Summary of Laws Related to Child and Adolescent Mental Health

July 2020
Table of Contents
Acknowledgements.......................................................................................................................... ii
Executive Summary.......................................................................................................................... 1
Scenarios .......................................................................................................................................... 3
Health Information Portability and Accountability Act (HIPAA) Privacy................................................. 7
Family Educational Rights and Privacy Act (FERPA)............................................................................. 13
Confidentiality of Substance Use Disorder Records ........................................................................... 18
Individuals with Disabilities Act (IDEA), Part B.................................................................................. 22
Protection of Pupil Rights Amendment ............................................................................................... 26
Federal Policy for the Protection of Human Subjects (Common Rule).................................................... 31
Acknowledgements

This summary report was supported by Cooperative Agreement number 6-NU38OT000316, funded by the Centers for Disease Control and Prevention. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of the Centers for Disease Control and Prevention or the Department of Health and Human Services.

The Public Health Informatics Institute (PHII) also extends its sincere gratitude to Denise Chrysler, JD of the Network for Public Health Law for her thoughtfulness, expertise and diligence in developing the summaries that are included in this report.
Executive Summary

Among the more interesting aspects of the U.S. federal government system is the interaction of national and state laws. Specifically, how individual privacy protections relate to collecting, using and sharing personal health information. Child and adolescent mental health information is particularly sensitive and subject to complex interactions of national and state legal requirements and constraints.

CDC/NCCDDD and the Public Health Informatics Institute (PHII) developed the following summary for the Leveraging Informatics Approaches to Increase STLT System Capacity to Measure Child and Adolescent Mental Health cooperative agreement. The report includes summaries of the following laws relevant to child and adolescent mental health information:

- The Health Insurance Portability and Accountability Act (1996)
- Confidentiality of Substance Use Disorder Records (42 U.S.C. §290dd-2)
- Common Rule (1991)

The summaries provide information about the intent of these national laws, as well as how they can be superseded by state laws that provide a higher level of privacy protection. They include references on how states allow minors to consent for treatment and data sharing (typically addressed separately).

Below are key points related to the summaries included in this report:

1. **A complex legal landscape governs data collection and sharing, especially with regard to sensitive health information related to adolescents and children.** Data sharing is governed by federal, state and local laws. The first step in collecting or sharing data is to identify applicable laws, which depend on the data type and source and how it will be used. Generally, when the federal government funds a program, federal confidentiality laws or policies apply to data collected as part of the program (e.g., WIC, SNAP, School Lunch Program, Homeless Management Information Systems funded under the Homeless Emergency Assistance and Rapid Transition to Housing Act, and programs funded under the Violence Against Women Act). These laws apply to both grantees and sub-grantees. Multiple laws may apply to each type or source of data, and these laws differ in permissible and prohibited disclosures and data sharing conditions and limitations. In addition to laws that protect data from disclosure, there might also be laws that regulate collection of data. Our summaries include two laws related to data collection: the Protection of Pupil Rights Amendment and the Common Rule.

2. **Law is a real and perceived barrier to collecting and sharing data but not a complete barrier, especially to collecting and sharing meaningful disaggregated data.** Law is often cited as a
significant barrier to data collection and use because of the effort it takes to analyze various laws that apply to data. Stakeholders sometimes indicate that they can’t share data because of HIPAA; however, this is often untrue. For example, HIPAA permits disclosure of identifiable information to a public health agency for public health purposes, including for public health surveillance, investigation and intervention. While it is true that law does place limits on data sharing, these limits are not complete barriers. All laws that were reviewed for this project allow de-identified data to be disclosed. Generally, laws only cover data that are personally identifiable, which means that de-identified data can be disclosed for any purpose. De-identified aggregated data might work well to identify trends and develop policies.

3. **It is possible to navigate law to facilitate data sharing.** To navigate legal issues that govern data collection, use and disclosure, one should start by providing or collecting factual information from the agency that wants to obtain or share data: What is your goal? What do you want to accomplish? What data do you need to do this? The pathway to collecting and disclosing data requires creativity to structure relationships and describe projects or studies in ways that satisfy legal criteria.

4. **When law is not clear on data collection and/or sharing, it is important to define, weigh and communicate the potential risks and benefits.** While there are risks in sharing data, there are also risks in not sharing data (e.g., failure to promote health of children and adolescents because of lack of data to inform policies and programs and measure their effectiveness). It is often part of attorneys’ jobs to protect their clients from exposure to liability, which may lead to compliance programs, policies and organizational cultures that unnecessarily restrict access to data. Agencies and organizations from many sectors, and their attorneys, need to understand the crucial role that data play in promoting the health for children and adolescents so that they are willing to invest the effort to find a legal pathway to share data.
Scenarios

Because more than one law may apply to any given mental health information collection or sharing scenario, the following table is included to illustrate which laws might apply to specific situations. It highlights the complexities in protecting vulnerable populations’ private information while improving understanding of child and adolescent mental health and well-being as public health concerns that require complete surveillance information.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Applicable Laws</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Aggregated and de-identified data are collected on a 15-year-old</td>
<td>- Protection of Pupil Rights Amendment (PPRA) (federal law)</td>
</tr>
<tr>
<td>via the Youth Risk Behavior Survey (YRBS) completed by students in</td>
<td>- States may have laws that govern the collection of information from students; any such laws will need</td>
</tr>
<tr>
<td>the classroom during school</td>
<td>to be identified for the relevant state.</td>
</tr>
<tr>
<td>B. Individual-level data are collected on a middle school student</td>
<td>- Protection of Pupil Rights Amendment (PPRA) (federal law)</td>
</tr>
<tr>
<td>via the Strengths and Difficulties Questionnaire (SDQ) completed by</td>
<td>- Family Educational Rights Privacy Act (FERPA) (federal law)</td>
</tr>
<tr>
<td>school staff (e.g., counselor, teacher)</td>
<td>- States may have laws that govern education records and/or collection of information from students; any such laws will need to be identified for the relevant state.</td>
</tr>
<tr>
<td>C. Individual-level data are collected on a ten-year-old in a health</td>
<td>- Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (federal law)</td>
</tr>
<tr>
<td>care setting via a health assessment completed by the patient and/or</td>
<td>- States may have laws that govern health information; any such laws will need to be identified for the relevant state.</td>
</tr>
<tr>
<td>parent</td>
<td></td>
</tr>
<tr>
<td>D. Individual-level data are provided by a 16-year-old who is part of</td>
<td>- Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (federal law)</td>
</tr>
<tr>
<td>a screening/intake process in a substance abuse treatment program</td>
<td>- Federal Alcohol/Drug Confidentiality Regulations, 42 CFR Part 2 (federal law)</td>
</tr>
<tr>
<td>Scenario</td>
<td>Applicable Laws</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>E. Individual-level data are collected by school staff on an eight-year-old who is covered by the Individuals with Disabilities Education Act (IDEA) or 504 education plans</td>
<td>- States may have laws that govern health and/or substance use disorder information; any such laws will need to be identified for the relevant state.</td>
</tr>
</tbody>
</table>
| F. Individual-level data are collected on an elementary-school student via a universal mental health screening tool administered as part of a school wellness initiative (i.e., Georgia’s Project AWARE) | - Protection of Pupil Rights Amendment (PPRA) (federal law)  
- Family Educational Rights Privacy Act (FERPA) (federal law)  
- States may have laws that govern education records and/or collection of information from students; any such laws will need to be identified for the relevant state. |
| G. Individual-level data are provided by a 17-year-old to a school nurse during a visit to an on-site school health clinic | - Family Educational Rights Privacy Act (FERPA) (federal law)  
- States may have laws that govern education records or health information; any such laws will need to be identified for the relevant state. |
| H. Individual-level data related to suicidal behaviors by a 15-year-old are gathered by an emergency room physician and documented in an electronic health record | - Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (federal law)  
- States may have laws that govern health information; any such laws will need to be identified for the relevant state. |
| I. Individual-level data are collected via a behavioral health screening survey administered by a school counselor during a small group session with high school students | - Protection of Pupil Rights Amendment (PPRA) (federal law)  
- Family Educational Rights Privacy Act (FERPA) (federal law)  
- States may have laws that govern education records and/or collection of information from students; any such laws will need to be identified for the relevant state. |
<table>
<thead>
<tr>
<th>Scenario</th>
<th>Applicable Laws</th>
</tr>
</thead>
<tbody>
<tr>
<td>J. Individual-level data are collected by a juvenile justice service</td>
<td>- States may have laws that govern juvenile justice records; any such laws will need to be identified for the relevant state.</td>
</tr>
<tr>
<td>provider as part of an assessment conducted with a 17-year-old</td>
<td>- A child welfare program may receive funding from federal programs that require compliance with privacy requirements as a condition of funding.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>K. Individual-level data are collected on an 11-year-old by a child</td>
<td>- The Federal Child Abuse Prevention, Adoption and Family Services Act (CAPTA) requires that states that receive CAPTA funding provide methods to preserve the confidentiality of all records in order to protect the rights of the child and the child's parents or guardians.</td>
</tr>
<tr>
<td>welfare service provider</td>
<td>- A child welfare program may receive funding from additional federal programs that require compliance with privacy requirements as a condition of funding.</td>
</tr>
<tr>
<td></td>
<td>- States may have laws that govern collection or confidentially of individual level data that are collected by a child welfare service provider; any such laws will need to be identified for the relevant state.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>L. Individual-level data are collected on a 13-year-old as part of a</td>
<td>- The YMCA may implement programs that receive federal, state or local funds that require recipients to adopt or comply with provisions about privacy or data collection.</td>
</tr>
<tr>
<td>survey completed during a YMCA event</td>
<td>- The YMCA may adopt privacy policies whether or not required to by law; if so, compliance by companies, including nonprofits, with their own privacy policies are subject to the Federal Trade Commission Act.</td>
</tr>
<tr>
<td></td>
<td>- States may have consumer protection or other laws that govern collection of information from individuals and/or minors; any such laws will need to be identified for the relevant state.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Scenarios of Laws Related to Child and Adolescent Mental Health

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Applicable Laws</th>
</tr>
</thead>
</table>
| M. Individual-level self-reported data are collected on a ten-year old via a behavioral health assessment conducted by the Georgia Department of Public Health as part of its Adolescent Health and Youth Development program | - State law provides for confidentiality of individual-level data collected by the state health department.  
- If the state health department receives federal funds for its Adolescent Health and Youth Development program, funding requirements may include protection of individuals’ privacy. |

* This document is provided for informational and educational purposes only. It does not constitute legal advice. For legal advice, please consult specific legal counsel. While this document covers key laws, it may not be exhaustive. In particular, these scenarios may involve programs that receive federal funding from multiple sources. For each source of funding, federal statutes, regulations, and funding agreements often establish requirements regarding the confidentiality of information about the individuals who are served and may establish permitted uses and disclosures.
Health Information Portability and Accountability Act (HIPAA) Privacy

<table>
<thead>
<tr>
<th>Type of data</th>
<th>Health information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source of data</td>
<td>Health care providers and health plans</td>
</tr>
<tr>
<td>Citation</td>
<td>Federal statute, the Health Information Portability and Accountability Act (HIPAA), 42 U.S. Code Part C—Administrative Simplification, 42 U.S. Code § 1320d et seq., implemented by Federal Regulations, 45 CFR Parts 160 and 164</td>
</tr>
</tbody>
</table>

**Brief description:** The HIPAA Privacy Rule sets national standards for health information privacy and security and provides individuals with certain rights regarding this information. HIPAA prohibits covered entities from using or disclosing protected health information (PHI) unless authorized by the individual or required or permitted by the privacy rule.

**To whom does this law apply?** HIPAA applies to covered entities and their business associates that use or disclose PHI. Covered entities as defined in the act are:

- Health plans such as Medicare, Medicaid, private health plans and HMOs.
- Most health care providers, including hospitals, health clinics, physicians, nurses, therapists, laboratories, pharmacies and nursing homes. Generally, health care providers are covered by HIPAA if they communicate electronically with health plans to obtain payment for services.
- Health care clearinghouses; generally, these are businesses that format and transmit billing information for payment.

A business associate is a person or organization that is not a part of the covered entity's workforce and has access to PHI in order to provide a service to a covered entity. Business associates must enter into a legally binding business associate agreement (BAA) with the covered entity.

**What records or information are covered?** HIPAA applies to the use and disclosure of PHI (see also below). “Use” is the utilization or sharing of PHI within the entity that maintains the PHI, whereas disclosure is the release, transfer or provision of access to PHI outside the entity holding the PHI.

HIPAA does not cover education records that are covered by FERPA. This means, for example, FERPA (but not HIPAA) applies to a school nurse or a health clinic that is operated by a school district. Conversely, HIPAA (but not FERPA) applies to a health clinic on school premises if it is operated by a public health agency or health care provider independent of the school district.

**What does this law require or prohibit?** Covered entities are prohibited from using or disclosing PHI without patient consent unless required or allowed by the HIPAA privacy rule. For example, a covered entity is required to provide PHI in response to an investigation by the agency that enforces HIPAA or to the patient at their request. “Allowed” refers to the many exceptions in HIPAA that permit disclosure of fully identifiable or partially identifiable data, without authorization, depending on the purpose of the use and disclosure. Generally, a covered entity must limit uses and disclosures of PHI to the minimum amount necessary to accomplish the intended purpose. The minimum necessary requirement does not apply to disclosures for treatment purposes or to mandatory reporting laws.

**What is protected health information?** PHI is information related to past, present or future physical or mental health status, provision of health care, or payment for provision of health care that identifies an
individual. Which it includes written, electronic, oral and demographic information. Generally, HIPAA is concerned with record-level data. However, while aggregate data may not directly identify an individual due to a combination of data elements, small cell size, or other data reasonably available, the risk of re-identification must also be considered with regard to aggregate data. For this reason, PHI includes both record-level and aggregate data “for which there is a reasonable basis” to believe that it can be used to identify the individual.

A limited data set (LDS) is PHI that excludes direct identifiers concerning the individual and his or her relatives, employers or household members. An LDS may include town, city, state, and zip code information. It can also include dates such as birthdate and health care encounter dates (e.g., dates of service, admission, and discharge). A covered entity may use and disclose an LDS for research, public health and health care operations purposes provided that the covered entity and LDS recipient enter into a data use agreement that includes specific assurances and data safeguards.

**Does HIPAA provide standards to render PHI de-identified?** Yes. Health information is considered de-identified if it meets either the “safe harbor” standard or the “expert determination” standard. While the risk of re-identification does not have to be “zero” (most likely impossible), these standards are to ensure that the risk that information will identify an individual is sufficiently small.

The **safe harbor de-identification standard** requires removal of eighteen identifiers of the individual or the individual’s relatives, employers, or household members. These include personal identifiers (e.g., name, address, and social security number), indirect identifiers such as most geographic information smaller than a state (e.g., zip code, county, census track) and dates other than a year (e.g., birthdate and health care encounter dates such as date of service, admission, and discharge). If these identifiers are removed, the data are deemed de-identified provided that the covered entity does not have actual knowledge that the remaining information can be used alone or in combination with other reasonably available information to identify a subject.

The **expert determination standard** requires a formal determination and documentation by a qualified expert using accepted analytic techniques to conclude that the risk of re-identification is substantially limited. This expert must have appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable. The safe harbor standard, rather than the expert determination standards, is often favored for de-identification because it does not require access to a qualified expert. However, with the required removal of geographic information and dates associated with an individual, safe harbor may render data that are less useful than the expert determination standard.

HIPAA permits a covered entity to assign to and retain with the de-identified health information, a code or other means of record re-identification if that code is not based on information about the individual and cannot be used to identify the individual. The covered entity cannot use the code for any other purpose and must safeguard its key for re-identification.

**What does consent require?** In HIPAA, a patient’s permission to disclose their PHI is called an authorization. The authorization must

- be in writing, either in paper or electronic form, in plain language, signed and dated
- describe information to be disclosed in a “specific and meaningful” way
- describe each purpose of disclosure, although “at the request of the individual” is sufficient
include the name or other specific identification of the person(s) or classes of persons to whom disclosure is to be made

inform the individual about the covered entity’s ability or inability to condition treatment, payment, or enrollment, or eligibility for benefits on providing authorization

inform the individual that information may be re-disclosed by the recipient and no longer protected

provide for expiration on a certain date, after a specific amount of time, or upon occurrence of an event, and

inform the patient of their right to revoke the authorization.

Are disclosures allowed if they are based on verbal permission? Yes. HIPAA allows disclosure of PHI in some circumstances if the individual is provided with an opportunity to agree or object (which may be verbal) to the disclosure. These circumstances include:

Proof of immunization. HIPAA permits disclosure of proof of immunization to a school about an individual who is a student or prospective student if law requires proof of immunization for attendance.

Family and friends. HIPAA permits disclosure of PHI to family, friends and others involved in the patient’s care on a need-to-know basis regarding care or payment for care. Where a patient is not present or is incapacitated, a health care provider may share the patient’s information with family, friends or others involved in the patient’s care or payment for care. However, the provider must determine that doing so is in the best interest of the patient.

Disaster relief. HIPAA permits disclosure of PHI to authorized disaster relief organizations (e.g., the American Red Cross) to notify the patient’s family, personal representative or individuals involved in the patient’s care of the patient’s location, general condition or death. The patient’s permission is not required to share the information if doing so would interfere with the disaster relief organization’s ability to respond to the emergency circumstances.

Are minors able to authorize disclosure of their own PHI? If a minor is able to consent on their own to health care under applicable state law, with limited exceptions, the minor may authorize disclosure of their own PHI.

When does HIPAA permit disclosure without authorization? Common HIPAA exceptions to share data without the patient’s authorization include:

De-Identified records and information. HIPAA does not apply to information that satisfies HIPAA’s de-identification standards. (See description above regarding de-identification standards.)

Business associate. HIPAA permits disclosure of PHI to an individual or entity that has access to PHI in order to provide a service to a covered entity, pursuant to a business associate agreement. Examples include billing services; document destruction services; outside attorneys and accountants; computer service technicians; software vendors; and cloud computing vendors. A business associate might also provide data-related services such as analysis, aggregation, creation of a limited data set and de-identification. In particular, HIPAA allows an entity to serve as a business associate for several covered entities, receive and aggregate data
from these entities, and then provide certain data back to each of the participating entities for health care operations without the patient’s authorization.

- **Treatment.** HIPAA permits disclosure of PHI among health care providers to treat the subject patient or a different patient. Treatment includes the coordination or management of health care and related services, consultation between providers, and the referral of patients for treatment. Psychotherapy notes are treated differently from other health information, requiring patient authorization for disclosure for any purpose with limited exceptions. Disclosure of PHI to government or community agencies that provide human or social support services, such as supportive housing, food and heating assistance, and other public benefits, might be permitted without an authorization if the treatment provider believes that disclosure is needed to support the individual’s health care and limits the disclosure to the minimum necessary. Otherwise, an authorization is required. The authorization may describe the data recipients broadly, for example, “to social services providers,” for purposes of “supportive housing, food and heating assistance, and public benefits.”

- **Payment.** HIPAA permits disclosure of PHI to another covered entity or a health care provider for the payment activities of the receiving entity.

- **Health care operations.** HIPAA permits covered entities that each have a relationship with the patient to disclose PHI for health care operations activities of the receiving entity. Health care operations are activities that are necessary for a covered entity to run its business. Examples are quality assurance and improvement, outcomes evaluation and development of clinical guidelines, case management and care coordination, and population-based activities relating to improving health or reducing health care costs.

- **Required by law.** HIPAA permits a covered entity to use or disclose PHI to the extent required by law, and the use or disclosure complies with and is limited to such law. For example, HIPAA permits covered entities to comply with mandatory reporting laws, such as required reporting to communicable disease surveillance systems, to prescription drug monitoring programs, and to child protective services for suspected child abuse or neglect.

- **Public health purposes.** HIPAA permits a covered entity to use or disclose PHI to a public health authority, including the CDC or a state, tribal, local, and territorial health department, that is authorized by law to collect or receive information for the purpose of preventing or controlling disease, injury or disability, including for public health surveillance, public health investigations, and public health interventions. For example, a covered entity may report vaccinations to an immunization information system, even when reporting is not mandated if state law permits public health to collect this information. A covered entity may also share PHI with a community-based or other organization that is a contractor or agent of a public health authority and is carrying out public health activities on the authority’s behalf. Finally, as discussed above, a covered entity may use and disclose a limited data set for public health purposes provided that the covered entity and LDS recipient enter into a data use agreement that includes specific assurances and data safeguards. Disclosure of an LDS for public health purposes, can be to entities that are not public health authorities.

- **Risk of contracting or spreading disease.** HIPAA permits PHI to be shared with persons at risk of contracting or spreading a disease or condition if other law, such as state law, authorizes the covered entity to notify such persons as necessary to prevent or control spread of the disease or otherwise to carry out public health interventions or investigations.
● **Suspected child abuse and neglect.** HIPAA permits disclosure of PHI, for example, from a clinical record, to an appropriate government authority authorized by law to receive reports of child abuse or neglect.

● **Victims of abuse, neglect or domestic violence.** HIPAA permits disclosure of PHI about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive these reports. Generally, the individual’s agreement is required. No agreement is needed to comply with a reporting mandate or if the covered entity believes the disclosure is necessary to prevent serious harm to the individual or other potential victims.

● **Avert a serious threat to health or safety.** HIPAA permits disclosure of PHI if necessary to avert a serious threat to health or safety of the person or to the public. The disclosure must be someone that the covered entity believes can prevent or lessen the threat and may include the target of the threat.

● **Research.** HIPAA permits PHI to be used or disclosed for research if an Institutional Review Board (IRB) or privacy board approves a waiver of authorization and documents that the research project satisfies certain criteria that justifies the waiver. As discussed above, a covered entity may use and disclose a limited data set for purposes of research, without the approval of an IRB or privacy board, provided that the covered entity and LDS recipient enter into a data use agreement that includes specific assurances and data safeguards. Additionally, a researcher may be allowed to review PHI, without approval of an IRB or privacy board, to prepare a research protocol or similar purposes preparatory to research subject to conditions to safeguard the information. A researcher may also be allowed to conduct research, without an IRB or privacy board approval, using the PHI of decedents if the PHI being sought is necessary for the research.

**What is the potential impact of the HIPAA Privacy Rule on individuals and families, schools and school districts, neighborhoods and communities, health care and health plans, and state and federal agencies?**

The HIPAA Privacy Rule protects the privacy of patients’ health information while ensuring that appropriate uses and disclosures of the information can be made when necessary to treat a patient, to protect the nation’s public health, and for other critical purposes. That said, individuals and families might be uneasy with the type or number of uses and disclosures of PHI that HIPAA permits without their authorization. In this regard, HIPAA permits disclosure for purposes that would not be permitted for education records covered by FERPA or substance use disorder records covered by 42 CFR 2, such as for treatment and public health activities.

Additionally, unlike FERPA and 42 CFR Part 2, HIPAA does not include prohibitions on re-disclosure of PHI. Thus, HIPAA’s restrictions would not apply to a recipient of PHI, unless the recipient is a covered entity or a business associate of a covered entity. Further, with the exception of psychotherapy notes, HIPAA treats all health information the same. Consequently, patients would not be entitled to additional protections for information related to mental health, substance use, reproductive health, and other sensitive areas. In particular, information that identifies a patient as having or having had a mental health or substance use disorder may adversely affect reputation, housing, employment, or be used in civil or criminal proceedings. HIPAA does permit patients to request restrictions on most permitted uses and disclosures and entitles patients to an accounting of most disclosures of their PHI.
HIPAA provides for disclosure of PHI for purposes of treatment, facilitating referral, consultation, case management and care coordination among health care providers. HIPAA also supports disclosure of necessary information to health plans for purposes of payment. Covered entities can share limited data sets with one another for health care operations, providing opportunities to improve health care systems and services generally, and with regard to specific populations.

HIPAA also allows covered entities to share PHI, without authorization, with public health agencies. These disclosures enable public health to access information necessary to prevent or control disease, injury, or disability, and supports public health surveillance, investigations, and interventions. Disclosures to governmental agencies, which do not carry out public health functions, and to community-based agencies, would be more restricted. Nevertheless, relationships might be structured to facilitate data sharing, support collaborative projects to improve the health of communities and address social, economic, and environmental factors that affect health.

HIPAA would allow disclosure of PHI, without authorization, to schools for some purposes such as disclosure by a health care provider to a school nurse for treatment purposes. However, generally, a school would need a prior written consent to share information back for treatment, absent a health or safety emergency. HIPAA would permit disclosure of a limited data set to a school or school district for research purposes. A covered entity and school might be able to structure their relationship to share information consistent with both HIPAA and FERPA, for example, to conduct a study in order to improve students’ attendance and performance.

While covered entities could release de-identified information to neighborhoods and communities, strict de-identification standards would make it difficult to provide community- or neighborhood-level data, or include dates and other information needed to assess and improve a community or address the needs of a particular population. Potentially, a limited data set could be disclosed to neighborhood and community organizations for activities that promote the public’s health. Furthermore, as discussed above, a public health agency might work collaboratively with neighborhood and community organizations, with relationships structured to facilitate data sharing and support collaborative projects to improve the health of communities.

**Resources:** For further information on HIPAA Privacy Rule, visit the webpage of the Office for Civil Rights at [https://www.hhs.gov/hipaa/index.html](https://www.hhs.gov/hipaa/index.html).

This summary is provided for informational and educational purposes only. It does not constitute legal advice. For legal advice, please consult specific legal counsel.
Family Educational Rights and Privacy Act (FERPA)

<table>
<thead>
<tr>
<th>Type of Data</th>
<th>Education records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source of Data</td>
<td>Educational agencies and institutions</td>
</tr>
<tr>
<td>Citation</td>
<td>Federal statute, 20 U.S.C. §1232g; Federal regulations, 34 CFR Part 99</td>
</tr>
</tbody>
</table>

Brief description: FERPA grants parents and eligible students the right to inspect, obtain, seek amendment of, and have some control over disclosure of education records and information in education records. It also requires an educational agency or institution to provide annual notice of its policies related to these rights. FERPA prohibits disclosure of personally identifying information from education records, without consent, unless permitted by FERPA. FERPA does not limit what public health, health care providers, or other sectors can disclose to educational agencies and institutions, although other laws might apply.

To whom does this law apply? FERPA applies to educational agencies or institutions that receive funds from the U.S. Department of Education, or by a party acting for the agency or institution. Examples include early childhood education such as Head Start, public elementary and secondary schools, colleges and universities, special education, job training, career and technical education, and adult education programs.

What records are covered? FERPA covers “education records.” These are records that are directly related to a student and maintained by an educational agency or institution or a party acting for the agency or institution such as a contractor. Education records include transcripts, attendance records, disciplinary records, special education assessments, and medical or health-related records. FERPA does not apply to treatment records of a student 18 or older or who is attending an institution of post-secondary education, but only when used in connection with treatment. Records of a law enforcement unit of an educational agency or institution that are created and maintained by the unit exclusively for law enforcement purposes are not covered by FERPA. As discussed below, if an outside party provides health or other services directly to students and is not acting on behalf of the educational agency or institution, FERPA does not apply to the records of the outside party.

When does FERPA apply to records concerning health-related services that are provided to students? Health-related services are frequently delivered to students while they are at school. Medication administration, hearing and vision screening, dental care and fluoride treatment, immunizations, asthma management, and mental health or behavioral health services are examples. These services support students’ success, ensuring that they are in school and able to learn. They also promote important public health objectives by preventing the spread of vaccine-preventable diseases and improving health outcomes.

Whether FERPA applies to records concerning health-related services depends on the relationship of the service provider to the educational agency or institution. For example, FERPA applies to medication records and notes created by a school nurse, whether the nurse is directly employed by the school district or works under a contract with the school district. Similarly, if a school district contracts with a public health or mental health agency to provide services to its students, FERPA applies. However, FERPA would not apply to the health records of school-based clinics operated by a health department, health system, or community mental health agency, as long as the provider is separate from, and not
acting on behalf of the school. Other laws, however, might apply to the provider that renders the service.

If the outside provider discloses information to the educational institution or agency – either with consent or as permitted by applicable law – information that the school receives is part of the education record, and thus, subject to FERPA. Parents maintain FERPA rights to access their child’s education record, even when their child is emancipated or is able to obtain health care services without parental permission or knowledge such as STD, mental health, or substance use disorder diagnosis or treatment. For this reason, health care professionals should carefully consider disclosure of sensitive information to the school and should clarify what, if any, health information would be held by the school should school staff support public health or others in rendering services.

What does FERPA require or prohibit? An educational agency or institution shall not disclose personally identifying information (PII) from an education record, absent prior written consent from the parent or eligible student, unless FERPA provides an exception to the general consent requirement. A third party that receives FERPA-protected information, such as a local health department under contract to provide school health services, may only re-disclose such information consistent with FERPA.

What is Personally Identifying Information? PII is information that, alone or in combination, would make the student’s identity easily traceable. It includes, but is not limited to:

- Names and addresses of the student or family members;
- Personal identifiers such as social security numbers, student numbers or biometric records;
- Indirect identifiers such as date of birth, place of birth and mother’s maiden name;
- Personal characteristics that would make a student’s identity easily traceable;
- Information requested by a person who the agency or institution reasonably believes knows the identity of the student to whom the education record relates.

FERPA does not specifically list partial addresses (such as city or county) or methods for communicating with students or their families (such as phone numbers or email addresses) as identifiers. Most likely, methods for communicating would be deemed “other information that, alone or in combination, would make a student’s identity easily traceable.” Whether geographic information is an identifier would also depend on whether the information, alone or in combination, would make the student’s identity easily traceable. Phone numbers, email addresses, and street addresses are “directory information;” as discussed below, directory information may be disclosed if parents have been provided with notice and have not opted out of disclosure.

Does FERPA provide standards to render PII de-identified? To de-identify information, the following identifiers, which are listed in FERPA, must be removed: the names and addresses of the student or family members; social security numbers, student numbers, or biometric records of the student; and indirect identifiers such as date of birth, place of birth and mother’s maiden name. Additionally, personal characteristics or other information must be removed that, alone or in combination, would make the student’s identity easily traceable. Before disclosing a student record, an educational agency or institution must determine if a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, identify the student with reasonable certainty. The risk of identification of individuals increases when releasing aggregate data on small subpopulations in a school or system or from the cumulative effect of multiple disclosures. The agency or institution might
reduce this risk by using statistical techniques to conceal identities, such as generalization, suppression, or perturbation. For example, date of birth might be generalized by using age or an age range, and information for small numbers of individuals with unique characteristics or a combination of characteristics might be suppressed.

What does consent require? Consent must be in writing, specify records that may be disclosed, state the purpose of disclosure, and identify the party or class of parties to whom disclosure may be made. Electronic consent is permitted.

Are minors able to consent to disclosure of their own PII? FERPA rights belong either to a student’s parent, guardian, or an individual acting as a parent or guardian or to an “eligible student.” An eligible student is a student who has turned 18 years of age or is attending an institution of post-secondary education at any age. Unlike many data privacy laws, FERPA does not specifically speak to the rights of emancipated minors.

When does FERPA permit disclosure without consent? Common FERPA exceptions to share data without consent include:

- **De-Identified records and information.** To be de-identified, the educational agency or institution must remove all PII and make a reasonable determination that a student is not personally identifiable, whether through single or multiple releases, and taking into account other reasonably available information. De-identified data might be used to identify trends or impact where individual students do not need to be identified.

- **Designated directory information.** Directory information would not generally be harmful or an invasion of privacy if disclosed. It includes the student’s name, address, email, telephone number, date of birth, grade, and similar information. The educational agency or institution must tell parents about its policy on disclosure of directory information and allow them a reasonable amount of time to opt out. This exception allows the school to provide class rosters and updated student contact information.

- **Personal knowledge.** School staff may disclose information that is based on personal observation, which is not recorded education record. For example, a teacher who witnesses a student bully another may tell the victim’s parent about the bullying.

- **Outsourcing school functions or services.** FERPA permits student information to be shared with “school officials” who have a “legitimate educational interest.” “School officials” includes other school employees such as teachers, school nurses and counselors. It might also include consultants, volunteers, contractors or other outside parties that provide a service for the school. “Legitimate educational interest” means that the data recipient needs to know the information to fulfill its professional responsibility. For example, an educational agency or institution may contract with a behavioral health specialist to provide services to its students with substance use disorders. The agency or institution must inform parents of its criteria for determining who constitutes a school official and what constitutes a legitimate educational interest.

- **Abuse and neglect.** The Federal Child Abuse Prevention, Adoption and Family Services Act (CAPTA) requires that states enact laws that require reporting of known and suspected instances of child abuse and neglect in order to receive grants for abuse prevention and treatment programs. CAPTA supersedes FERPA and would allow disclosure of information concerning child abuse and neglect be made to persons or entities determined by the state to have a need for the information.
Conducting a study. An educational agency or institution may disclose student information, pursuant to a written agreement, to public health agencies, mental health agencies and other organizations to evaluate and improve health education programs and health accommodations in schools. For example, a school may provide asthma, mental health or other information to a public health agency to evaluate and improve efforts regarding students’ attendance and performance. A school may be able to provide substance use disorder information for a study but would need to first ascertain whether 42 CFR Part 2 applies to the information. If so, the school would need to ensure compliance with its requirements. Key: The public health agency or other data recipient must be assisting the educational agency or institution with its educational mission; the data recipient must use and protect information pursuant to a written agreement and consistent with the purpose for which information is disclosed.

*Audit or evaluation.* State and local educational authorities, such as a state education department or a local school district, may access information from student records for the purpose of auditing or evaluating a federal- or state-supported educational program. The educational authority may enter into an agreement to designate a public health agency, community mental health or other organization to serve as its authorized representative. For example, a local school district might designate a community mental health agency as its authorized agent to evaluate how well the school district is meeting the mental and behavioral health needs of its students.

*Health or safety emergency.* An educational agency’s or institution’s disclosure of student information must be necessary to protect the health or safety of the student or others. Disclosure must be related to an actual, impending, or imminent emergency, limited to the period of the emergency, and made to parties that are able to respond to the emergency. The educational institution or agency must make a case-by-case determination, considering the totality of circumstances, based on “an articulable and significant threat.” If there is a rational basis for this determination, the U.S. Department of Education will not substitute its judgment for that of the agency or institution. A health or safety emergency might include disease outbreaks, urgent environmental threats, and threats of student violence or suicide. The agency or institution must record in the student’s education record the articulable and significant threat that formed the basis for the disclosure and the parties to whom the information was disclosed. This exception does not include routine non-emergency reporting, for example, to public health agencies, even when state law mandates such reporting.

What is the potential impact of FERPA on individuals and families, schools and school districts, neighborhoods and communities, healthcare and health plans, and state and federal agencies?

Education records may include information about a student and the student’s family, including information about the student’s abilities, academic achievement, behavior, and health conditions, that are personal and potentially stigmatizing. FERPA provides strong privacy protections of student information. For example, educational agencies and institutions must have administrative and technical controls in place to protect PII and must notify the parent of the types and locations of education records and how they are used and shared, and parental rights to amend, access, and restrict certain disclosures of information. Except for directory information, permitted disclosure of PII under FERPA without consent is very limited.

Unlike HIPAA, there is no provision that allows educational agencies or institutions to disclose PII to protect or promote public health absent consent. This thwarts public health reporting requirements and voluntary data sharing for public health surveillance, analysis, policy development, intervention and evaluation. Disclosure of PII is limited to the following situations: a) a health and safety emergency b)
when a public health agency assists an educational agency or institution in serving its students; or c) when a public health agency assists an educational agency or institution with an evaluation, audit or study. On the other hand, an educational agency or institution may be able to provide meaningful data that has demographic, geographical, temporal and socioeconomic details, unless these details would make it possible to identify the student with reasonable certainty.

Unlike HIPAA, absent consent, there is no provision that allows educational agencies or institutions to provide PII to health care providers for treatment except when needed to respond to a health emergency or the student is 18 years or older or in post-secondary school. While consent requirements may delay or limit data sharing, they also promote student, family and community trust.

**Resources:** For further information on FERPA, visit the webpage of the U.S. Department of Education at [https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html](https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html).

This summary is provided for informational and educational purposes only. It does not constitute legal advice. For legal advice, please consult specific legal counsel.
Confidentiality of Substance Use Disorder Records

<table>
<thead>
<tr>
<th>Type of Data</th>
<th>Substance use disorder records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source of Data</td>
<td>Substance use disorder programs</td>
</tr>
</tbody>
</table>

**Brief description:** 42 CFR Part 2 (Part 2) protects the confidentiality of information about a person receiving diagnosis, treatment or referral for treatment for an alcohol or drug problem (known as a substance use disorder or SUD) at a federally-assisted SUD program. Part 2 prohibits disclosure of information that identifies an individual as a patient with an SUD without the patient’s written consent unless permitted by Part 2. The federal Substance Abuse and Mental Health Services Administration (SAMHSA) oversees Part 2 implementation.

**To whom does this law apply?** Part 2 applies to any federally-assisted substance use disorder program (“Part 2 program”). Examples are treatment or rehabilitation programs, employee assistance programs, programs within general hospitals, school-based programs, and private practitioners that hold themselves out as providing substance use disorder diagnosis, treatment, or referral for treatment. A general medical facility (such as an emergency department or community health center) is usually not a Part 2 program, although a general medical facility might include an identified unit or specific personnel that are an SUD program. In this situation, the general medical facility is not subject to 42 CFR Part 2, but the specific SUD program is. A general medical facility does not become a federally assisted SUD program by screening individuals for excessive alcohol or drug use and providing them with information and referral for early intervention and treatment.

**What records are covered?** Part 2 applies to any information, whether recorded or not, that is created by, received, or acquired by a Part 2 program. Examples include screening self-assessment results for risk or other indicators, diagnosis, treatment or referral for treatment information, billing information, emails, voicemails, and texts.

**What does this law require or prohibit?** A Part 2 program shall not disclose any information that would identify a patient as having or having had an SUD either directly, by reference to publicly available information, or through verification of such identification by another person. Part 2 requires the patient’s prior written consent to disclose patient identifying information unless Part 2 provides an exception to the general consent requirement. If disclosure is permitted, a Part 2 program must limit disclosure to information which is necessary to carry out the purpose of the disclosure. A third party that receives Part 2-protected information may only re-disclose such information consistent with Part 2.

Part 2 is far more restrictive than disclosures that are permitted under the HIPAA Privacy Rule. Unlike HIPAA, generally, Part 2 requires prior written consent to disclose information that identifies a patient as having or having had an SUD for purposes of treatment, payment, health care operations and public health activities and to comply with state reporting laws such as reporting to state prescription drug monitoring programs.
**What is Patient Identifying Information?** Patient identifying information (PII) means the name, address, social security number, fingerprints, photograph, or similar information (see below) by which the identity of a patient can be determined with reasonable accuracy either directly or by reference to other information. PII does not include a number assigned to a patient by a Part 2 program for internal use only, if that number does not consist of, or contain numbers (such as a social security, or driver’s license number), which could be used to identify a patient with reasonable accuracy from sources external to the program. *This means that a Part 2 program could provide coded information to a health department, school, or other collaborator for a study, and be able to use results internally to improve its operations or conduct longitudinal studies, for example, to evaluate health outcomes of policy or system changes for patient groups or individual patients.*

**Does Part 2 provide standards to render PII de-identified?** Yes. The patient’s name, address, social security number, fingerprints, and photograph must be removed. Additionally, *similar information*, by which the identity of a patient can be determined with reasonable accuracy either directly or by reference to other information, must be removed. Based on SAMHSA’s interpretation, “similar information” incorporates data elements that must be removed to meet the HIPAA Privacy Rule’s “safe harbor” test for de-identifying health information. This means that geographic information that identifies an individual by county, city, five-digit zip code, census track, and other subdivisions smaller than a state must be removed. Data may be identified by the first three-digits of a zip code if this geographic area has more than 20,000 residents. Additionally, dates (other than a year) that are directly associated with an individual must be removed, such as date of birth or death, date of service, admission date, and discharge date. The year of birth or age for children and individuals under age 90 may be retained; however, to identify patients who are over age 89 years in a dataset, they must be grouped as patients who are age 90 or older. Beginning March 27, 2021, the CARES Act, explicitly incorporates both HIPAA’s “safe harbor” test and HIPAA’s “expert determination test” for concluding that a dataset about patients with an SUD is not personally identifiable and requires that SUD information disclosed to a public health agency meet HIPAA’s de-identification criteria.

**What does consent require?** Consent must:

- be in writing, either in paper or electronic form, signed and dated,
- describe how much and what kind of information may be disclosed,
- describe each purpose of disclosure,
- identify to whom disclosure may be made and must include, with certain exceptions, the name of the individual; the name of the entity may be used for treating providers, third party payers, or organizations that facilitate health information exchange (HIE),
- provide for expiration on a certain date, upon occurrence of an event, or when the information is no longer necessary to serve the purpose of the consent, and
- inform the patient of their right to revoke the consent.

If information is disclosed to an HIE, the patient must consent to further disclosure to providers or other entities that participate in the HIE. The consent may identify the patient’s treating providers by a general designation, provided that the patient is informed of their right, upon request, to a list of specific recipients to which their information has been disclosed. Beginning March 27, 2021, under the CARES Act, a patient’s prior written consent may be given once for all such future uses or disclosures for purposes of treatment, payment, and health care operations, as permitted by the HIPAA Privacy Rule, until such time as the patient revokes such consent in writing.
**Are minors able to consent to disclosure of their own PII?** If a minor is able to consent on their own to substance use disorder treatment under applicable state law, with limited exceptions, consent to disclose PII must be given by the minor. If a parent or other legal representative must consent to treatment, with limited exceptions, consent to disclose PII must be given by *both* the minor and a legal representative.

**When does Part 2 permit disclosure without consent?** Common Part 2 exceptions to share data without consent include:

- **De-Identified records and information.** Part 2 permits disclosure of information that does not identify a patient as having or having had an SUD. (See description above regarding “patient identifying information.”)

- **Qualified Services Organizations (QSO).** Part 2 permits disclosure, pursuant to a Qualified Services Organization Agreement, of PII to an individual or entity that provides services to a Part 2 program. Examples include data processing, health information storage or exchange, medical staffing or other professional services, or services to prevent or treat child abuse or neglect, including training on nutrition and childcare and individual and group therapy. As another example, a Part 2 program may contract with a health care IT vendor or consultant to provide population health management services by analyzing patient data and providing recommendations to improve health outcomes through system change.

- **Medical emergencies.** Part 2 permits disclosure of PII to medical personnel to the extent necessary to meet a bona fide medical emergency in which the patient’s prior informed consent cannot be obtained.

- **Suspected child abuse and neglect.** Part 2 permits reporting under state law of incidents of suspected child abuse or neglect to the appropriate state or local authorities. However, Part 2’s restrictions continue to apply to the SUD record maintained by the Part 2 program; disclosure of the SUD record would require consent or a court order.

- **To avert a substantial risk of death or serious bodily injury.** Part 2 permits PII to be disclosed to avert a substantial risk of death or serious bodily injury if authorized by a court order based on a showing of good cause.

- **Research.** Part 2 permits disclosure of PII for the purpose of conducting scientific research if the data recipient is subject to the HIPAA Privacy Rule and/or the Department of Health and Human Services Federal Policy for the Protection of Human Subjects (Common Rule) and documents that its use of PII complies with HIPAA and the Common Rule, as applicable. Disclosure for scientific research may occur without the individual’s informed consent provided that the research project satisfies legal criteria for exemption, modification, or waiver of consent. For example, patient consent might not be required for disclosure of PII to a public health department or a school that is conducting a federally-funded research project that is exempt from IRB review under the Common Rule.

- **Notifications to law enforcement.** Part 2 permits law enforcement agencies to be notified if an immediate threat to the health or safety of an individual exists due to a crime on program premises or against program personnel. A Part 2 program is permitted to report the crime or attempted crime to a law enforcement agency or to seek its assistance.
What is the potential impact of Part 2 on individuals and families, schools and school districts, neighborhoods and communities, healthcare and health plans, and state and federal agencies?

By providing strong privacy protections, Part 2 reduces the risk that individuals receiving treatment for SUDs, and their families, will experience adverse consequences, for example, in relation to criminal or civil proceedings, family or custody matters, reputation, employment, or housing. By protecting individuals from adverse consequences of disclosure, individuals are more likely to seek treatment for a SUD. The law also reduces group stigma that may occur from identifying a specific community or population with a high incidence of individuals with alcohol or drug problems.

On the other hand, because of strict consent requirements, schools, school districts, health care and health plans may lack important information to best treat individuals with SUDs, coordinate care, and facilitate access to social support. Additionally, strict standards for de-identification reduces the value of aggregate data for community assessment or policy development. In this regard, aggregate data available to state, federal and local agencies, and community organizations may lack geographic, demographic, and temporal details—as well as social, economic, and environmental characteristics—needed for studies, analysis and effective, targeted interventions and evaluation.

Resources: For further information on 42 CFR Part 2, visit the webpage of the Substance Abuse and Mental Health Services Administration (SAMHSA) at https://www.samhsa.gov/about-us/who-we-are/laws-regulations/confidentiality-regulations-faqs.

This summary is provided for informational and educational purposes only. It does not constitute legal advice. For legal advice, please consult specific legal counsel.
Individuals with Disabilities Act (IDEA), Part B

<table>
<thead>
<tr>
<th>Type of Data</th>
<th>Education records related to children with disabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source of Data</td>
<td>State and local educational agencies</td>
</tr>
<tr>
<td>Citation</td>
<td>Federal statute, 20 U.S.C. §1400 et seq.; Federal regulations, 34 CFR Part 300</td>
</tr>
</tbody>
</table>

**Brief description:** The Individuals with Disabilities Act (IDEA) protects the rights of children with disabilities to a free, appropriate, public education that is tailored to meet their individual needs and prepares them for further education, employment and independent living. IDEA provides specific federal assistance to states to establish a comprehensive statewide system to provide special education and related services through local school districts and other public agencies. IDEA also requires school districts to make certain services and benefits available to children with disabilities enrolled by their parents in private schools. The term “child with a disability” means: (1) a child with intellectual disabilities, hearing impairments (including deafness), speech or language impairments, visual impairments (including blindness), serious emotional disturbance, orthopedic impairments, autism, traumatic brain injury, other health impairments, or specific learning disabilities; and (2) who, by reason thereof, needs special education and related services.

A state must have policies and procedures in effect that ensure that the state educational agency and participating agencies comply with regulatory requirements to protect the confidentiality of information related to the child. This summary covers data privacy and disclosure related to children and youth ages 3 through 21 who receive special education and related services under IDEA Part B (Part B). It does not cover data privacy and disclosure related to infants and toddlers, birth through age two, with disabilities and their families, who receive early intervention services under IDEA Part C.

**To whom does this law apply?** Part B applies to the state educational agency and “participating agencies,” which are defined as “any agency or institution that collects, maintains or uses personally identifiable information, or from which information is obtained, under Part B of the Act.” Participating agencies include agencies or institutions that provide preschool special education programs as well as those that provide special education programs for older children.

**What records or information are covered?** Part B covers information collected, used or maintained under Part B. Part B confidentiality requirements apply from the time a child is referred for special education and related services, and not before a referral. Related services are those services a disabled child needs in order to benefit from special education, such as speech therapy, occupational therapy, physical therapy, rehabilitation and nursing services, counseling, and transportation.

**What does this law require or prohibit?** A state must have policies and procedures in effect that ensure that the state educational agency and participating agencies comply with regulatory requirements to protect the confidentiality of any personally identifiable information collected, used or maintained under Part B. A state may establish policies and procedures that provide greater confidentiality protections than Part B requires.

Part B requires schools to provide the parents of a child with a disability with a notice that explains procedural safeguards available under IDEA, including safeguards related to the confidentiality of information about the child. IDEA grants parents the right to inspect, obtain, seek amendment of, and
have some control over disclosure of identifiable information to third parties. Generally, a participating agency shall not disclose “personally identifiable information” (PII) without consent to parties other than officials of participating agencies. If Part B PII is contained in education records, the participating agency must also comply with the confidentiality requirements in the Family Educational Rights and Privacy Act (FERPA) and may disclose this PII without parental consent if the disclosure is permitted under FERPA.

**What is Personally Identifying Information?** “Personally identifiable” means information that contains:

(a) The name of the child, the child's parent, or other family member;
(b) The address of the child;
(c) A personal identifier, such as the child's social security number or student number; or
(d) A list of personal characteristics or other information that would make it possible to identify the child with reasonable certainty.

**Does IDEA provide standards to render PII de-identified?** Yes. To be de-identified, the name of the child, the child's parent, or other family member must be removed. Additionally, the child’s address, personal identifiers, personal characteristics or other information that would make it possible to identify the child with reasonable certainty must be removed.

**What does consent require?** Consent to disclose PII must

- be in writing and signed; electronic or digital signatures are permitted for consent, provided the participating agency takes necessary steps to ensure that there are appropriate safeguards to protect the integrity of the process;
- provide relevant information in the parent’s native language or other mode of communication;
- list the activities and the records to be released and to whom;
- inform the parent that the granting of consent is voluntary on the part of the parent and may be revoked at any time; and
- explain that if the parent revokes consent, that revocation is not retroactive; additionally, if the parent revokes consent in writing for their child’s receipt of special education services, the public agency is not required to amend the child’s education records to remove any references to the child’s receipt of special education and related services because of the revocation of consent.

**Are minors able to consent to disclosure of their own PII?** Part B rights transfer from the parent to the child when the child reaches the age of majority, provided that the child has not been determined to be incompetent under state law. Thus, upon reaching the age of majority, the child can consent to disclosure of information protected by Part B. Like FERPA, IDEA does not mention the rights of emancipated minors. State educational agencies may recognize the rights of minors who are emancipated under state law in their policies and procedures to implement IDEA.

**When does Part B permit disclosure without consent?** Common exceptions to share data without consent include:

- *De-Identified records and information.* Part B permits disclosure of information that is not personally identifying. (See description above regarding “personally identifying information.”)
● **Officials of participating agencies.** Part B permits disclosure to officials of participating agencies with some exceptions. For example, if a child is enrolled or is going to enroll in a private school that is not in the local educational agency (LEA) of the parent’s residence, parental consent must be obtained before PII about the child is exchanged between officials in the LEA of the parent’s residence and the LEA where the private school is located.

● **Information in education records that may be disclosed without consent.** Part B permits disclosure of Part B information that is included in the student’s education record if FERPA permits disclosure without consent. For example, FERPA allows disclosure without consent to school officials, including contractors that provide a service to the school with a legitimate educational interest in the information; to other organizations for studies on behalf of the school, for example, to improve student performance; and as necessary to respond to a health or safety emergency.

● **Education records covered by the Uninterrupted Scholars Act (USA).** USA permits the disclosure of education records without consent to a caseworker or other representative of a state or local child welfare agency for the care and protection of the student. For example, USA would allow a Children’s Protective Services caseworker to obtain PII from the education record of a student in foster care placement. While this exception to consent has not been added to the FERPA or IDEA regulations, the U.S. Department of Education has issued guidance that educational agencies and institutions under FERPA, and participating agencies under IDEA, may disclose education records under this exception.

**What is the potential impact of Part B on individuals and families, schools and school districts, neighborhoods and communities, health care and health plans, and state and federal agencies?**

Part B records concern referral and receipt of special education and related services. Thus, they may include information about the child’s performance, abilities and behavior that are highly personal and potentially stigmatizing to the child and their family. Part B provides strong privacy protections to reduce these risks. For example, participating agencies must have administrative and technical controls in place to protect PII and must notify the parent of the types and locations of education records collected and how they are used and of parental rights regarding PII, including the parent’s right to request destruction of certain information related to the child when the information is no longer needed to provide educational services to the child. Like FERPA, permitted disclosure of PII under Part B without consent is very limited.

Unlike HIPAA, there is no provision that allows participating agencies to provide PII to protect or promote public health absent consent. This thwarts public health reporting requirements and voluntary data sharing for public health surveillance, analysis, policy development, intervention and evaluation. Disclosure of PII is limited to the following situations: a) a health and safety emergency b) when a public health agency assists a participating agency in serving its students; or c) when a public health agency assists a participating agency with a study (e.g., to improve student performance by ensuring that students are healthy, at school and able to learn). On the other hand, a participating agency may be able to provide meaningful data that has demographic, geographical, temporal and socioeconomic details, unless these details would make it possible to identify the child with reasonable certainty.

Unlike HIPAA, absent consent, there is no provision that allows participating agencies to provide PII to health care providers for treatment except when needed to respond to a health emergency, or to health plans. The participating agency must obtain consent to disclose PII to obtain third party payment for
health-related services that the disabled child needs to benefit from special education. While consent requirements may delay or limit data sharing, they also promote student, family and community trust.

**Resources:** For further Information on IDEA, visit the webpage of the U.S. Department of Education at [https://sites.ed.gov/idea/](https://sites.ed.gov/idea/).

This summary is provided for informational and educational purposes only. It does not constitute legal advice. For legal advice, please consult specific legal counsel.
Protection of Pupil Rights Amendment

<table>
<thead>
<tr>
<th>Type of data</th>
<th>Education survey, analysis and evaluation records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source of data</td>
<td>State and local educational agencies</td>
</tr>
<tr>
<td>Citation</td>
<td>Federal statute, the Protection of Pupil Rights Amendment (PPRA), 20 U.S.C. §1232h; implemented by Federal Regulations, 34 CFR Part 98</td>
</tr>
</tbody>
</table>

**Brief description:** The Protection of Pupil Rights Amendment (PPRA) protects the privacy of elementary and secondary school students, as well as the privacy of their parents, related to the collection and subsequent analysis of certain types of data. While most privacy laws protect subsequent use and disclosure of existing data, PPRA is concerned with data collection activities, applying to data that are frequently deemed to be sensitive and could serve as the basis for prejudicial or discriminatory treatment. Even though data covered by PPRA are sensitive, these data are relevant to several areas of significant public health importance, including sexual and reproductive health, behavioral health, substance abuse and mental health. Consequently, PPRA’s requirements and limits may affect individuals wishing to preserve their privacy as well as individuals with poorly understood health issues that might desire or benefit from increased public health surveillance and intervention.

PPRA applies to the programs and activities of a state educational agency (SEA), a local educational agency (LEA) and other recipients of funds under any program administered by the U.S. Department of Education (ED). As discussed below, PPRA requires that LEAs adopt policies that provide parents and eligible students (i.e., at least 18 years old or an emancipated minor) rights of notice, inspection and consent, and requires LEAs to develop and adopt policies addressing specific situations related to the collection and analysis of protected information. Certain PPRA requirements will apply to a private elementary or secondary school that does not receive ED funds if the ED directly funds a “protected information survey” that is administered to its students.

PPRA prohibits a school from requiring students to provide information on attitudes, habits, traits, opinions, beliefs or feelings relating to “eight protected topics”:

1. political affiliations;
2. mental and psychological problems that are potentially embarrassing to the student and/or his or her family;
3. sexual behavior and attitudes;
4. illegal, anti-social, self-incriminating, and demeaning behavior;
5. critical appraisals of other individuals with whom the student has close family relationships;
6. privileged and analogous relationships (e.g., mental health counselors, lawyers, physicians, and ministers);
7. religious practices, affiliations, or beliefs; or
8. income (excluding for program eligibility or financial assistance).

PPRA also imposes requirements of notice, inspection, and parental opt-out and consent which could place additional administrative burdens on the effective school and public health surveillance of these issues.
To whom does this law apply? PPRA applies to a state board of education or other agency that is responsible for the supervision of public elementary and secondary schools in a state (SEA); an elementary school, secondary school, school district, or local board of education (LEA); and to other recipients of funds under any program administered by the ED. PPRA does not apply to a post-secondary institution or to a high school equivalency program. Generally, the ED does not provide funds to private elementary and secondary schools, and PPRA would not apply. However, there is one important exception. Certain PPRA requirements apply when the ED directly funds a survey, in whole or part. This means that PPRA applies to a protected information survey that is administered in a private school if the survey is supported by the ED. For example, if the ED provides funds to a university to conduct a mental health research project, PPRA applies to collection of data from private school students related to any of the eight protected topics.

What records or information are covered? PPRA applies to:

- Survey instruments
- Instructional material used as part of the educational curriculum
- All instructional material, including teachers’ manuals, films, tapes, or other supplementary instructional material, which are used in connection with any research or experimentation program or project.

In terms of the types of data, PPRA applies to:

- Student physical examination and screening information with certain exceptions, which include a survey administered to a student in accordance with the Individuals with Disabilities Education Act (IDEA) and a hearing, vision, or scoliosis screening
- Student personal information
- Cognitive, evaluative, diagnostic, clinical, aptitude and achievement information from tests and assessments.

PPRA also applies to student information revealed through survey, analysis, or evaluation where the primary purpose is to obtain information related to one or more of the eight protected topics.

What does this law require or prohibit?

PPRA’s requirements differ depending on whether or not a survey is funded by the ED.

Surveys funded by the U.S. Department of Education. If the ED funds, in whole or part, a survey:

- All instructional material used by students in ED-funded surveys, evaluations and analyses must be available to parents or eligible students for inspection before the child uses it. Instructional materials include teacher’s manuals, films, tapes or other supplemental material that will be used in connection with the survey, analysis or evaluation.
- No student shall be required to submit to a survey, analysis or evaluation that reveals information related to any of the eight protected topics without the written prior consent of the parent or eligible student.

These requirements apply to both public and private elementary and secondary schools.
Surveys funded by sources other than the Department of Education. If the ED provides no funding, PPRA does not require prior written consent to a survey, analysis, or evaluation that reveals information related to any of the eight protected topics. Instead, under the law, the LEA must directly notify the parent or eligible student of the administration of a survey regarding one or more of the eight protected topics, the right to inspect the survey upon request, and the right to opt out of participating. The LEA must provide this notice to parents and eligible students at least annually at the beginning of the school year. In the notification, the LEA shall notify parents or eligible students of the specific or approximate dates during the school year when these surveys are scheduled.

Example: Applying PPRA’s requirements. The Youth Risk Behavior Survey (YRBS) monitors six categories of health-related behaviors that contribute to the leading causes of death and disability among youth and adults, including behaviors that contribute to unintentional injuries and violence, sexual behaviors related to unintended pregnancy and sexually transmitted diseases, including HIV infection, alcohol and other drug use, tobacco use, unhealthy dietary behaviors, and inadequate physical activity. Asking students about several of these categories of health-related behaviors would reveal information concerning several of PPRA’s eight protected topics.

The YRBS is funded by the Centers for Disease Control and Prevention, within the U.S. Department of Health and Human Services. Since the survey is not funded by the ED, the prior written consent requirement would not apply to its administration. The notification, inspection and opportunity to opt out requirements described above would apply to the LEA, and the parent or eligible student may exercise their right to opt out of participation in the YRBS. Note, while PPRA does not require prior written consent before administering the YRBS, a school district may decide to obtain prior written consent and adopt policies to this effect.

Additional PPRA requirements. In addition to protected information surveys, the LEA shall notify parents and eligible students of the following other activities, along with the right to opt out:

- Collection, disclosure or use of personal information for marketing or commercial purposes
- Certain physical examinations and screenings.

LEAs must also provide parents and eligible students with the following rights of inspection upon their request:

- Surveys developed by third parties
- Surveys used to collect personal information for marketing or commercial purposes
- Instructional material used as part of the educational curriculum; instructional material does not include academic tests or academic assessments

PPRA requires LEAs to develop “arrangements” to protect student privacy with respect to:

- Administration of a survey regarding one or more of the protected topics
- Collection, disclosure and use of personal information for marketing and commercial purposes

LEAs must also develop a policy regarding the administration of a physical examination or screening of a student. Local policy could include additional de-identification and disclosure requirements.
LEAs, at a minimum, must provide notice to parents of these policies, at least annually at the beginning of the school year and within a reasonable period of time if any substantive change is made to the policies.

What is personal information? PPRA does not clearly distinguish between the collection and use of identifiable and de-identified information. The term “personal information,” defined as “individually identifiable information,” is primarily used in the context of the sale of student information or student information used for marketing. PPRA provides a non-exhaustive list of identifiers (i.e., names, addresses, phone numbers, and social security numbers).

An exception to PPRA’s rules protecting student personal information for marketing and commercial purposes applies where the collection, disclosure or use is for the exclusive purpose of developing, evaluating, or providing educational products or services for or to students or educational institutions. An example is a test or assessment used by schools to provide cognitive, evaluative, clinical, aptitude and achievement information about students and the subsequent analysis and public release of the aggregate data from the tests and assessments. Note, this example concerns data collection, disclosure or use for commercial purposes, including the development, evaluation, or provision of educational products or services, and not to inform services for a particular student (roughly analogous to population-level surveillance).

PPRA requires LEAs to develop “arrangements to protect student privacy” with respect to surveys and evaluations relating to the eight protected topics. PPRA also mandates that LEAs develop policy regarding administration of a physical examination or screening, which could include privacy requirements. Local policy might further define personal information with respect to these data.

Does PPRA provide standards to render personal information de-identified? Removal or suppression of the listed identifiers, as well as other direct or indirect identifiers, could be sufficient to render student personal information de-identified under PPRA. Local policy should be consulted to determine additional requirements.

What does consent require? PPRA does not define consent for disclosure of personal information and directs local educational agencies to develop their own privacy policies. The ED’s PPRA Model Notice and Consent/Opt-Out for Specific Activities reflects that a parent is required to sign, date and return the consent form.

Are students able to consent to disclosure of their own personal information? While determining consent requirements for disclosure is a local education responsibility, PPRA is instructive and may guide local policy. PPRA enables students to consent to submit to a survey when they are at least 18 years old or are emancipated. LEAs may follow this model.

When does PPRA permit disclosure without consent? PPRA is silent with respect to consent for disclosure of personal information and directs local educational agencies to develop their own privacy policies. Evaluation of local educational policy to determine whether disclosure of de-identified information is permissible without consent may be useful.

However, the data collection, disclosure or use for the purpose of developing, evaluating or providing educational products or services, including tests and assessments to provide cognitive, evaluative,
diagnostic, clinical, aptitude or achievement information about students, is excepted from PPRA’s regulation.

What is the potential impact of PPRA on individuals and families, schools and school districts, neighborhoods and communities, health care and health plans, and state and federal agencies?

PPRA restricts the collection of certain types of information that are frequently deemed to be sensitive and could serve as the basis for prejudicial or discriminatory treatment. At the same time, the requirements and limits contained in PPRA relate to several areas of data that are important to public health, including sexual and reproductive health, behavioral health, substance abuse and mental health. Consequently, PPRA affects individuals wishing to preserve their privacy as well as individuals with poorly understood health issues that might desire or benefit from increased public health surveillance. Requirements of notice, inspection, and parental opt-out and consent could place additional administrative burdens on the effective school and public health surveillance of these issues.


This summary is provided for informational and educational purposes only. It does not constitute legal advice. For legal advice, please consult specific legal counsel.
Federal Policy for the Protection of Human Subjects (Common Rule)

<table>
<thead>
<tr>
<th>Type of data</th>
<th>Identifiable private information or data collected by an investigator through interaction with a research subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source of data</td>
<td>Data may be from any source, which is collected for purposes of research or collected for another purpose and then used for research</td>
</tr>
<tr>
<td>Citation</td>
<td>Federal statute, Public Health Service Act, 42 U.S.C. §289 et seq.; Federal regulations, 45 CFR Part 46</td>
</tr>
</tbody>
</table>

**Brief description:** The Federal Policy for the Protection of Human Subjects (Common Rule) is a set of regulatory provisions that has been adopted by 20 federal agencies and departments, including the U.S. Department of Health and Human Services (HHS). The Common Rule protects the rights and interests of research subjects and ensures that research on human beings is conducted in an ethical manner. All participating agencies and departments have adopted the same basic protections (Subpart A). Subpart A specifies how human subjects research is to be conducted and reviewed, establishing basic requirements for Institutional Review Boards (IRBs), informed consent and assurance of regulatory compliance. In addition to basic protections that apply to all research subjects, the HHS regulations include additional protections for research involving pregnant women, human fetuses, and neonates; prisoners; and children (Subparts B, C, and D). In particular, in Subpart D, HHS establishes limits on research that it will fund and adds certain protections if the research presents more than minimal risk to children. In addition to the Common Rule, research use may require compliance with other laws that apply to specific data types or sources, such as the Family Educational Rights Privacy Act (FERPA) for education records, the HIPAA Privacy Regulations for health care records, and 42 CFR Part 2 for substance use disorder records.

The Common Rule was substantially revised in 2017. With one exception, the revised Common Rule applies to studies starting on or after January 21, 2019. The one exception, the revised cooperative research requirements for projects that involve more than one institution, applies to studies starting on or after January 20, 2020. This summary discusses the Common Rule as revised.

**To whom does this law apply?** The Common Rule applies to an institution that is engaged in non-exempt research that involves human subjects and is conducted, sponsored or regulated by a participating federal agency or department. The institution may be public or private and include, for example, a federal, state, tribal, or territorial governmental entity, university, school, community-based organization, or private research or business entity. To determine whether the Common Rule applies to an institution for a particular project, the following questions and definitions apply:

1. **Q Is the institution engaged in an activity that is research involving human subjects?**
   - **Research** is an activity that involves a systematic investigation designed to develop or contribute to generalizable knowledge. The Common Rule explicitly states that public health surveillance activities are not research. For example, suicide reporting to a health department for surveillance purposes is not research. On the other hand, a study to compare outcomes of suicide prevention programs would be research, even if conducted by a public health agency.

   While not explicitly excluded from the definition of research, other activities undertaken by a public health agency to carry out its statutory mandate might not be research. For
example, a public health intervention might not be research if undertaken for the purpose of protecting and maintaining the health and welfare of the population(s) for which the public health agency is responsible, rather than for the purpose of developing or contributing to generalizable knowledge. Most likely, public health’s implementation of a suicide prevention program for adolescents and evaluation of its program would not be research, whereas comparison of different programs or interventions for purposes of generalizable knowledge would be research.

Since public health practice and research both use systematic scientific methods, it can be difficult to distinguish research and non-research. As described below, the Common Rule includes exemptions that might make it unnecessary to resolve close “research” versus “non-research” decisions. For example, disclosure of identifiable health-related data by a HIPAA-covered health care provider or health plan is exempt from the Common Rule if disclosed for “public health activities and purposes” in compliance with the HIPAA Privacy Rule.

- Research involves human subjects if the activity involves living individuals and any of the following:
  1. Obtaining information or biospecimens through intervention with the individual and using, studying or analyzing the information or biospecimens. Intervention includes physical procedures to gather information such as drawing a blood sample and manipulations of the subject (such as through deceit), or the subject’s environment, that are performed for research purposes.
  2. Obtaining information or biospecimens through interaction with the individual and using, studying or analyzing the information or biospecimens. Interaction includes communication or interpersonal contact between the investigator and subject such as conducting an oral interview or written survey.
  3. Obtaining, using, studying, analyzing or generating identifiable private information or identifiable biospecimens. Identifiable private information and identifiable biospecimens are described below.

Q Is the human subjects research conducted, supported, or regulated by a participating federal agency or department? For example, the Common Rule applies to research that is conducted or funded by the Centers for Disease Control and Prevention, the Substance Abuse & Mental Health Services Administration, and the U.S. Department of Education.

Q Is the human subjects research eligible for exemption from the requirements of the Common Rule?

- The Common Rule exempts eight categories of research activities. The Common Rule either does not apply or has limited applicability, depending on the category of exemption. HHS has prohibited all research involving prisoners and some research involving children from exemption. If a study does not qualify for exemption, then it must comply with all of the Common Rule requirements, including IRB review and approval. Here are some commonly used exemptions:
  - Research, including research that involves children, that is conducted in educational settings is exempt if the research study only involves normal education practices such as research on regular and special education...
instructional strategies, or research on the effectiveness of or the comparison among instructional techniques, curricula or classroom management methods.

- Research on adults and children that involves educational tests (for example, cognitive, diagnostic, aptitude, and achievement tests) or observation of public behavior is exempt if the investigator does not participate in the testing or activities being observed. Research on adults that involves surveys, interviews, or observation of public behavior (including observation that includes participation by the investigator in the activities being observed), is exempt. For all research under this category, the information obtained must be recorded by the investigator in such a manner that the subjects cannot readily be identified. Additionally, any disclosure of the subjects’ responses outside the research must not place the subjects at risk of criminal or civil liability or be damaging to the subjects’ financial standing, employability, educational advancement, or reputation. If the subjects can be readily identified, an IRB must conduct a limited review to ensure that there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data.

- Research and demonstration projects, including those that involve children, that are conducted or supported by a federal agency and are designed to study, evaluate, improve, or otherwise examine public benefit or service programs are exempt.

  - The Common Rule also exempts secondary research use of identifiable private data or identifiable biospecimens if certain conditions are met. Secondary research involves the use of data or biospecimens that were collected for another purpose, such as research use of information that was collected for clinical care, for public health surveillance, or for a different research project. To be exempt from IRB review, any one of the following circumstances must be met:

    1. The identifiable private information or identifiable biospecimens are publicly available.

    2. Information is recorded by the investigator in such a manner that the subjects cannot readily be identified directly or through identifiers linked to the subjects, the investigator does not contact the subjects, and the investigator will not re-identify subjects.

    3. The research involves only information collection and analysis involving the investigator’s use of identifiable health information that is regulated by the HIPAA Privacy Rule for the purposes of “health care operations,” “research,” or for “public health activities and purposes” as these terms are described in HIPAA.

    4. The research is conducted by, or on behalf of, a federal department or agency using government-generated or government-collected information obtained for non-research activities, if the research generates identifiable private information that is or will be maintained on information technology that is subject to certain federal laws that apply to the collection or use of data.
Secondary research might not qualify for exemption under any of the four circumstances described above. An example is a research project where the investigator records identifiable private data and the data are not regulated by HIPAA. In this situation, the Common Rule allows for broad consent to research. Broad consent is a new type of informed consent provided under the revised Common Rule pertaining to storage, maintenance and secondary research with identifiable private information or identifiable biospecimens. Broad consent may be used for research that involves data or biospecimens of both adults and children. Broad consent omits some of the elements of informed consent and requires additional elements. (Informed consent is discussed below under “What does consent require?”)

Importantly, broad consent allows an individual to consent to current research and future research based on a general description of the types of research that might be done. This means that research using private identifiable data or identifiable biospecimens is not limited to a specific research project; research that meets the general description may be conducted without contacting the research subject for further permission. Secondary research, for which broad consent is required, is exempt from full IRB review. However, limited IRB review is required as follows:

- **Storage or maintenance for secondary research** for which broad consent is required: Storage or maintenance of identifiable private information or identifiable biospecimens (for example, a data or tissue repository), for potential secondary research use requires that an IRB conduct a limited IRB review and makes certain determinations. These determinations concern compliance with broad consent requirements; adequate provisions to safeguard privacy of research subjects and confidentiality of data; and the need for additional safeguards, if indicated, to protect the rights and welfare of subjects who are likely to be vulnerable to coercion or undue influence, such as children, prisoners, individuals with impaired decision-making capacity, or economically or educationally disadvantaged persons.

- **Secondary research use** for which broad consent is required: Research involving the use of identifiable private information or identifiable biospecimens for secondary research use is exempt if the following criteria are met:
  1. Broad consent for the storage, maintenance and secondary research use of the identifiable private information or identifiable biospecimens was obtained in accordance with the requirements of the Common Rule;
  2. Documentation of informed consent or waiver of documentation of consent was obtained in accordance with the Common Rule;
  3. An IRB conducts a limited IRB review and determines that: (i) adequate provisions are in place to safeguard privacy of research subjects and confidentiality of data, and (ii) the research to be conducted is within the scope of the broad consent; and
  4. The investigator does not include returning individual research results to subjects as part of the study plan. This provision does not prevent an investigator from abiding by any legal requirements to return individual research results.
What records or information are covered? If the investigator obtains information or biospecimens for research through *intervention* with the research subject (such as a blood draw or manipulating the subject or the subject’s environment) or *interaction* with the subject (such as through an interview or survey), the Common Rule applies regardless of whether the information or biospecimen is identifiable. If the investigator obtains, uses, studies, analyzes or generates private information, the Common Rule applies only if the information is identifiable.

What does this law require or prohibit? The Common Rule requires that an institution that is engaged in non-exempt research that involves human subjects and is conducted, sponsored, or regulated by a participating federal agency or department file an assurance of compliance with the rule’s requirements for the protection of human subjects in research. The Common Rule establishes requirements for IRB membership, function, operations, review of research and record keeping. It specifies how research that involves human subjects is to be conducted and reviewed, including specific rules for obtaining and documenting informed consent.

What is Identifiable private information or an identifiable biospecimen? Information is *identifiable* if the identity of the subject is or may readily be ascertained by the investigator or associated with the information. Likewise, a biospecimen is *identifiable* if the identity of the subject is or may readily be ascertained by the investigator or associated with the biospecimen. Information is *private* if it concerns behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, or it concerns information that has been provided for specific purposes by an individual and that the individual can reasonably expect will not be made public (e.g., a medical record or education record). The Common Rule requires that federal departments and agencies, in consultation with experts, periodically evaluate the effect of developing technologies or techniques on the risk of data re-identification and may use guidance to alter the interpretation of information deemed individually identifiable based on their findings.

Does the Common Rule provide standards to render private information or a biospecimen de-identified? No specific standards are provided. If the identity of the subject is or may readily be ascertained by the investigator or associated with the information, then the information is identifiable.

What does consent require? Consent to participate in research must be “informed,” which covers both the substance of the consent and the process for obtaining consent. Consent must also be documented consistent with the requirements of the Common Rule. An electronic informed consent process is allowed if it satisfies Common Rule requirements.

The Common Rule includes extensive requirements for informed consent. While not exhaustive, many of the key components are listed below.

Informed consent must:

- Be obtained under circumstances that provide the prospective subject sufficient opportunity to discuss and consider whether or not to participate and that minimizes the possibility of coercion or undue influence;
- Provide information in a language understandable to the prospective subject;
- Provide information that a reasonable person would want to have in order to make an informed decision about whether to participate and an opportunity to discuss that information;
- Include a concise and focused presentation of the key information that is most likely to assist a prospective subject in understanding the reasons why one might or might not want to participate in the research;
- Present information in sufficient detail relating to the research and must be organized and presented in a way that facilitates the prospective subject's understanding of the reasons why one might or might not want to participate;
- Not include any exculpatory language through which the subject is made to waive or appear to waive any of the subject's legal rights, or releases or appears to release the investigator, the sponsor, the institution, or its agents from liability for negligence.

Informed consent must also include the following elements and notices:
- A statement that the study involves research, an explanation of the purposes of the research and the expected duration of the subject's participation, a description of the procedures to be followed, and identification of any procedures that are experimental;
- A description of any reasonably foreseeable risks or discomforts to the subject;
- A description of any benefits to the subject, or to others, that may reasonably be expected from the research;
- A disclosure of appropriate alternative procedures or courses of treatment, if any, that might be advantageous to the subject for research that involves treatment;
- A statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained;
- For research involving more than minimal risk, an explanation as to whether any compensation and an explanation as to whether any medical treatments are available if injury occurs, and, if so, what they consist of or where further information may be obtained;
- An explanation of whom to contact for answers to pertinent questions about the research and research subjects' rights and whom to contact in the event of a research-related injury to the subject;
- A statement that participation is voluntary, refusal to participate will involve no penalty or loss of benefits to which the subject is otherwise entitled, and the subject may discontinue participation at any time without penalty or loss of benefits to which the subject is otherwise entitled; and
- Notice about whether participants' information or biospecimens collected as part of the current research might be stripped of identifiers and used for other research in the future.

If research involves only the storage, maintenance and secondary research uses of identifiable private information and identifiable biospecimens, broad consent may be obtained in lieu of informed consent. The Common rule states the elements required for broad consent, which includes some of the elements described above and some additional elements. Broad consent permits use of information and biospecimens for multiple studies or future studies that are described more generally in the consent and is not limited to a specific research project.
The IRB may approve a waiver or alteration of consent, as discussed below in “When does the Common Rule permit disclosure of identifiable private information or identifiable biospecimens without consent?”

**Are minors able to consent to disclosure of their private information for research?** The Common Rule requires the “legally effective informed consent” of the subject or the subject’s legally authorized representative. This means that if a minor is emancipated under state law, the minor may exercise the same rights as an adult to consent to research. The Common Rule appears to allow a minor to consent to research that involves treatment or procedures to which a minor may consent under state law. For example, state law may allow a minor to consent to medical care in general, without their parent’s permission, or to specific types of diagnosis and treatment such as for drug abuse, alcoholism, mental or emotional disorder, sexually transmitted disease, pregnancy, or family planning services. However, the Common Rules is not explicit on this issue. Possibly, the research project will satisfy criteria to be exempt from review (see discussion, above, regarding exemptions). If not, for proposed research that involves medical care for which the minor can consent, the safest course of action is to request that the IRB review the research project to determine whether it meets criteria for waiver of consent, which are discussed below. Whether or not a minor can consent to research, a minor’s assent (affirmative agreement) to participate in research must be obtained depending on the minor’s age, maturity and psychological state.

**When does the Common Rule permit disclosure of identifiable private information or identifiable biospecimens without consent?**

As discussed above, the Common Rule includes categories that exempt research activities from compliance with the Common Rule, including consent requirements. If research is not exempt, an IRB may approve a waiver or alteration (for example, consent that omits some of the required elements) of consent if it determines that the research project meets certain criteria. An IRB may approve a waiver or alteration of consent for research that involves both children and adults.

First, an IRB may approve a waiver or alteration of consent for a research or demonstration project that is conducted or approved by state or local officials and is designed to study, evaluate, improve or otherwise examine public benefit or service programs. To waive or alter consent for public benefits research, the IRB must find that the research could not practicably be carried out without the waiver or alteration.

More generally, the IRB may approve a waiver or alteration of consent for a research project if it finds:

- The research involves no more than minimal risk to the subjects;
- The research could not practicably be carried out without the requested waiver or alteration;
- If the research involves using identifiable private information or identifiable biospecimens, the research could not practicably be carried out without using such information or biospecimens in an identifiable format;
- The waiver or alteration will not adversely affect the rights and welfare of the subjects; and
- Whenever appropriate, the subjects or legally authorized representatives will be provided with additional pertinent information after participation.
What is the potential impact of the Common Rule on individuals and families, schools and school districts, neighborhoods and communities, healthcare and health plans, and state and federal agencies?

Research depends on a vast array of data, including data that are highly sensitive and concern vulnerable individuals or populations. The Common Rule provides a system to weigh competing interests of the individual in privacy and autonomy and society’s interest in research to protect the public’s health, improve education, advance science and medicine, address health disparities and contribute to knowledge. The Common Rule’s protections of research subjects, however, only applies to research that is conducted, supported or regulated by a federal department or agency that has adopted the Common Rule. While not required, an institution may adopt policies to follow the Common Rule for all research in which it participates, regardless of funding source.

Generally, informed consent is required, providing individuals a choice of whether to participate in research. Additionally, an IRB determines whether the project includes adequate protections of research subjects. In particular, to approve a research study, an IRB must find that:

- Risks to research subjects are minimized;
- Risks to subjects are reasonable in relation to anticipated benefits, if any, to the subjects;
- Selection of subjects is equitable;
- Informed consent will be sought and documented from each prospective research subject or the subject’s legally authorize representative, in accordance with and to the extent required by the Common Rule;
- If broad consent is permitted, it is obtained and documented in compliance with the Common Rule;
- When appropriate, the research plan makes adequate provision for monitoring the data collected to ensure the safety of subjects; and
- When appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data.

In addition, when some or all of the subjects are likely to be vulnerable to coercion or undue influence, such as children, prisoners, individuals with impaired decision-making capacity, or economically or educationally disadvantaged persons, the IRB ensures that additional safeguards have been included in the study to protect the rights and welfare of these subjects.

While the Common Rule provides many protections for research subjects, a research project might be exempt from compliance or only require limited IRB Review. Research that qualifies for exemption usually involves little or no risk to subjects. Exempt research, including research that involves private data, is then able to proceed quickly, without the expense and delay associated with a full IRB review.

**Resources:** For further Information on the Common Rule, visit the webpage of the Office of Human Research Protection at [https://www.hhs.gov/ohrp/regulations-and-policy/regulations/common-rule/index.html](https://www.hhs.gov/ohrp/regulations-and-policy/regulations/common-rule/index.html).

This summary is provided for informational and educational purposes only. It does not constitute legal advice. For legal advice, please consult specific legal counsel.