. "How Can Covered Entities Use and Disclose Protected Health Information for Research and Comply with the Privacy Rule?" website. Available at http://privacyruleandresearch.nih.gov/pr_08.asp. Accessed January 31, 2012.

This document was compiled from June-December 2011 and reflects the laws and programs current then. It reflects only portions of the laws relevant to public health emergencies and is not intended to be exhaustive of all relevant legal authority. This resource is for informational purposes only and is not intended as a substitute for professional legal or other advice. The document was funded by CDC Award No. 1U38HM000454 to the Association of State and Territorial Health Officials; Subcontractor PI Elliott, Logan Circle Policy Group LLC.