The Office of the National Coordinator for Health Information Technology

Legal and Ethical Architecture for PCOR Data

CHAPTER 3:

LINKING LEGAL AND ETHICAL REQUIREMENTS TO PCOR DATA

Submitted by:
The George Washington University
Milken Institute School of Public Health
Department of Health Policy and Management

TABLE OF CONTENTS

Chapter 3

Linking Legal and Ethical Requirements to PCOR Data

INTRODUCTION

The legally relevant PCOR data characteristics identified in Chapter 2 are associated with specific legal requirements in the statutes and regulations that govern access and use of health information for PCOR. This chapter summarizes those specific legal requirements and links them directly to the key characteristics of PCOR data described in Chapter 2. More detailed summaries of the relevant statutes and regulations are provided in Appendix A.

LINKING LEGAL REQUIREMENTS TO RELEVANT PCOR CONSIDERATIONS

There is not a single statute or set of statutes and regulations that provides a uniform and consistent framework for PCOR. Rather, many federal and state statutes and regulations (summarized in detail in the Legal Appendix) govern and impose privacy and security requirements on health information that may be used for PCOR. These statutes and regulations stipulate different requirements, the applicability of which vary (and perhaps even overlap or contradict) based on, for example: what type of data is being collected, accessed, used, or disclosed; the identity of the organization that collected the information; the purpose for which it was collected; the identity of the requesting organization; and the purpose for which the data was requested. This complex legal environment may make it difficult for stakeholders, including researchers, providers, consumers, payers, and health information organizations, to be certain of the legal requirements that govern the health information they hold or acquire and their use and/or disclosure of that information.

Chapter 2 identified a series of issues that must be addressed or considered in order to determine: 1) whether a statute and/or regulation applies (i.e., what information it protects and who it applies to) and if so, 2) how it applies (i.e., how the information it protects may be used by the entities it governs and requirements related to this). This chapter organizes relevant legal provisions according to seven key data considerations:

- Identifiability and Content;
- Subject;
- Source;
- Access and Use/Purpose;
- Consent/Authorization;
- Security; and
- Legal Status

Issues related to identifiability, content, subject, and source help to identify whether a particular law and/or regulation apply. For example, the Health Insurance Portability and Accountability Act of 1996

(HIPAA)[1] Rules[2] protect individually identifiable health information that meets certain requirements. If the health information in question is not individually identifiable, HIPAA does not apply no matter who holds the data, what kind of data it is, etc. Issues related to access, use/purpose, consent/authorization, and security help to identify what requirements must be met. For example, if individually identifiable health information is requested from a hospital by a researcher and HIPAA is triggered, the hospital must comply with the specific HIPAA requirements that govern disclosures for research.

The following section links the relevant statutes and regulations that govern PCOR to these seven core issues.

Identifiability and Content

Identifiability is a legal concept that refers to the ability to link information to a particular individual. It is assessed based upon the presence of certain data elements and/or data characteristics. The federal and state privacy statutes and regulations that govern the use and disclosure of health information ONLY protect identifiable health information; all of these statutes and regulations define identifiability differently, but none are triggered by the use of de-identified information (i.e., no individually identifying elements remain in the data). Even if information has been de-identified, however, privacy statutes and regulations may still apply depending on the process of de-identification, the remaining data elements, and the potential for data re-identification.

Even if information meets a law or regulation's definition of "identifiable," each statute and regulation protects only certain types of identifiable information. In particular, the applicability of a particular statute or regulation will depend on the data's content. Content pertains to the subject matter or substance of the data, which may include contact, demographic, medical, insurance, and/or employment information. Data that includes sensitive information (e.g., mental health, substance abuse, genetics, and/or HIV status) might be subject to additional regulation. Other relevant data characteristics must also be present in order for a particular statute or regulation's protections to apply to the information (e.g., data source, purpose of collection)—these are discussed in other sections.

Key Statutes and Regulations Related to Identifiability and Content

Health Insurance Portability and Accountability Act (HIPAA): In general, the HIPAA Rules govern "protected health information" (PHI), which is **individually identifiable information** (including genetic information) maintained or transmitted in any form or medium (e.g., orally, electronically, or on paper) that:

1. Is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and
2. Relates to:
    a. The provision of care to an individual;
    b. An individual's past, present, or future physical or mental health condition; or
    c. Payment for care provided to an individual, whether made in the past or present or expected in the future.[3]

[1] HIPAA, Pub. L. No. 104-191, 110 Stat. 139 (1996) (codified as amended in scattered sections of 45 U.S.C.).

[2] 45 C.F.R. Parts 160 and 164 (2017).

[3] 45 C.F.R § 160.103 (2017).

Under HIPAA, information is individually identifiable if it directly identifies the individual or if there is a reasonable basis to believe the information could be used to identify the individual.[4] The HIPAA Rules do not govern employment records or education records subject to FERPA.[5] In general, all PHI is subject to the same requirements wherever HIPAA applies, though there are additional restrictions applicable to [identifiable] psychotherapy notes and genetic information. Other provisions apply depending on the subject of the information (e.g., minors, prisoners) and/or the purpose of disclosure (e.g., sale, research). These limitations are discussed in more detail in the relevant section below.

Note that **health information that has been de-identified is not considered to be PHI for purposes of HIPAA applicability**.[6] There are two methods by which information can be considered "de-identified" under HIPAA[7]—the Safe Harbor method and the Expert Determination method. The Safe Harbor method requires that the information be stripped of 18 specified identifiers (see Table 1 below).[8] Even where these 18 identifiers are removed, an individual's information is only considered de-identified under the Safe Harbor method if the Covered Entity does not have actual knowledge that the information could be used (on its own or in combination with other information) to identify the individual.[9] Note that a limited data set (LDS), which is information stripped of 16 specified identifiers, is still considered PHI (i.e., individually identifiable health information).[10] The Expert Determination method requires that a person appropriately qualified in de-identification methods determines that there is very small risk that an anticipated recipient of the information could use the information (on its own or in combination with other reasonably available information) to identify the individual.[11]

[4] 45 C.F.R § 160.103 (2017).

[5] Note that HIPAA also does not apply to what FERPA defines as "treatment records," which are excluded from FERPA's definition of "education records" (45 C.F.R. § 160.103, referencing 20 U.S.C. § 1232g(a)(4)(B)(iv)).

[6] 45 C.F.R §160.103 (2017); 45 C.F.R Part 164 §§ 302, 400, and 500(a) (2017).

[7] U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR). Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (2012), *available at*: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

[8] 45 C.F.R. § 164.514(b)(2)(i) (2017).

[9] 45 C.F.R. § 164.514(b)(2)(ii) (2017).

[10] 45 C.F.R. § 164.514(e)(2) (2017).

[11] 45 C.F.R. § 164.514(b)(1) (2017).

Table 1: Safe Harbor Method of De-Identification

The following elements must be removed as each relates to the individual subject of the information or to that individual's relatives, employers, or household members:
Names
All geographic subdivisions smaller than a **state**, including street address, **city**, **county**, precinct, **ZIP code**, and their equivalent geocodes, *except* for the initial three digits of the ZIP code if (according to the current publicly available data from the Bureau of the Census): • The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; OR • The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000
All elements of dates (except year) for dates **that are directly related to an individual**, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
Telephone numbers
Fax numbers
Email addresses
Social security numbers
Medical record numbers
Health plan beneficiary numbers
Account numbers
Certificate/license numbers
Vehicle identifiers and serial numbers, including license plate numbers
Device identifiers and serial numbers
URLs (Web Universal Resource Locators)
IP (Internet Protocol) address numbers
Biometric identifiers, including finger and voice prints
Full-face photographs and any comparable images
Any other unique identifying number, characteristic, or code

*Note: Items in bold may be included in a limited data set.

Common Rule:[12] NOTE: In September 2015, the federal departments and agencies that have adopted the Common Rule published a Notice of Proposed Rulemaking (NPRM) proposing significant changes to the regulations.[13] Changes were published in a Final Rule on January 19, 2017, with a January 19, 2018, effective date (and extended and/or suspended effective dates for certain provisions).[14] The Common Rule provisions referenced in this Chapter reflect the 2017 Final Rule provisions. Future changes may be

[12] 45 C.F.R. Part 46, Subpart A (2017) (note: HHS version of the Common Rule).

[13] "Common Rule" Departments and Agencies, Notice of Proposed Rulemaking: Federal Policy for the Protection of Human Subjects, 80 Fed. Reg. 53933 (2017).

[14] "Common Rule" Departments and Agencies, Final Rule: Federal Policy for the Protection of Human Subjects, 82 Fed. Reg. 7149 (2017).

made to the regulations, and researchers and other stakeholders should continue to monitor the status of the Common Rule.

The Common Rule Subpart A applies to all federally supported research involving human participants. Research (i.e., a systematic investigation designed to develop or contribute to generalizable knowledge)[15] involves human participants when an investigator:

- Obtains information or biospecimens about a living individual through intervention or interaction with the individual and uses, studies, or analyzes the information or biospecimens; or
- Obtains, uses, studies, analyzes, or generates ***identifiable*** private information or ***identifiable*** biospecimens about a living individual.[16]
    - Information and biospecimens are identifiable if the individual's identity is or may be readily ascertained by the investigator or associated with the information[17] or the biospecimen.[18]
    - Information is private when it is about behavior where an individual can reasonably expect that no observation or recording is taking place and information provided for specific purposes that the individual can reasonably expect will not be made public;[19]

The Common Rule also exempts several types of research from ALL of its requirements, including the following types related to data identifiability and content[20] (see section on Source below for discussion of additional exemptions):

1. Research that only involves interactions using educational tests, survey procedures, interview procedures, or observation of public behavior[21] or that involves benign behavioral interventions[22] in conjunction with information collection from a participant[23] if:
    a. The researcher records information so that the participant's identity cannot be readily ascertained (directly or through linked identifiers); or

---

[15] 82 Fed. Reg. 7149 at 7260-61 (to be codified at 45 C.F.R. § 46.102(l)).

[16] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(e)(1)).

[17] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(e)(5), (6)).

[18] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(e)(5), (6)).

[19] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(e)(4)).

[20] 82 Fed. Reg. 7149 at 7261 (to be codified at 45 C.F.R. § 46.104).

[21] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(2)).

[22] Note: benign behavioral interventions are brief in duration, harmless, painless, not physically invasive, and not likely to have a significant, adverse, lasting impact on the participants; further, the researcher must not have any reason to think the participants will find the interventions offensive or embarrassing (82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(3)(ii)).

[23] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(3)(i)). (Note that this exemption is only available to research with an adult participant, and the participant must prospectively agree to the intervention and information collection).

b. Disclosure of a participant's responses outside the research setting would not reasonably place the participant at risk of criminal or civil liability or be damaging to the participant's financial standing, employability, educational advancement, or reputation;

2. Secondary research use of identifiable private information or identifiable biospecimens if:
   a. The researcher records such information so that the subject's identity cannot be readily ascertained (directly or through linked identifiers);[24] or
   b. Such use is limited to information collection and analysis regulated under the HIPAA Privacy Rule as a use or disclosure for the purposes of "health care operations" or "research" or for "public health activities and purposes";[25] and

3. Research and demonstration projects designed to study, evaluate, improve, or examine public benefit or service programs that are conducted, supported by, or subject to approval of a federal department or agency.[26]

The Common Rule also exempts some types of research from most, BUT NOT ALL, of its requirements based on identifiability and content (see section on Source below for discussion of additional partial exemptions):

1. Interactions using educational tests, survey procedures, interview procedures, or observation of public behavior[27] or involving benign behavioral interventions[28] in conjunction with information

[24] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(4)(ii)). (Note that for secondary research use in this context, the researcher may not contact and will not re-identify the subject).

[25] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(4)(iii)). (Note: "research" and "health care operations" are defined at 45 C.F.R. § 164.501 (2017); "public health activities and purposes" are defined at 45 C.F.R. § 164.512(b) (2017)).

[26] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(5)). (Note: each federal department or agency must establish (on a publicly accessible federal website or in another manner determined by the department or agency head) a list of the research or demonstration projects it conducts or supports under this provision).

[27] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(2)).

[28] Note: benign behavioral interventions are brief in duration, harmless, painless, not physically invasive, and not likely to have a significant, adverse, lasting impact on the participants; further, the researcher must not have any reason to think the participants will find the interventions offensive or embarrassing (82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(3)(ii)).

collection[29] if an IRB conducts a limited review and determines that provisions to protect privacy and confidentiality are adequate;[30]

2. Storage or maintenance of identifiable private information or biospecimens for ***potential*** secondary research use if an IRB conducts a limited review and determines that broad consent will be appropriately obtained and documented;[31] and that, should there be a change in storage or maintenance of the information or biospecimens, the provisions in place to protect privacy and confidentiality are adequate;[32] or
3. Secondary research use of identifiable private information or biospecimens if:
    a. The investigator does not include "returning individual research results to [subjects]" as part of the study plan; and
    b. An IRB conducts a limited review and determines that the planned research is within the scope of broad consent;[33] and provisions in place to protect privacy and confidentiality are adequate.[34]

42 C.F.R. Part 2:[35] NOTE: In 2016, the Substance Abuse and Mental Health Services Administration (SAMHSA) proposed several major modifications to align the Part 2 regulations with the current U.S. healthcare system.[36] SAMHSA finalized changes to Part 2 in a Final Rulemaking issued on January 18, 2017.[37] The finalized changes to Part 2 went into effect on March 21, 2017; the Part 2 provisions referenced in this chapter reflect the 2017 Final Rule provisions. In conjunction with publishing the Final Rule, SAMHSA issued a Supplemental Notice of Proposed Rulemaking to propose additional clarifications to the amended Part 2 regulations and seek public comment on these proposals.[38] Future changes may

---

[29] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(3)(i)). (Note that this exemption is only available to research with an adult participant, and the participant must prospectively agree to the intervention and information collection).

[30] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.111(a)(7)). (Note: for this exemption, the information obtained by the researcher may be recorded in a way that allows the participant's identity to be readily ascertained, directly or through linked identifiers).

[31] 82 Fed. Reg. 7149 at 7262-63 (to be codified at 45 C.F.R. § 46.104(d)(7)).

[32] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.111(a)(8)).

[33] 82 Fed. Reg. 7149 at 7262-63 (to be codified at 45 C.F.R. § 46.104(d)(7)). (Note that broad consent must be obtained in accordance with relevant requirements).

[34] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.111(a)(8)).

[35] 42 C.F.R. Part 2 (2017).

[36] HHS Substance Abuse and Mental Health Services Administration (SAMHSA) Notice of Proposed Rulemaking: Confidentiality of Substance Use Disorder Patient Records ("Part 2 NPRM") 81 Fed. Reg. 6988 (2016).

[37] SAMHSA Supplemental Notice of Proposed Rulemaking: Confidentiality of Substance Use Disorder Patient Records ("Part 2 Supplemental NPRM") 82 Fed. Reg. 6052 (2017).

[38] SAMHSA Final Rule: Confidentiality of Substance Use Disorder Patient Records ("Part 2 Final Rule") 82 Fed. Reg. 5485 (2017).

be made to Part 2, and researchers and other stakeholders should continue to monitor the status of Part 2.

Part 2 restricts disclosure of all information, whether recorded or not, obtained by a Part 2 program (see section on Source below for more information) for purposes of providing substance use disorder services that would directly or indirectly[39] identify a patient as having or having had a substance use disorder.[40]

Under Part 2, information is identifying if it includes elements such as "name, address, social security number, fingerprints, photograph, or similar information by which a patient's identity can be determined with reasonable accuracy directly or by reference to other publicly available information."[41]

GINA: GINA protects genetic information from being collected or used for certain purposes. Genetic information is defined as information (other than information about sex or age) about:

1. An individual's genetic tests;[42]
2. The individual's family members' genetic tests; and
3. The manifestation of a disease or disorder in the individual's family members.

In addition to this definition, GINA required that the Secretary of the U.S. Department of Health and Human Services (HHS) modify the HIPAA Rules to explicitly include genetic information within the definition of PHI. In 2013, HHS issued a Final Rule that made multiple, significant changes to the HIPAA Rules, including adoption of the modification(s) required by GINA.[43]

Privacy Act of 1974:[44] The Privacy Act limits the disclosure of records about individuals that are maintained by a federal agency and contain the individual's "name or identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph."[45]

---

[39] Indirect identification could occur by reference to other publicly available information or through verification of such an identification by another person.

[40] 42 C.F.R. § 2.12(a)(1) (2017).

[41] 42 C.F.R. § 2.11 at "Patient identifying information" (2017) (Note that this definition explicitly does not include a number assigned to [an individual] by a [Part 2] program if that number does not consist of or contain numbers (e.g., social security number or driver's license number) that could be used to identify [the individual] with reasonable accuracy and speed from sources external to the [Part 2] program).

[42] Note that a genetic test is defined as "analysis of human DNA, RNA, chromosomes, proteins, or metabolites that detects genotypes, mutations, or chromosomal changes" (*see, e.g.,* GINA Title I, § 101(d) (2008)).

[43] Final Rule: Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566 at 5689 (2013) (codified at 45 C.F.R. § 160.103 at "Health information" (2017)).

[44] The Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified at 5 U.S.C. § 552a).

[45] 5 U.S.C. § 552a(a)(4) (1974).

Family Educational Rights and Privacy Act (FERPA): FERPA protects education records and personally identifiable information contained within those records.[46] This includes health information collected at school-based clinics, for enrollment, or for other education-related purposes. Education records are records maintained by a federally funded educational agency, institution, or party acting for such an agency or institution that are directly related to a student. FERPA defines "personally identifiable information" as including the student's: name, address, personal identifiers (e.g., social security number, biometric record), indirect identifiers (e.g., date of birth, place of birth, mother's maiden name), family members' names, family members' addresses, information requested by a person who the educational agency or institution reasonably believes knows the identity of the individual to whom the record relates, and other information that (alone or in combination) is linked or linkable to the student that would allow a reasonable person in the school community (who does not have personal knowledge of the relevant circumstances) to identify the student with reasonable certainty.[47] The term "education records" does *not* include the following records:[48]

1. Those created by instructors, teachers, or administrators accessible only by the teacher or a substitute;
2. Those created for law enforcement purposes by a law enforcement unit of an education agency;
3. Those regarding educational agency or institution employees that are made in the normal course of business and only pertain to their employment; and
4. Those regarding a postsecondary student or student over the age of 18 created by a healthcare professional for treatment purposes *if* such records are only made, maintained, or used in connection with treatment of the student (e.g., "treatment records"). Treatment records may be disclosed for purposes other than treatment, but only if the disclosure meets an exceptions or with written consent.

State Law: States typically provide enhanced protection for sensitive information. This generally includes, but is not limited to: HIV/AIDS status, information related to sexually transmitted diseases (STD), mental health, domestic violence, women's reproductive health, alcohol and/or substance abuse, and health of the legally incompetent, including minors.

Subject

Subject refers to the person or thing that is the focus of the data. Human subjects protection and/or privacy laws apply to information depending not only on the content of the information but also on the subject of the information. Further, these laws may limit what data may be collected or used from certain classes of subjects and/or how such data can be used. Classes granted special protection may include minors, prisoners, incompetents, and pregnant women.

[46] 20 U.S.C. § 1232g(b)(1).

[47] 34 C.F.R. § 99.3(2017).

[48] 34 C.F.R. § 99.3(2017).

Key Statutes and Regulations Related to Subject

Health Insurance Portability and Accountability Act (HIPAA): HIPAA governs Regulated Entities' use and disclosure of **any** living individual or other entity's PHI[49] and any deceased individual's PHI for 50 years after the individual's death.[50] With respect to applying HIPAA's provisions, Covered Entities must treat an individual's personal representative as if the representative were the individual.[51] A personal representative is someone with authority to act on behalf of the individual in making decisions related to health care under applicable state or other law.[52] Persons legally authorized to act as a personal representative on behalf of an unemancipated minor may include a parent, guardian, or other person acting *in loco parentis* on behalf of the minor, though in states that grant the minor capacity to consent to a particular healthcare service, the minor must request that the person be treated as his/her personal representative.[53]

The only other subject-specific provisions in HIPAA relate to inmates (i.e., a person incarcerated or otherwise confined to a correctional institution[54]). HIPAA permits Covered Entities to disclose PHI about inmates to law enforcement officials and correctional institutions without the inmate's authorization for limited health and safety-related purposes.[55] An individual is no longer an inmate when released on parole, probation, supervised release, or is otherwise no longer in lawful custody.[56]

Common Rule: Subpart A applies to federally supported research involving human participants (i.e., a living human being).[57]

Subparts B–D provide additional (or modified) protections for certain vulnerable populations involved in federally supported research:

1. Subpart B applies to research involving pregnant women, human fetuses, newborns of uncertain viability, and nonviable newborns;[58]
2. Subpart C applies to biomedical and behavioral research involving prisoners (i.e., individuals involuntarily confined or detained in a penal institution or alternative facilities);[59] and

---

[49] 45 C.F.R. § 160.103 at "Person" (2017) (An entity can be a trust or estate, partnership, corporation, professional association or corporation, or other public or private entity).

[50] 45 C.F.R. § 160.103 at "Protected health information" ¶ (2)(iv) (2017).

[51] 45 C.F.R. § 164.502(g)(1) (2017).

[52] 45 C.F.R. § 164.512(g)(2)(2017).

[53] 45 C.F.R. § 164.512(g)(3)(i) (2017).

[54] 45 C.F.R. § 164.501 at "Inmate" (2017).

[55] 45 C.F.R. § 164.512(k)(5)(i) (2017).

[56] 45 C.F.R. § 164.512(k)(5)(iii) (2017).

[57] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(e)(1)).

[58] 45 C.F.R. § 46.201(a) (2017).

[59] 45 C.F.R. § 46.301(a) (2017).

3. Subpart D applies to research involving children (i.e., individuals under the legal age of consent for the treatment or procedures involved in the research).[60]

Part 2: Part 2 protects identifying information about patients, which includes any individual who has applied for or received diagnosis, treatment, or referral for treatment of a substance use disorder at a Part 2 program (see section on Source below for more information).[61] Part 2 does not treat minor patients' information differently where the relevant state's law grants the minor legal capacity to seek treatment without parental consent.[62] Where a state does not grant the minor such capacity,[63] or where a minor lacks capacity to make a rational choice (i.e., mental capacity),[64] Part 2 includes limitations on information disclosures (discussed below in the section on Consent/Authorization).

GINA: GINA protects genetic information[65] about individuals[66] and their family members. It also protects genetic information about any fetus carried by the individual (or their family member) and any embryo legally held by the individual (or their family member) utilizing assisted reproductive technology. A family member includes an individual's dependent(s) and an individual's first-, second-, third-, and fourth-degree relatives.

Privacy Act of 1974: The Privacy Act protects information about U.S. citizens and permanent legal residents held by a federal agency in a system of records.[67]

Family Educational Rights and Privacy Act (FERPA): FERPA protects education records directly related to students that are maintained by educational agencies and institutions. A student is any individual who is

---

[60] 45 C.F.R. § 46.401(a) (2017).

[61] 42 C.F.R. § 2.11 at "Patient" (2017).

[62] 42 C.F.R. § 2.14(a) (2017).

[63] 42 C.F.R. § 2.14(b) (2017).

[64] 42 C.F.R. § 2.14(c) (2017).

[65] "Genetic information" is: (1) information about an individual's genetic tests (i.e., analysis of human DNA, RNA, chromosomes, proteins, or metabolites that detects genotypes, mutations or chromosomal changes); (2) information about the individual's family members' genetic tests; (3) information about the manifestation of a disease or disorder in the individual's family members; (4) requests for or receipt of genetic services (i.e., a genetic test, genetic counseling, or genetic education) by the individual, and (5) participation by the individual or any of the individual's family members in clinical research that includes genetic services (*see, e.g.,* GINA Title I, § 101(d) (2008)).

[66] GINA does not apply to individuals in the U.S. military, those receiving health benefits through the VA or Indian Health Service, or federal employees obtaining health care through the Federal Employees Health Benefits Plan (FEHBP).

[67] 5 U.S.C. § 552a(a)(2) (1974).

or has been in attendance at a federally funded public or private agency or institution that provides educational services and/or instruction to students.[68]

State Law: States often have their own laws and regulations governing health information pertaining to certain classes of individuals, which may mirror federal protections or provide additional protections. States also often govern information about classes of individuals not specifically protected by federal laws or regulations, including:

1. Adult individuals who lack [legal] capacity to make certain decisions;
2. Minors involved with the juvenile corrections system; and
3. Individuals who are on parole, probation, or other similar type of supervision.

Federal law defers to state law for specifics about certain subjects, such as the age to consent to certain health-related services and legal requirements related to personal representatives (e.g., documentation required).

Source

Source pertains to the person, entity, and/or setting in which the data originated or was collected. Persons that originate data may include patients, providers, health plans, and government agencies, and data may be collected in a variety of settings, including clinics, homes, laboratories, etc. Privacy laws and regulations only govern certain data sources' use and disclosure of the identifiable data types described above. A data source may be the original collector (e.g., a provider in a clinical setting) or may refer to a data holder that obtains data from an original or secondary source and then shares that data with another person or entity (e.g., a data repository, registry, or research network, or clearinghouse that provides data to researchers). Determining the source of data, and thus the applicability of laws and regulations, depends on other considerations, including: (1) the form or method of data collection; (2) whether data collection/generation is ancillary to another event (e.g., a clinic encounter) or occurs as the primary event (e.g., an individual voluntarily submitting their data to a research network); and (3) whether and how data are aggregated or combined with other sources.

Key Statutes and Regulations Related to Source

Health Insurance Portability and Accountability Act (HIPAA): The HIPAA Rules apply to health plans, healthcare clearinghouses,[69] and any healthcare providers (regardless of size) that electronically transmit health information in connection with certain transactions.[70] These health-related entities are collectively known as "Covered Entities."[71] In addition, the rules apply to Covered Entities' "Business Associates," which are individuals or groups (other than members of the Covered Entity's workforce) that

---

[68] 34 C.F.R. § 99.3 (2017).

[69] A healthcare clearinghouse is a business or agency that processes nonstandard health information it receives from another entity into a standard format, or vice versa (e.g., billing services, re-pricing companies) (45 C.F.R. § 160.103 (2017)).

[70] Covered transactions include, but are not limited to, benefit eligibility inquiries and claims (*see generally* 45 C.F.R. Part 162 (2017)).

[71] 45 C.F.R §160.103 (2017).

can or do access PHI when providing certain services or functions to or on behalf of a Covered Entity.[72] Covered Entities and their Business Associates together are referred to as "Regulated Entities."[73] The HIPAA Rules only protect the use and disclosure of PHI (see section on Identifiability above for more information) by Regulated Entities. The use or disclosure of PHI by other types of individuals or organizations that are not Regulated Entities is not governed by HIPAA.

Common Rule: Subpart A applies to federally supported research involving human participants. Research is federally supported if it is conducted, supported, or otherwise subject to regulation by a federal department or agency.[74]

The Common Rule specifically excludes some activities from its definition of research; these activities are not subject to any provisions of the Common Rule.[75] For example, public health surveillance activities, including the collection and testing of information or biospecimens, that are conducted, supported, requested, ordered, required, or authorized by a public health authority are not considered "research" for purposes of Common Rule applicability.[76]

The Common Rule also exempts several types of research from ALL of its requirements, including the following types related to data source[77] (see section above on Identifiability and Content for discussion of additional exemptions):

1. Secondary research use of publicly available identifiable private information or identifiable biospecimens;[78] and

2. Secondary research use of identifiable private information or identifiable biospecimens where such research is conducted by or on behalf of a federal department or agency using government-generated or -collected information obtained for non-research activities[79] and maintained in systems of records (SORs) subject to the Privacy Act of 1974,[80]

---

[72] 45 C.F.R §160.103 (2017) (Business Associate services are limited to legal, actuarial, accounting, consultation, data aggregation, management, administrative, accreditation, or financial services; relevant functions include claims processing, data analysis, utilization review, and billing).

[73] *See, e.g.* OCR Final Rule: Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566 (2013).

[74] 82 Fed. Reg. 7149 at 7259 (to be codified at 45 C.F.R. § 46.101(a)).

[75] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(l)).

[76] 82 Fed. Reg. 7149 at 7261 (to be codified at 45 C.F.R. § 46.102(l)(2)).

[77] 82 Fed. Reg. 7149 at 7261 (to be codified at 45 C.F.R. § 46.104).

[78] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(4)(i)).

[79] 5 U.S.C. § 552a (1974).

[80] 5 U.S.C. § 552a (1974).

if certain other requirements are met.[81]

Part 2: The Part 2 regulations govern the disclosure and use of certain information maintained by "federally assisted" substance use disorder programs.[82] A program includes:

1. Individuals, entities, and identified units in general medical facilities that provide substance use disorder services (i.e., diagnosis, treatment, or referral for treatment) and hold themselves out as providing such services (e.g., advertises services, certified to provide addiction services—any activity that would lead one to conclude that the individual or entity provides substance use disorder services[83]); and
2. Medical personnel or other staff working within a general medical facility whose primary function is to provide substance use disorder services *and* who are identified as such providers.[84]

A program is "federally assisted" if it is conducted by any federal department or agency (directly or via contract), is carried out under any federal license, certification, registration, or authorization (e.g., Medicare/Medicaid certification, DEA registration to dispense a controlled substance used to treat substance use disorders), or receives any federal financial assistance (e.g., grants, federal tax-exempt status).[85]

Part 2 only protects substance abuse information that has been obtained by a federally assisted program. The restrictions on disclosure also apply to individuals and entities that have received patient records directly from Part 2 programs or from other lawful holders of patient identifying information and who have been properly notified of the prohibition on re-disclosure.[86]

GINA: GINA Title I governs collection and use of genetic information about individuals and their family members by health plans and health insurance issuers for certain purposes. GINA does not apply to life insurance plans, long-term care plan issuers, or disability insurers. GINA Title II governs employers' collection and use of genetic information about employees.

Privacy Act of 1974: The Privacy Act governs federal agency disclosure of records contained in a system of records, which is a group of any records under any agency's control from which information is

---

[81] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(4)(iv)) (Note: identifiable private information generated by the research must be maintained on information technology subject to and in compliance with the Privacy Impact Assessments requirements of the E-Government Act of 2002's Privacy Provisions (44 U.S.C. § 3501 note at § 208(b) (2002)) and, if applicable, the information used in the research must have been collected subject to the Paperwork Reduction Act of 1995 (44 U.S.C. § 3501 *et seq.*)).

[82] 42 C.F.R. § 2.2(a) (2017).

[83] SAMHSA. "Applying the Substance Abuse Confidentiality Regulations: FAQs" at Question 10 (2011), *available at*: https://www.samhsa.gov/about-us/who-we-are/laws-regulations/confidentiality-regulations-faqs.

[84] 42 C.F.R. § 2.11 at ¶ "Program" (2017).

[85] 42 C.F.R. § 2.12(b) (2017).

[86] 42 C.F.R. § 2.12(d)(2)(i) (2017).

retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

Family Educational Rights and Privacy Act (FERPA): FERPA applies to all educational agencies and institutions that receive federal education funding (e.g., public schools and districts, private and public colleges, universities, and other postsecondary institutions) but typically exempts private and religious elementary and secondary schools.[87] Where a clinic is operating in a school (e.g., a community health center offering satellite clinics in schools), FERPA would apply if the clinic is an agent of the school (i.e., if, under its agreement with a school, the clinic is carrying out the school's responsibilities and is subject to school direction). FERPA will also apply to health information collected directly by these schools, such as by school-based health professionals or for enrollment.

Food & Drug Administration (FDA) Law: There are several FDA-specific human subjects protection regulations scattered throughout Title 21 of the C.F.R.; these regulations are specific to the type of research being conducted. Parts 312 (clinical investigations of new drugs), 812 (clinical investigations of devices), and 814 (clinical investigations of Humanitarian Use Devices (HUD)[88]) all contain requirements that are in addition to or modify the requirements of Parts 50 and 56.

State Law: States generally have laws governing state-based disease registries, compulsory health information reporting (e.g., communicable diseases, vital statistics) by certain entities, health information exchanges (HIEs), and all-payer claims databases (APCDs). States also regulate health insurers, public health entities, and facility and provider licensure—requirements pertaining to these entities may relate to data sharing, confidentiality, and patient consent.

Access and Use/Purpose

The privacy laws and regulations govern access (i.e., who may, may not, or must be allowed to view, create, edit, or share protected data) and define the acceptable procedural parameters surrounding access. Factors that impact a person's ability to access data include: ownership interests (persons or entities may have the ability to limit access to data in which they have ownership interests), the data's content (access to information subject to heightened protections, such as psychotherapy notes, may be restricted), the position or affiliation of the persons seeking to access data, and the stated reason for accessing the data.

While access deals with **who** may use information, use/purpose deals with **how and why** they may use the information. Every privacy law and regulation sets forth parameters for collecting, using, and sharing data, which include the purpose and method of collecting and sharing information as well as uses that are prohibited or substantially limited. Common and generally relevant uses/purposes for collecting/sharing data include patient care, research, claims processing, advertising/marketing, and personal uses. In general, the laws and regulations allow the collection, use, or disclosure of an individual's information for any purpose with that individual's approval—this concept is discussed more fully in the section below on Consent. This section specifically addresses uses and disclosures that may occur without the individual subject's express approval.

---

[87] 34 C.F.R. § 99.1 (2017).

[88] HUD are devices intended to benefit patients in treating or diagnosing a disease that affects or is manifested in 4,000 or fewer individuals in the United States annually.

Key Statutes and Regulations Related to Access and Use/Purpose

Health Insurance Portability and Accountability Act (HIPAA): The Privacy Rule governs when and how PHI can be disclosed, which can be grouped into four broad categories:

1. Required Disclosures: a Regulated Entity **must** disclose PHI to the individual subject of the PHI (or his/her personal representative) upon his/her request and to HHS for enforcement purposes and for HIPAA-related compliance investigations;[89]
2. Prohibited Disclosures: a Regulated Entity may not disclose PHI for certain purposes (e.g., most sales of PHI[90]) and may only disclose certain types of PHI (e.g., psychotherapy notes,[91] minors' PHI[92]) in limited circumstances, even with the individual's authorization;
3. Permissive Disclosures (see Table 2 below for a complete list): a Covered Entity **may** disclose PHI **without first obtaining the individual subject of the information's authorization** for a variety of purposes (though some of these purposes require that, where practicable, the individual be given the opportunity to informally object to the disclosure);[93]
4. Authorized Disclosures: Any disclosures not required, permitted, or prohibited by the rule require written authorization from the individual who is the subject of the information.[94]

Table 2: List of HIPAA Permissive Exceptions Available to Covered Entities[95]

General Purpose of Covered Entity Disclosure	To Whom a Covered Entity May Disclose—and Relevant Limitations
For treatment purposes[96]	To any entity for its own or any healthcare provider's treatment activities
For payment purposes	To any entity for its own payment activities or to a Covered Entity or healthcare provider for the receiving entity's payment activities

[89] 45 C.F.R. § 164.502(a)(2) (2017).

[90] 45 C.F.R. § 164.502(a)(5) (2017).

[91] 45 C.F.R. § 164.502(d)(2) (2017).

[92] 45 C.F.R. § 164.502(g) (2017).

[93] 45 C.F.R. Part 164, §§ 510 512 (2017).

[94] 45 C.F.R. § 164.502(a)(1) (2017).

[95] *See e.g.*, 45 C.F.R. Part 164, §§ 510 512 (2017); OCR."Research" (*last updated* June 5, 2013), *available at*: https://www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html; OCR Disclosures for Public Health Activities (2003), *available at* http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/publichealth/publichealth.pdf; OCR Research: 45 C.F.R. Part 164 §§ 501, 508, 512(i) (2003), *available at* http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/research/research.pdf; OCR Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care (2015), *available at* http://www.hhs.gov/sites/default/files/provider_ffg.pdf.

[96] Disclosures for these purposes are not subject to the minimum necessary limitation (45 C.F.R. § 164.502(b)(2)(i) (2017)).

General Purpose of Covered Entity Disclosure	To Whom a Covered Entity May Disclose—and Relevant Limitations
For healthcare operations purposes	To any entity for its own healthcare operations purposes or to another Covered Entity for certain of the receiving CE's healthcare operations purposes, if both parties have/had a relationship with the patient and the PHI pertains to that relationship
	To any entity in the form of a limited data set, if the Covered Entity and the intended recipient first execute a valid Data Use Agreement
As required by law	To a government authority about a patient who the entity reasonably believes to be a victim of abuse, neglect, or domestic violence
	In the course of any judicial or administrative proceeding, in response to an order, subpoena, discovery request, or other lawful process
	To a law enforcement official for limited purposes (e.g., suspect identification, reporting crime on premises, about suspected victims of crime)
For public health activities	To a public health authority that is legally authorized to collect the PHI to control or prevent disease, injury, or disability
	To an authorized government entity to report child abuse or neglect
	To an FDA-regulated entity about an FDA-regulated product or activity for quality, safety, or effectiveness activities
	To a person who may have been exposed to or be at risk of contracting or spreading a communicable disease
	To an employer about an employee if the entity is providing health care to the employee at the employer's request in order to conduct an evaluation relating to workplace medical surveillance or to evaluate whether an employee has a work-related illness or injury
	Proof of immunization information to a school about a student or prospective student
	To anyone the provider believes can lessen or prevent a serious and imminent threat to an individual or the public
	To any entity in the form of a limited data set, if the Covered Entity and the intended recipient first execute a valid Data Use Agreement
For health oversight activities	To a health oversight agency[97] for legally authorized oversight activities
About decedents	To coroners and medical examiners to identify a deceased person, determine cause of death, or other legally authorized duties
	To a funeral director to carry out their legally authorized duties
	To organ procurement organizations for the purpose of facilitating donations and transplantations

[97] A health oversight agency is defined by HIPAA as "an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant" (45 C.F.R. § 164.501 (2017)).

General Purpose of Covered Entity Disclosure	To Whom a Covered Entity May Disclose—and Relevant Limitations
For research purposes	To researchers as authorized by an IRB or Privacy Board for limited, specific research purposes
	To any entity in the form of a limited data set, if the Covered Entity and the intended recipient first execute a valid Data Use Agreement
For specialized government functions	About Armed Forces personnel where disclosure is deemed necessary by appropriate military authorities to execute military missions
	To authorized federal officials for national security and intelligence activities
	To authorized federal officials for the provision of protective services to the President
	To a correctional institution or law enforcement officer about an inmate or an individual in lawful custody
For worker's compensation	To entities legally authorized to receive such information for purposes of providing benefits for work-related injuries or illnesses
For directory purposes	To anyone identifying the patient by name,[98] if information disclosed is limited to location in the facility and general health status
For involvement in the patient's care	To any family member, close friend, or patient-designated representative to the extent that the information disclosed is directly relevant to the recipient's involvement with the patient's care or payment for care[99]
For notification, identification, or location of person responsible for patient's care	To any entity, if the information disclosed is limited to the patient's location and general health status or death.
Disclosures incident to any permitted or required disclosures	To any entity if the provider has in place reasonable safeguards to protect the privacy of patient information

The Privacy Rule requires that most permissive exception disclosures be limited to the "minimum [amount of PHI] necessary" to achieve the purpose for which the information was released or

[98] Providers must inform patients of directory disclosures and give them the opportunity to object to such disclosures or restrict them (may be accomplished via the provider's Notice of Privacy Practices or a verbal acknowledgement) (45 C.F.R. § 164.510(a)(2) (2017)). If patient is incapacitated, provider may make directory disclosures, but as soon as practicable, must inform patient of such disclosures and give patient the opportunity to object to or restrict further disclosures (45 C.F.R. § 164.510(a)(3) (2017)).

[99] Providers must give patients the opportunity to agree or object to such disclosures, by obtaining the patient's verbal or written approval, giving the patient the opportunity to object verbally or in writing, or inferring, based on professional judgment, that the patient does not object to such a disclosure and that disclosure is in the patient's best interest (45 C.F.R. § 164.510(b)(2) (2017)). If the patient is incapacitated, the provider may disclose if, using professional judgment, s/he determines that it is in the patient's best interest (45 C.F.R. § 164.510(b)(3) (2017)).

requested.[100] Determining what amount is the "minimum necessary" is at the discretion of the Covered Entity making the disclosure, using professional judgment under the circumstances.[101] Note, however, that the disclosing Covered Entity may rely on the intended recipient's request as the minimum necessary for the stated purpose when the requestor is: (1) another Covered Entity; (2) a member of the disclosing Covered Entity's workforce; (3) a public official for a purpose permitted under § 164.512; (4) a researcher acting in compliance with § 164.512(i); or (5) an entity providing professional services to the disclosing Covered Entity as its Business Associate.[102] The minimum necessary limitation does not apply to a disclosure made without authorization when required by law, to a provider for treatment purposes, or to the Secretary for compliance or enforcement purposes nor to disclosures made to the individual subject of the information or pursuant to an individual's authorization.[103]

Other than an individual's request for access, which is a required disclosure, it is important to underscore the permissive nature of the rest of these exceptions—the Covered Entity may, but is not required to, make disclosures without authorization for these specified purposes. If it is the Covered Entity's custom or common practice to first obtain written authorization for any disclosure (other than those required by the Rule), the Covered Entity may choose to maintain that custom or practice. However, such custom or practice is not mandated by the Privacy Rule, nor is there a HIPAA penalty for making use of these exceptions (or declining to do so). If a Covered Entity does or plans to make certain permissive disclosures, it must specify the general types of disclosures in its Notice of Privacy Practices (NPP), which it must make available to all individuals. While the Privacy Rule gives providers the flexibility to utilize permissive exceptions in accordance with their own customs and preferences (so long as safeguards to protect such disclosures are followed), there are certain situations in which more restrictive standards apply:

1. A "more stringent"[104] state law prohibits certain disclosures without express authorization (e.g., information related to HIV/AIDS or mental illness);
2. The PHI is a substance abuse treatment record governed by 42 C.F.R. Part 2;
3. The Covered Entity is subject to more restrictive federal standards governing privacy and confidentiality (e.g., Title X grantees and Community Health Centers); or
4. The information is held in a record covered by FERPA.

---

[100] 45 C.F.R. § 164.502(b) (2017).

[101] The Privacy Rule specifies limited circumstances in which a Covered Entity is permitted to rely on a requested disclosure as the minimum necessary (assuming such reliance is reasonable under the circumstances) (45 C.F.R. § 164.514(d)(3)(iii) (2017)). These circumstances include: (1) disclosures to public officials permitted under § 164.512; (2) information requested by another Covered Entity; (3) requests made by a professional who is member of its workforce for purposes of providing professional services to the Covered Entity; (4) requests made by its Business Associate for the purpose of providing professional services to the Covered Entity; (5) research disclosures under § 164.512, if appropriate documentation has been provided.

[102] 45 C.F.R. § 164.514(d)(3)(iii) (2017).

[103] 45 C.F.R. § 164.502(b)(2) (2017).

[104] 45 C.F.R. § 160.203(b) (2017).

Common Rule: In order for researchers to collect or use an individual's information for research, every entity involved in the research process must comply with requirements set forth in Subpart A.

1. Research Institutions. Every institution engaged in non-exempt research must submit a written assurance stating that it will comply with the Common Rule's requirements.[105] Federal departments and agencies also have authority to enforce Common Rule compliance directly against IRBs operated by institutions that do not hold a written assurance.[106] Where research takes place at an institution in which IRB oversight is conducted by an IRB not operated by that institution, the institution and the organization operating the IRB must document the institution's reliance on the IRB for research oversight and the responsibilities each entity will undertake to ensure compliance with the Common Rule's requirements.[107]

2. Institutional Review Boards (IRBs). An IRB must review and approve all non-exempt research protocols in accordance with Common Rule requirements,[108] such as determining that, where appropriate, there are adequate provisions to protect subjects' privacy and to maintain data confidentiality.[109] IRBs also must review research at least annually or—as determined by the IRB[110]—more frequently, depending on the degree of risk involved[111] (IRBs may use an expedited review process for eligible research activities,[112] including for exempt research protocols where limited review is required as a condition of exemption[113]).

Beginning on January 20, 2020,[114] all institutions engaged in cooperative research (with very limited exceptions) must rely on a single IRB for study approval.[115]

Part 2: Disclosure of Part 2 patient identifying information without written consent is permitted for limited purposes, including:

---

[105] 82 Fed. Reg. 7149 at 7259 (to be codified at 45 C.F.R. § 46.103).

[106] 82 Fed. Reg. 7149 at 7259 (to be codified at 45 C.F.R. § 46.101(a)).

[107] 82 Fed. Reg. 7149 at 7261 (to be codified at 45 C.F.R. § 46.103(e)).

[108] 82 Fed. Reg. 7149 at 7263 (to be codified at 45 C.F.R. § 46.109(a)).

[109] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.111(a)(7)).

[110] 82 Fed. Reg. 7149 at 7263 (to be codified at 45 C.F.R. § 46.108(a)(3)(i)).

[111] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.109(e)).

[112] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.110(b)) (Note: expedited review is available for: (1) research appearing on the list of categories published by the HHS Secretary in the Federal Register and available through OHRP unless the reviewer determines that the study involves more than minimal risk; (2) minor changes in previously approved research during the period for which approval is authorized; and (3) research for which limited review is a condition of exemption).

[113] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.110).

[114] 82 Fed. Reg. 7149 at 7259 (to be codified at 45 C.F.R. § 46.101(l)(2)).

[115] 82 Fed. Reg. 7149 at 7265 (to be codified at 45 C.F.R. § 46.114(b)(1)).

1. To medical personnel who need the information to treat a patient during a medical emergency in which the patient's prior informed consent could not be obtained;[116]
2. By the program or other lawful holder of Part 2 data for purposes of conducting scientific research, if the Part 2 program director determines that the information recipient meets one or both of the following requirements, as applicable:
    a. Is a HIPAA Regulated Entity and has obtained patient authorization or a HIPAA-compliant authorization waiver or alteration; and/or
    b. Is subject to the Common Rule and provides documentation that the recipient is in compliance with the Common Rule or is conducting research exempt from the Common Rule.[117]
3. By scientific researchers using data obtained from a Part 2 program in research reports, if the data is in aggregate form and all patient identifying information has been rendered non-identifiable.[118]
4. To certain specified entities for audit and evaluation activities of the program;[119]
5. To the parent, guardian, or authorized representative of a minor applicant for substance use disorder service of facts relevant to reducing a substantial threat to the life or physical well-being of any individual if the program director determines that the disclosure may reduce such a threat and that the minor lacks capacity to consent to the disclosure;[120] and
6. By the program director about a patient (other than a minor patient or those adjudicated incompetent) who has a medical condition that prevents knowing or effective action on their own behalf for purposes of obtaining payment for services from a third-party payer.[121]

Researchers using patient identifying information obtained from a Part 2 program may request linkages to data sets from a data repository holding patient identifying information if the request is reviewed and approved by an IRB registered with HHS.[122]

This includes disclosing whether an individual is or has been a patient with the program.[123] The restrictions on disclosure also apply to individuals and entities that have received patient records directly from Part 2 programs or from other lawful holders of patient identifying information and who have been properly notified of the prohibition on re-disclosure.[124]

---

[116] 42 C.F.R. § 2.51(a)(1) (2017).

[117] 42 C.F.R. § 2.52(a) (2017).

[118] 42 C.F.R. § 2.52(b)(3) (2017).

[119] 42 C.F.R. § 2.53 (2017).

[120] 42 C.F.R. § 2.14(c) (2017).

[121] 42 C.F.R. § 2.15(a)(2) (2017).

[122] 42 C.F.R. § 2.52(c)(1)(i) (2017).

[123] 42 C.F.R. § 2.13(c)(1) (2017)

[124] 42 C.F.R. § 2.12(d)(2)(i) (2017).

GINA: Title I prohibits health plans and health insurance issuers from using genetic information to make eligibility, coverage, underwriting, or premium-setting decisions about covered individuals.[125] Generally, health plans and issuers may not request or require that beneficiaries undergo genetic testing or provide genetic information.[126] However, health plans may request that beneficiaries voluntarily provide genetic information for research, require genetic information for determining medical appropriateness of covered services, and obtain genetic information incidentally in the course of obtaining other information.[127]

Title II of GINA prohibits employers from using genetic information to discriminate against employees or applicants[128] and generally may not acquire employee or applicant genetic information,[129] subject to exceptions that are limited to legitimate business purposes. Title II also governs the confidentiality of acquired genetic information. Genetic information must be kept confidential and in a medical record separate from the employee's personnel file.[130] Genetic information may be disclosed to the employee at his or her written request and in several other circumstances, including:

1. To an occupational or health researcher; and
2. To a public health organization, if the information concerns a contagious disease that presents an imminent threat of serious harm or death and the employee is informed of the disclosure.[131]

Privacy Act of 1974: The Privacy Act allows a federal agency to release individually identifiable information to identified individuals (or to their designees with written consent) or pursuant to one of 12 exemptions for disclosure.[132] These exemptions include disclosure to federal agency employees, the Census Bureau, the National Archives and Records Administration, other government entities for civil and criminal law enforcement purposes, the Comptroller General, Congress or its committees, and a consumer reporting agency. Additional exemptions include disclosures for statistical research, disclosures required by FOIA, disclosures in response to emergency circumstances, and disclosures pursuant to a court order. In addition, research is commonly included as a permitted release under agency systems of records (SORs). FOIA requires federal executive agencies to disclose their records to individuals upon request, subject to nine exemptions. These exemptions prevent the disclosure of information that is considered sensitive or of a personal nature, including information about a specific individual contained in personnel or medical files, the disclosure of which would be an "unwarranted invasion of personal privacy."[133]

---

[125] *See, e.g.* GINA Title I, § 102(a)(4) (2008) (Note: GINA does not apply to life insurance, casualty insurance, or long term care insurance).

[126] *See, e.g.* GINA Title I, § 101(b) (2008).

[127] *See, e.g.* GINA Title I, § 101(b) (2008).

[128] *See, e.g.* GINA Title II, § 202(a), codified at 42 U.S.C. 2000ff-1(a) (2008).

[129] *See, e.g.* GINA Title II, § 202(a), codified at 42 U.S.C. 2000ff-1(a) (2008).

[130] GINA Title II, § 206(a), codified at 42 U.S.C. 2000ff-5(a) (2008).

[131] GINA Title II, § 206(b), codified at 42 U.S.C. 2000ff-5(b) (2008).

[132] 5 U.S.C. § 552a(b) (1974).

[133] 5 U.S.C. § 552(b)(6) (1974).

Family Educational Rights and Privacy Act (FERPA): An educational agency or institution (or its agent) may disclose "education records" without written consent in several circumstances, which include:

1. When released to authorized representatives of the Comptroller General, the Attorney General, the Secretary of Education, or state and local educational authorities;
2. When a disclosure is required by law, judicial order, or subpoena;
3. When the disclosure is to accrediting organizations to perform accrediting functions;
4. When disclosed to organizations that conduct studies related to: predictive test development, validation, or administration; student aid program administration; and instructional improvements for or on behalf of educational agencies or institutions;
5. When disclosed to Department of Agriculture or Food and Nutrition Services representatives that need the information to monitor and evaluate the child nutrition programs; and
6. When disclosure is needed in an emergency to protect the health and safety of the student or others; and
7. To a parent about their postsecondary student's violation of any federal, state, or local law or institutional rule or policy governing the use or possession of alcohol or a controlled substance, if the student is under 21 at the time of disclosure (unless such disclosure is prohibited by state law).[134]

Consent/Authorization

Information may be accessed and used without the individual subject's approval for certain purposes and in certain circumstances. Beyond these situations, privacy and/or human subjects protection laws generally require entities like researchers and providers to obtain the individual's consent or authorization prior to collecting, using, or sharing data about that individual. Whether consent or authorization is necessary will depend upon the content of the data and the purposes for collecting or sharing the data. Consent/authorization procedures generally require notifying individuals of the intended uses and disclosures of their information and having individuals execute a document stating that they consent to or authorize the uses or disclosures of their information. Additional protections or considerations related to consent or authorization may apply where the subject is a special class (e.g., minor, pregnant woman, prisoner, etc.). In general, the term "consent" is used to refer to informed consent to participate in research (a concept governed by the Common Rule). Authorization is used to refer to authorization given by an individual subject of information to an entity to disclose that information to a third party. Authorization is a term used in HIPAA, and here it is used to encompass all similar permissions (e.g., as they apply to Part 2, GINA, etc.). Specific requirements that pertain to the content of an authorization to disclose information or an informed consent form are provided in Table 3 below.

[134] 34 C.F.R. § 99.31 (2017).

Table 3: Federal Requirements for Consent to Disclose Identifiable Health Information

Federal Requirements	HIPAA[135]	Common Rule[136]	GINA[137]	Part 2[138]	Privacy Act[139] (HHS)
Required elements:					
Patient's name				X	
Specific description of information[140]	X	X	X	X	X
Identify person(s) or entity authorized to make the requested disclosure	X			X	
Identify person(s) or entity authorized to receive the requested information	X	X	X	X	X
Describe the intended use(s) of the requested information[141]	X	X	X	X	X
The expiration date or event	X	X		X	
Date signed	X	X		X	
Signature (and/or electronic signature where acceptable) of the individual or his/her personal representative	X	X		X	
Provide the following information:					
The individual's right to withdraw authorization (if any) and any applicable exceptions to that right.	X	X		X	
Whether any benefits may be conditioned on releasing the information and applicable consequences of refusal to consent. This includes stating that refusal will involve no penalty or loss of benefits where relevant.	X	X	X		

[135] 45 C.F.R. §164.508(c)(1) (2017).

[136] 45 C.F.R. Part 46 §§ 116(a),117(a) (2017).

[137] GINA Title II, § 206(b), 42 U.S.C. 2000ff-5(b) (2017).

[138] 42 C.F.R. § 2.31(a) (2017).

[139] 5 U.S.C. § 552a (as amended) (2017).

[140] Note that for a consent under Part 2, the information to be disclosed must be limited to the minimum amount of information necessary to accomplish the stated purpose of the disclosure (42 C.F.R. § 2.31(a)(5) (2017)).

[141] Note that in the case of an authorization for use or disclosure of PHI for future research purposes, the authorization must adequately describe such purposes so that it would be reasonable for the individual to expect his or her PHI could be used for such future research (OCR. Final Rule: Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 82 Fed. Reg. 5566 at 5612 (2013)).

Federal Requirements	HIPAA	Common Rule	GINA	Part 2	Privacy Act (HHS)
The potential for re-disclosure of the information (if any). This includes stating that information may not be re-disclosed without further authorization, where applicable.	X	X		X	
Other requirements:					
The authorization must be written in plain language.	X	X			
Provide the individual with a copy of the form.	X	X			

Key Statutes and Regulations Related to Consent/Authorization

Health Insurance Portability and Accountability Act (HIPAA): As a threshold matter, the Privacy Rule requires written authorization for any disclosure except those required by the Rule. Where a personal representative is authorized to act on behalf of the individual (discussed above in section on Subjects), the personal representative may execute a valid authorization.

Common Rule: In general, an individual must give specific informed consent to participate in research before the research may begin.[142] The primary researcher must comply with several requirements related to obtaining and documenting informed consent, including providing specific information about the research protocol to potential participants.[143] IRBs may waive or alter some or all informed consent requirements under certain circumstances.[144] Note that there is a different set of waiver and alteration criteria and requirements for research involving public benefit or service programs conducted by or subject to the approval of state or local officials.[145]

An IRB may approve a research proposal in which an investigator will obtain identifiable private information without informed consent for the purpose of "screening, recruiting, or determining eligibility" of prospective subjects, if the investigator will obtain the information through oral or written communication with the prospective subject or by accessing records or stored identifiable biospecimens.[146] In addition to including standard elements in the informed consent, investigators must also provide specific information where it is relevant to the research protocol.[147] This includes informing the participant about the following:

---

[142] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.111(a)(4)).

[143] 82 Fed. Reg. 7149 at 7265-67 (to be codified at 45 C.F.R. § 46.116).

[144] 82 Fed. Reg. 7149 at 7267 (to be codified at 45 C.F.R. § 46.116(f)).

[145] 82 Fed. Reg. 7149 at 7267 (to be codified at 45 C.F.R. § 46.116(e)) (Note: this is distinct from research and demonstrations projects conducted or supported by a federal department or agency that are designed to study, evaluate, improve, or examine public benefit or service programs, which are exempt from Common Rule requirements entirely (*see* 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(5)).

[146] 82 Fed. Reg. 7149 at 7267 (to be codified at 45 C.F.R. § 46.116(g)).

[147] 82 Fed. Reg. 7149 at 7266 (to be codified at 45 C.F.R. § 46.116(c)).

1. Biospecimens may be used for commercial profit and whether the participant will or will not share in such profit;[148]
2. Whether or not clinically relevant research results, including individual research results, will be disclosed to participants and, if so, under what conditions;[149] and
3. For research involving biospecimens, whether the research will or might include whole genome sequencing.[150]

Broad consent is a special kind of informed consent required for certain secondary use of identifiable biospecimens and identifiable private information (in addition to other requirements—see above sections discussing exemptions). Because a secondary use is a use other than that for which the biospecimen or private information was originally collected, researchers may seek a participant's consent to future unspecified research during the initial informed consent process. Where participants give such "broad consent," additional informed consent would not be required for the same or another researcher to use the information or biospecimens collected during the original research study. Researchers may rely on broad consent to conduct studies on stored information or biospecimens in lieu of seeking IRB waiver of the specific informed consent requirement. Broad consent incorporates some parts of the specific informed consent process, such as rules governing how consent can be obtained[151] and requirements for information that must be provided to the subject,[152] and includes requirements for provision of information specific to secondary use.[153]

Part 2: Part 2 bars most disclosures of that information without written consent by the patient and/or his/her personal representative.[154] This includes disclosing whether an individual is or has been a patient with the program.[155] Programs may disclose substance use disorder patient information with valid written consent from the patient.[156] There are certain other requirements for consent in special circumstances (e.g., minors, disclosures to central registries, etc.). A valid consent must include nine separate elements (see Table 3),[157] including identification of the intended recipient of the information. If the intended recipient is an individual, an entity with a treating relationship with the patient, or a third-party payer, the consent must specifically name the recipient.[158] If the recipient is an entity without

---

[148] 82 Fed. Reg. 7149 at 7266 (to be codified at 45 C.F.R. § 46.116(c)(7)).

[149] 82 Fed. Reg. 7149 at 7266 (to be codified at 45 C.F.R. § 46.116(c)(8)).

[150] 82 Fed. Reg. 7149 at 7266 (to be codified at 45 C.F.R. § 46.116(c)(9)).

[151] 82 Fed. Reg. 7149 at 7265-66 (to be codified at 45 C.F.R. § 46.116(a)(1)-(4), (6)).

[152] 82 Fed. Reg. 7149 at 7266 (to be codified at 45 C.F.R. § 46.116(d)(1)).

[153] 82 Fed. Reg. 7149 at 7266-67 (to be codified at 45 C.F.R. § 46.116(d)(2)-(7)).

[154] 42 C.F.R. §§ 2.2(b)(1) and 2.13 (2017).

[155] 42 C.F.R. § 2.13(c)(1) (2017).

[156] 42 C.F.R. § 2.33 (2017).

[157] 42 C.F.R. § 2.31(a) (2017).

[158] 42 C.F.R. § 2.31(a)(4)(i), (ii), and (iii)(A) (2017).

a treating relationship with the patient (other than a third-party payer), the consent must give the entity's name *and:*

- The name(s) of an individual participant with the entity (e.g., Dr. Smith, Research Scientist at Jones Research Institution);
- The name of an entity participant(s) with a treating provider relationship with the patient (e.g., Southeastern Hospital, member of Eastern HIO); or
- A general designation of an individual or entity participant or class of participants, limited to those with a treating provider relationship with the patient (e.g., all current and future treating providers at Northern Academic Medical Center).[159]

Part 2 allows minors to consent to disclosure if their state grants minors the legal capacity to seek treatment without parental consent. In such states, only the minor can consent to information disclosure. If the state requires the minor to obtain parental consent before receiving substance abuse treatment, then both the minor and the parent/guardian must give written consent to disclosure (special rules apply when a minor lacks the capacity to make a rational choice). Note that there is no payment exception to the consent rule. That is, a provider must obtain the written consent of the minor (and the parent/guardian if the state does not give the minor capacity to consent to treatment) before disclosing information to a third-party payer.

GINA: Genetic information may be disclosed to the employee at his or her written request.

Privacy Act of 1974: The Privacy Act allows a federal agency to release individually identifiable information to identified individuals (or to their designees with written consent).

Family Educational Rights and Privacy Act (FERPA): An educational agency or institution (or its agent) may only disclose "education records" with written parental consent or the consent of a student age 18 or older or enrolled in a postsecondary institution, unless an exception applies.

Security

Security refers to the means by which data are protected from unauthorized use or access. Various federal laws and regulations set forth requirements for security measures that must be in place to protect identifiable health information. Security measures generally include technical, administrative, and physical safeguards. Technical safeguards include items such as encryption, firewalls, passwords, antivirus software, and SSL/TLS transmission. Physical safeguards include measures that limit an individual's access to facilities, workstations, and devices that house data or may be used to access data (e.g., policies that limit server room access to authorized personnel). Administrative safeguards include plans and policies for identifying security risks, preventing security breaches, monitoring security, remedying security breaches, and training employees on proper security procedures.

Key Statutes and Regulations Related to Security

Health Insurance Portability and Accountability Act (HIPAA): The Security Rule requires Regulated Entities to establish and maintain reasonable and appropriate administrative, physical, technical, and

[159] 42 C.F.R. § 2.31(a)(4)(iii)(B) (2017).

organizational safeguards for protecting PHI that the Regulated Entity creates, receives, maintains, or transmits in electronic form (known as e-PHI).[160]

Regulated Entities must:

1. Ensure the confidentiality, integrity, and availability of all e-PHI;
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
3. Protect against any reasonably anticipated uses or disclosures of e-PHI that are not permitted or required by the Privacy Rule; and
4. Ensure its workforce's compliance with the Security Rule.[161]

The Security Rule provides Regulated Entities considerable flexibility in meeting these requirements. Entities may use any security measure that allows them to reasonably and appropriately implement the Rule's standards and implementation specifications.[162] However, when deciding which security measures to use, an entity must always account for several factors, including: its size, complexity, and capabilities (including technical infrastructure, hardware, and software capabilities); the costs of security measures; and the probability and criticality of potential risks to e-PHI.[163]

Part 2: Part 2 programs and any other lawful holder of patient identifying information must have policies and procedures in place to protect against unauthorized uses and disclosures of information as well as any reasonably anticipated threats or hazards to the security of patient identifying information.[164] These policies must address transfer/transmission, removal, destruction, maintenance, use, and access with respect to paper and electronic records, as well as information de-identification and creation and receipt of electronic information.[165]

Legal Status

Legal Status refers to rights and responsibilities related to the data that may be triggered by ownership rights, agency principles, and/or contractual obligations. Legal status determines who may assert rights to that information. Individuals or entities with ownership interests may grant, restrict, or deny access to information. Contractual obligations, such as data use agreements, vendor contracts, or terms of service agreements, may apply. Principles of agency may give a researcher the rights and obligations of the healthcare organization that employs him or her. Finally, some state laws, such as consumer protection and patient privacy laws, may confer rights and responsibilities with respect to access to data or data held by researchers.

---

[160] 45 C.F.R. § 164.306 (2017).

[161] 45 C.F.R. § 164.306(a) (2017).

[162] 45 C.F.R. § 164.306(b)(1) (2017).

[163] 45 C.F.R. § 164.306(b)(2) (2017).

[164] 42 C.F.R. § 2.16(a) (2017).

[165] 42 C.F.R. § 2.16(a)(1)-(2) (2017).

Key Statutes and Regulations Related to Legal Status

Health Insurance Portability and Accountability Act (HIPAA): HIPAA sets forth requirements for Covered Entities to enter into contractual arrangements in certain circumstances.

A Covered Entity may permit a Business Associate to create, receive, maintain, or transmit PHI on the Covered Entity's behalf but must first enter into a written contract or similar arrangement (i.e., a Business Associate Agreement) with the Business Associate that meets relevant requirements.[166] The contract provides assurances that the Business Associate will appropriately safeguard the PHI and must include several provisions relating to the obligations of both parties.[167]

When disclosing a limited data set (LDS) without first obtaining the individual subject's authorization, which is permissible for purposes of research, healthcare operations, and public health functions and activities, the Covered Entity must enter into a data use agreement (DUA) with the intended recipient of the LDS.[168] A DUA provides assurances to the disclosing Covered Entity that the intended recipient of the LDS will only use or disclose that PHI for limited purposes and must contain certain of information.[169] If a Covered Entity knows of a pattern of activity or practice of the LDS recipient that constitutes a material breach or violation of the DUA, the Covered Entity must take reasonable steps to cure the breach or end the violation, as applicable.[170] If such steps are unsuccessful, the Covered Entity must discontinue PHI disclosures to the recipient and report the problem to the HHS Secretary.

State Law: A number of areas of state law may apply to health care and research, including the areas of consumer protection, privacy, research practices, and health information exchange. Some states have laws addressing ownership of health information in particular. States generally have laws governing allowable terms and enforcement of contracts. States may also have laws that address the creation of an agency relationship or the scope of an agent's authority, but interpretation of agency is typically left to courts. Contracts may include terms related to an agency relationship and terms as well.

---

[166] 45 C.F.R. Part 164 §§ 314(a) and 504(e) (2017).

[167] 45 C.F.R. § 164.504(e)(2) (2017).

[168] 45 C.F.R. § 164.514(e)(4)(i) (2017).

[169] 45 C.F.R. § 164.514(e)(4)(ii) (2017).

[170] 45 C.F.R. § 164.514(e)(4)(iii) (2017).