The Office of the National Coordinator for Health Information Technology

Legal and Ethical Architecture for PCOR Data

APPENDIX A: STATUTES AND REGULATIONS RELEVANT TO PCOR

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

This appendix includes summaries of the statutes and regulations discussed throughout the Architecture relevant to PCOR.

INTRODUCTION

Health care is one of the most highly regulated industries. The foundation of the U.S. healthcare system is patient and public health information that primarily supports patient and provider decision-making, payment, and research. Health information, even more so than financial information, is considered to be highly sensitive and protected by a vast array of federal and state statutes and regulations, organizational policies and procedures, and ethical considerations.

At the federal level, statutes and regulations may be organized by their primary focus. For example, some statutes and regulations are specific to the types of health information content they govern; others are specific to certain activities, such as research; and still others are specific to the settings of care where care is delivered.

Content-Specific Statutes and Regulations: These statutes and regulations govern certain specific types of health information that may be used to support PCOR and CER, assuming the relevant requirements are met. For example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations govern protected health information. Part 2 of Title 42 of the Code of Federal Regulations (Part 2) governs substance abuse information held by federally assisted programs, and the Genetic Information Nondiscrimination Act of 2008 (GINA) governs genetic information used for various purposes. These statutes and regulations are both permissive and prohibitive in nature, describing to whom and for what purposes these types of information may or may not be disclosed as well as any other associated requirements. Other content-specific statutes and regulations include: the Patient Safety and Quality Improvement Act (PSQIA—patient safety work product); the Privacy Act of 1974 (individually identifiable information held by a federal agency); and the [federal] Freedom of Information Act (FOIA).

Research-Specific Statutes and Regulations: These statutes and regulations govern the health-related research enterprise, including PCOR and CER if certain requirements are met. For example, the Common Rule governs federally supported human subjects research. Similar to the Common Rule, FDA regulations govern experiments on human subjects involving products, drugs, or devices subject to FDA review and/or approval.

Setting-Specific Statutes and Regulations: These statutes and regulations govern health information that is collected, used, and/or disclosed by certain settings of care. For example, Title 38 of the U.S. Code governs health care delivered to Veterans, Section 330 of the Public Health Services Act (PHSA) governs health care delivered in community health centers, and the Family Educational Rights and Privacy Act (FERPA) governs health information included in student education records.

Table 1: Federal Laws—Primary Focus

Federal Laws	Content-Specific	Research-Specific	Setting-Specific
Common Rule Subparts A–E		X	
FDA Research Regulations		X	
Family Educational Rights and Privacy Act (FERPA)			X
Genetic Information Nondiscrimination Act (GINA)	X		
HIPAA Administrative Regulations	X		
42 C.F.R. Part 2	X		
Public Health Services Act § 330 Grantees (Community Health Centers)			X
Patient Safety and Quality Information Act (PSQIA)	X		
Privacy Act of 1974/Freedom of Information Act (FOIA)	X		
Title X Providers (Family Planning Clinics)			X
Veteran's Administration Confidentiality Regulations (Title 38 USC § 7338)			X

At the state level, statutes and regulations that relate to health information vary greatly. For purposes of this project, the most relevant state statutes and regulations typically govern the privacy of health information for specific populations and specific types of information (e.g., individuals with HIV/AIDs, individuals with mental health conditions, and minors). For these populations, state laws are typically more stringent than HIPAA requirements and thus must be followed as they relate to the collection, use, and disclosure of health information for these individuals.

OVERVIEW OF FEDERAL LAWS: CONTENT-SPECIFIC

Health Insurance Portability and Accountability Act of 1996 (HIPAA)[335]

Purpose. HIPAA and its enabling regulations (the HIPAA Rules) set a national framework for the management, transmission, and disclosure of health information. At HIPAA's core lies an effort to balance individuals' right to control access by third parties to information about their health and health care against providers' and payers' need to exchange and manage this information for treatment, payment, and healthcare operations. As a result, HIPAA gives healthcare providers, payers, and clearinghouses considerable flexibility over information management and exchange, if done prudently, while at the same time giving individuals some ability to control information flow.

The U. S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) is responsible for implementing and enforcing four separate sets of HIPAA regulations:[336]

1. The Privacy Rule, which governs the privacy and confidentiality of individually identifiable health information;[337]
2. The Security Rule, which identifies baseline administrative, physical, and technical safeguards to protect electronic health information;[338]

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

[336] There are also general regulations that contain definitions and relevant technical specifications applicable to all four rules (45 C.F.R. Part 160, Subparts A and B) as well as general provisions applicable to the Privacy, Security, and Breach Notification Rules (45 C.F.R. Part 164, Subpart A).

[337] 45 C.F.R. Part 164, Subpart E (2017).

[338] 45 C.F.R. Part 164, Subpart C (2017).

3. The Enforcement Rule, which sets forth the enforcement system for all the HIPAA Rules;[339] and
4. The Breach Notification Rule, which establishes a notification and reporting protocol in the event of an unauthorized disclosure.[340]

Scope. The HIPAA Rules regulate "protected health information" (PHI). PHI is individually identifiable information that is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse that relates to:

1. The provision of care to an individual;
2. An individual's past, present, or future physical or mental health condition; or
3. An individual's payment for care, whether made in the past or present or expected in the future.[341]

Information is individually identifiable when it directly references an individual or could be used to identify the individual.[342] The HIPAA Rules do not govern Covered Entities' employment records or education records subject to FERPA[343]—even if those records contain health information.[344]

The HIPAA Rules apply to health plans, healthcare clearinghouses,[345] and all healthcare providers, regardless of size, that electronically transmit health information in connection with certain transactions[346]—collectively, these are known as "Covered Entities."[347] In addition, the HIPAA Rules apply to Covered Entities' "Business Associates," which are individuals or groups (other than members of the Covered Entity's workforce) that have access to PHI when providing certain services or functions to or on behalf of a Covered Entity.[348] Covered Entities and their Business Associates together are referred to as "Regulated Entities."[349] The HIPAA Rules do not apply to any other types of individuals or organizations.[350]

---

[339] 45 C.F.R. Part 160, Subparts C, D, and E (2017).
[340] 45 C.F.R. Part 164, Subpart D (2017).
[341] 45 C.F.R. § 160.103 at "Health information" (2017).
[342] 45 C.F.R. § 160.103 at "Individually identifiable health information" (2017).
[343] Note that HIPAA also does not apply to what FERPA defines as "treatment records" (see FERPA section for more information), which are excluded from FERPA's definition of "education records" (45 C.F.R. § 160.103 (2017), referencing 20 U.S.C. 1232g(a)(4)(B)(iv)).
[344] 45 C.F.R. § 160.103, at (2) of "Protected health information" (2017).
[345] 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 at "Healthcare clearinghouse" (2017)).
[346] Covered transactions include, but are not limited to, benefit eligibility inquiries and claims (45 C.F.R. Part 162 (2017)).
[347] 45 C.F.R. § 160.103 at "Covered Entity" (2017).
[348] 45 C.F.R. § 160.103 at "Business Associate" (2017). Note that 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.
[349] *See, e.g.* U.S. Department of Health and Human Services (HHS) Office for Civil Rights (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).
[350] The healthcare component of a hybrid entity (defined by HIPAA as: "a single legal entity that is a covered entity whose business associate activities include both covered and non-covered functions and that designates healthcare components in accordance with [relevant HIPAA provisions]" (45 C.F.R. § 164.103 (2017))) is subject to all HIPAA requirements applicable to Covered Entities to the extent that it performs covered functions.

Information De-Identification

Health information that has been de-identified is not considered to be PHI for purposes of HIPAA applicability.[351] Information can be de-identified under HIPAA in either of two ways:

1. Safe Harbor Method:[352] Information is de-identified under this method when all of 18 direct identifiers are removed (*see* Table 2: Federal Requirements for Consent to Disclose Identifiable Health Information). However, information is not de-identified under this method if the Covered Entity knows that the information (stripped of these 18 identifiers) could still be used, alone or in combination with other information, to identify the individual.
2. Statistical/Expert Method:[353] Under this method, an individual with sufficient knowledge in and experience with statistical and scientific methods and principles for de-identifying information must analyze the information. Information is considered de-identified when the expert individual, after applying these methods and principles, determines that there is very small risk that an anticipated recipient could identify an individual either from the information alone or in combination with other available information.

When information has been de-identified, regardless of the method employed, a Regulated Entity may assign a code or use another means of record identification that allows the information to be re-identified, if certain criteria are met:

1. The code may not be derived from or related to information about the individual;
2. It must be impossible for the code to be translated so as to identify the individual;
3. The Regulated Entity may not use or disclose the code for any purpose; and
4. The Regulated Entity may not disclose the mechanism for re-identification.[354]

Although HIPAA's methods are the only federal standards available for de-identifying information, concerns regarding the potential to re-identify "de-identified" data have arisen due to the increase in data collection from all facets of life, the aggregation and sale of such data, and advances in computer science and machine learning.[355] The subjective nature of the expert determination method and the susceptibility of information de-identified via the Safe Harbor method to the "mosaic effect" (whereby data from multiple sources can be pieced together to obtain private information) raise concerns about the efficacy of both HIPAA methods for de-identification.

Recognizing these concerns, the Health Information Technology Policy Committee (HITPC) Privacy and Security Workgroup's August 2015 Health Big Data Recommendations included the following recommendations for addressing the risk of re-identification:

1. Enable the Office for Civil Rights (OCR—the HHS office that enforces the HIPAA Rules) to take an active role in managing the HIPAA de-identification standards, including methodology review,

[351] 45 C.F.R. § 160.103 at "Covered Entity" (2017); 45 C.F.R. Part 164 §§ 302, 400, 500(a) (2017).
[352] 45 C.F.R. § 164.514(b)(2)(i) (2017).
[353] 45 C.F.R. § 164.514(b)(1) (2017).
[354] 45 C.F.R. § 164.514(c) (2017).
[355] *See* Paul Ohm Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA Law Rev. 1701 (2010).

recommending updates to methodologies and policies, and obtaining the assistance of third-party experts (e.g., the National Institute of Standards and Technology);
2. Develop programs to evaluate the ability of statistical methodologies to reduce re-identification risks to "very low;" and
3. Encourage the use of proven de-identification methods by having OCR assign Safe Harbor status to methods that prove effective within specific contexts.[356]

The Privacy Rule

Purpose. The HIPAA Privacy Rule's dual purpose is to regulate the use and disclosure of PHI by Regulated Entities and to establish an individual's rights with respect to their own PHI held by a Covered Entity. Although the Privacy Rule establishes important safeguards for health information privacy, the Rule is fundamentally and intentionally designed to create a privacy "operating system" for the core of the American healthcare system. This approach to health information management protects information while still enabling stakeholders to engage in the types of information exchange vital to health care and the overall operation of the healthcare system. In particular, the Privacy Rule gives significant latitude to exchange information among providers of clinical care and between providers and insurers for essential health care functions. The Privacy Rule was initially published in 2000 and then later updated in 2002 and 2013.

Scope. The Privacy Rule regulates all PHI held or transmitted by a Covered Entity or its Business Associate, in any form or medium (electronic, paper, or oral).[357] The 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 a designated representative) upon his/her request for access and to HHS for enforcement purposes and for HIPAA-related compliance investigations;[358]
2. Prohibited Disclosures: a Regulated Entity may not disclose PHI for certain purposes (e.g., most sales of PHI[359]) and may only disclose certain types of PHI (e.g., psychotherapy notes,[360] minors' PHI[361]) in limited circumstances;
3. Permissive Disclosures (*see* Table 4: List of Permissive Exceptions Available to Covered Entities): 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 an informal opportunity to object to the disclosure[362]);[363]

---

[356] Health Information Technology Policy Committee (HITPC) Privacy and Security Workgroup Health Big Data Recommendations at 14 (2015), available at: https://www.healthit.gov/sites/faca/files/HITPC_Health_Big_Data_Report_FINAL.pdf.

[357] 45 C.F.R. § 164.502(d)(2) (2017).

[358] 45 C.F.R. § 164.502(a)(2) (2017).

[359] 45 C.F.R. § 164.502(a)(5) (2017). Note: a Covered Entity may sell PHI after obtaining the individual subject's valid written authorization for such sale, if the authorization states the disclosure of PHI will result in remuneration to the Covered Entity (45 C.F.R. § 164.508(a)(4) (2017)).

[360] 45 C.F.R. § 164.508(a)(2) (2017).

[361] 45 C.F.R. § 164.502(g) (2017).

[362] 45 C.F.R. § 164.510 (2017).

[363] 45 C.F.R. § 164.512 (2017); *see also* HHS Office for the National Coordinator for Health Information Technology (ONC) and OCR Permitted Uses and Disclosures: Exchange for Treatment (2016), *available at* http://www.hhs.gov/sites/default/files/exchange_treatment.pdf; ONC and OCR Permitted Uses and Disclosures: Exchange for Health Care Operations (2016), *available at* http://www.hhs.gov/sites/default/files/exchange_health_care_ops.pdf.

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.[364]

The Privacy Rule requires written authorization for any disclosure except those required or permitted by the Rule. The permissive disclosure exceptions to the authorization requirement are critical to enable proper functioning of the healthcare system. For example, the exception permitting disclosure without authorization for treatment purposes allows a health center to provide a specialist with a patient's entire medical record upon request, enabling the specialist to fully understand the patient's medical condition and provide the most appropriate treatment. To balance Regulated Entities' legitimate needs to exchange PHI with patients' interest in the privacy of their information, the Privacy Rule requires that most disclosures be limited to the "minimum [amount of PHI] necessary" to achieve the purpose for which the information was released or requested.[365] Determining what amount is the "minimum necessary" is at the discretion of the Covered Entity making the disclosure, using professional judgment under the circumstances.[366] The requirement to limit disclosures to the minimum amount necessary does not apply to disclosures without authorization that are required by [state or other] law, made to a provider for treatment purposes, or made to the Secretary for compliance or enforcement purposes nor to disclosures made to the individual subject of the PHI or made pursuant to an individual's authorization.[367]

It is important to underscore the permissive nature 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 some or all otherwise-permitted disclosures, 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 the permissive exceptions (or declining to do so). While the Privacy Rule gives providers the flexibility to utilize permissive exceptions in accordance with their own customs and preferences (when certain safeguards are employed, such as the minimum necessary standard), there are specific situations in which more restrictive standards apply:

1. A "more stringent"[368] 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.

---

[364] 45 C.F.R. § 164.502(a)(1) (2017).
[365] 45 C.F.R. § 164.502(b) (2017).
[366] 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.
[367] 45 C.F.R. § 164.502(b)(2) (2017).
[368] 45 C.F.R. § 160.203(b) (2017).

The Security Rule

Purpose. The Security Rule requires Regulated Entities to establish and maintain reasonable and appropriate administrative, physical, technical, and organizational safeguards for protecting PHI that the Regulated Entity creates, receives, maintains, or transmits in electronic form (known as e-PHI).[369]

Scope. 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 complies with the Security Rule.[370]

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.[371] 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.[372]

The Enforcement Rule

Purpose. The Enforcement Rule governs the HIPAA enforcement process, establishing protocols for compliance investigations, hearings, and penalties for violations.

Scope. The Enforcement Rule does not give individuals the right to sue Regulated Entities whom they believe have violated the provisions of the HIPAA Rules.[373] Instead, the Rule allows aggrieved individuals to file a complaint with OCR.[374] OCR may investigate complaints, and an investigation is required when a preliminary review of the facts indicates a possible violation due to willful neglect.[375] The Enforcement Rule utilizes a four-tiered penalty structure to correspond to the levels of culpability associated with a HIPAA violation.[376] Regulated Entities that violate the HIPAA Privacy, Security, and Breach Notification Rules may be liable for penalties up to $1.65 million[377] per violation category, per year (subject to annual increase for inflation), depending on their level of culpability.[378]

---

[369] 45 C.F.R. § 164.306 (2017).
[370] 45 C.F.R. § 164.306(a) (2017).
[371] 45 C.F.R. § 164.306(b)(1) (2017).
[372] 45 C.F.R. § 164.306(b)(2) (2017).
[373] Note that § 13410(e) of the Health Information Technology for Clinical Health (HITECH) Act, a part of the American Recovery and Reinvestment Act of 2009 (ARRA), gave State Attorneys General authority to bring civil actions on behalf of their state's residents for violations of the HIPAA Privacy and Security Rules (ARRA, Pub. L. No. 111-5, 115 Stat. 123 at Div. A, Title XIII, 123 Stat. 271-76 (2009)).
[374] 45 C.F.R. § 160.306(a) (2017).
[375] 45 C.F.R. § 160.306(c) (2017).
[376] 45 C.F.R. § 160.404 (2017).
[377] The violation amount is adjusted on an annual basis in accordance with inflation (45 C.F.R. § 160.404(a) (2017)).
[378] 45 C.F.R. § 160.404 (2017).

The Breach Notification Rule

Purpose. The Breach Notification Rule requires Regulated Entities to disclose breaches of unsecured PHI (PHI in any form or medium that has not been rendered "unusable, unreadable, or indecipherable to unauthorized individuals" [379]) to the individuals affected, the HHS Secretary, and, in certain circumstances, the media.

Scope. A breach of unsecured PHI is a use or disclosure that is impermissible under the Privacy Rule and that "compromises the security or privacy of the [PHI]." Any disclosure that is impermissible under the Privacy Rule is presumed to be a breach unless the Regulated Entity conducts a risk assessment that demonstrates a low probability that the PHI was compromised.[380] In the event of a breach, the Regulated Entity must provide notification to the affected individuals that includes a description of the breach and the type of PHI involved and what the Covered Entity is doing to investigate the breach, mitigate losses, and protect against further breaches.[381] The Regulated Entity must also concurrently notify the HHS Secretary of the breach,[382] and in some cases must notify relevant media outlets.[383] The notification requirements are not applicable in certain situations, such as where a disclosure was made in good faith to an otherwise-authorized member of the Regulated Entity's workforce.[384]

42 C.F.R. Part 2 (Substance Abuse Information) [385]

Purpose. Part Two of Title 42 of the Code of Federal Regulations (C.F.R.) governs the confidentiality of substance use disorder patient records obtained by federally assisted programs. These protections exist to ensure that individuals in a substance abuse treatment program are not more vulnerable with respect to their privacy than those who do not seek treatment.[386]

The Part 2 regulations were issued in 1970 and updated in 1987. In 2016, the Substance Abuse and Mental Health Services Administration (SAMHSA) proposed several major modifications to better align the regulations with the current U.S. healthcare system.[387] SAMHSA finalized changes to Part 2 in a Final Rulemaking issued on January 18, 2017.[388] The finalized changes to Part 2 went into effect on March 21, 2017; these changes are reflected in the summary below. 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.[389] Future changes may be made to Part 2, and researchers and other stakeholders should continue to monitor the status of Part 2.

---

[379] 45 C.F.R. § 164.402 (2017).
[380] 45 C.F.R. § 164.402 (2017).
[381] 45 C.F.R. § 164.404(a)(1) (2017).
[382] 45 C.F.R. § 164.408(a) (2017). Notice to the HHS Secretary must be in the manner specified on HHS's website.
[383] 45 C.F.R. § 164.406(a) (2017).
[384] 45 C.F.R. § 164.402 (2017).
[385] 42 C.F.R. Part 2 (2017).
[386] 42 C.F.R. § 2.2(b)(2) (2017).
[387] U.S. Department of Health and Human Services, 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).
[388] SAMHSA Supplemental Notice of Proposed Rulemaking: Confidentiality of Substance Use Disorder Patient Records ("Part 2 Supplemental NPRM") 82 Fed. Reg. 6052 (2017).
[389] SAMHSA Final Rule: Confidentiality of Substance Use Disorder Patient Records ("Part 2 Final Rule") 82 Fed. Reg. 5485 (2017).

Scope. The Part 2 regulations govern the disclosure and use of certain information maintained by "federally assisted" substance use disorder programs.[390] 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, is certified to provide addiction services—any activity that would lead one to conclude that the individual or entity provides substance use disorder services[391]); 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.[392]

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).[393]

There are several situations in which the Part 2 regulations do not apply. Relevant exemptions include:

1. Veteran's Administration (VA): substance use disorder patient information maintained in connection with the VA's provision of services to a veteran with a service-related disability (this information is covered by VA-specific regulations, discussed below);
2. Program Communications: communication of information within a Part 2 program or between a Part 2 program and an entity with direct administrative control over that program,[394] to the extent the information is needed by personnel in connection with providing substance use disorder services;
3. Qualified Service Organizations (QSOs)[395]: communication of information between a Part 2 program and a QSO where the QSO needs the information to provide services to the program; [396] and
4. Vital Statistics: disclosures of information relating to a patient's cause of death in accordance with laws that require death or other vital statistics collection or that permit cause of death inquiries.[397]

Part 2 restricts disclosure of all information, whether recorded or not, obtained by a Part 2 program for purposes of providing substance use disorder services that would identify a patient as having or having had a substance use disorder, either through direct or indirect identification (i.e., by reference to other

---

[390] 42 C.F.R. § 2.2(a) (2017).

[391] 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.

[392] 42 C.F.R. § 2.11 at "Program" (2017).

[393] 42 C.F.R. § 2.12(b) (2017).

[394] Note that entities with direct administrative control over Part 2 programs are subject to the Part 2 disclosure restrictions with respect to the information communicated to them by the Part 2 program (42 C.F.R. § 2.12(d)(2)(i)(B) (2017)).

[395] A QSO is an individual or entity that provides professional services (e.g., data processing, dosage preparation, population health management, legal services, etc.) or services to prevent or treat child abuse or neglect to a Part 2 program (42 C.F.R. § 2.11 at "Qualified service organization" ¶ (1) (2017)). A QSO must have a written agreement with the program in which the QSO acknowledges that it is bound by the Part 2 regulations and agrees to resist any efforts to obtain access to patient records in judicial proceedings except as permitted by Part 2. (42 C.F.R. § 2.11 "Qualified service organization" (2) (2017)).

[396] 42 C.F.R. § 2.12(c) (2017).

[397] 42 C.F.R. § 2.15(b)(1) (2017).

publicly available information or through verification of such an identification by another person).[398] Part 2 bars most disclosures of that information without written consent by the patient and/or his/her personal representative.[399] This includes disclosing whether an individual is or has been a patient with the program.[400] 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.[401]

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

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;[402]
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.[403]

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.[404]
4. To certain specified entities for audit and evaluation activities of the program;[405]
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;[406] 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.[407]

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 Institutional Review Board (IRB) registered with HHS.[408] After providing a researcher with

[398] 42 C.F.R. § 2.12(a)(1) (2017).
[399] 42 C.F.R. Part 2 §§ 2(b)(1) and 13 (2017).
[400] 42 C.F.R. § 2.13(c)(1) (2017).
[401] 42 C.F.R. § 2.12(d)(2)(i) (2017).
[402] 42 C.F.R. § 2.51(a)(1) (2017).
[403] 42 C.F.R. § 2.52(a) (2017).
[404] 42 C.F.R. § 2.52(b)(3) (2017).
[405] 42 C.F.R. § 2.53 (2017).
[406] 42 C.F.R. § 2.14(c) (2017).
[407] 42 C.F.R. § 2.15(a)(2) (2017).
[408] 42 C.F.R. § 2.52(c)(1)(i) (2017).

linked data, the data repository must destroy or delete the linked data from its records to render the information non-retrievable.[409]

Programs may disclose substance use disorder patient information with valid written consent from the patient.[410] 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 2: Federal Requirements for Consent to Disclose Identifiable Health Information),[411] 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.[412] If the recipient is an entity without 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).[413]

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.[414] 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.[415]

Genetic Information Nondiscrimination Act of 2008 (GINA)[416]

Purpose. GINA protects individuals'[417] genetic information[418] from being used by employers, health plans, and health insurance issuers in a discriminatory manner. GINA does not apply to life insurance plans, long-term care plan issuers, or disability insurers.

[409] 42 C.F.R. § 2.52(c)(2)(i) (2017).
[410] 42 C.F.R. § 2.33 (2017).
[411] 42 C.F.R. § 2.31(a) (2017).
[412] 42 C.F.R. § 2.31(a)(4)(i),(ii), and (iii)(A) (2017).
[413] 42 C.F.R. § 2.31(a)(4)(iii)(B) (2017).
[414] 42 C.F.R. § 2.16(a) (2017).
[415] 42 C.F.R. § 2.16(a)(1), (2) (2017).
[416] Genetic Information Nondiscrimination Act of 2008 (GINA), Pub. L. No. 110-233, 122 Stat. 881 (Title I amended scattered provisions of 29 U.S.C. §§ 1182 *et seq.*, 42 U.S.C. §§ 300gg-1 *et seq.*, 42 U.S.C. § 1395ss, 42 U.S.C. § 1320d-9, and 26 U.S.C. §§ 9802 *et seq*; Title II is codified at 42 U.S.C. §§ 2000f *et seq*.); implementing regulations found throughout multiple titles of the C.F.R.
[417] 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).
[418] "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)).

Scope. GINA is comprised of two titles. 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.[419] Generally, health plans and issuers may not request or require that beneficiaries undergo genetic testing or provide genetic information.[420] 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.[421]

Title II prohibits most employers[422] from using genetic information to discriminate against employees or applicants[423] and generally prohibits employers from acquiring employee's or applicant's genetic information,[424] subject to exceptions that are limited to legitimate business purposes. Title II also governs the confidentiality of lawfully acquired genetic information. Genetic information must be kept confidential and stored in a medical record separate from the employee's personnel file.[425] Genetic information may be disclosed to the employee at his or her written request and without the employee's consent 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.[426]

Patient Safety and Quality Improvement Act of 2005 (PSQIA)[427]

Purpose. PSQIA was enacted in response to concerns about patient safety and *To Err is Human: Building a Safer Health System* (a 1999 Institute of Medicine Report) and aims to encourage reporting of adverse events in order to improve patient safety.[428]

Scope. PSQIA protects patient safety work product (PSWP), which includes data, reports, records, memoranda, analyses, or statements that could result in improved patient safety, healthcare quality, or healthcare outcomes.[429] PSQIA established a voluntary reporting program where providers share PSWP with Patient Safety Organizations (PSOs), which aggregate and analyze the information.[430] Identifiable

---

[419] *See, e.g.* GINA Title I, § 102(a)(4) (2008).

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

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

[422] Title II does not apply to employers with fewer than 15 employees.

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

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

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

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

[427] PSQIA, Pub. L. No. 109-41, 119 Stat. 424 (2005) (amending scattered sections of the Public Health Services Act (PHSA), 42 U.S.C. §§ 299 *et seq*.).

[428] HHS Agency for Healthcare Research and Quality (AHRQ) "Patient Safety and Quality Improvement Act of 2005" (2008), *available at*: http://archive.ahrq.gov/news/newsroom/press-releases/2008/psoact.html

[429] PSQIA, 42 U.S.C. § 299b-21(7)(A) (2005).

[430] PSQIA, 42 U.S.C. § 299b-21(6) (2005).

PSWP is subject to privilege and confidentiality requirements, each of which have specific exceptions that permit disclosure under certain circumstances, including:

1. To carry out patient safety activities;
2. If the PSWP is non-identifiable, whether voluntarily disclosed or not;
3. By a provider to the FDA with respect to a product or activity regulated by the FDA;
4. To entities carrying out research, evaluation, or demonstration projects authorized, funded, certified, or otherwise sanctioned by HHS; and
5. For business operations if disclosure is consistent with the goals of patient safety improvement.[431]

Privacy Act of 1974[432] and Freedom of Information Act (FOIA)[433]

Purpose. The Privacy Act protects information about individuals (e.g., patients and practitioners) held or collected by the federal government that can be retrieved by a personal identifier (e.g., name, Social Security number). FOIA permits disclosure of information contained within a federal agency record, unless the information is exempted from disclosure.

Scope. 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.[434] 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) that each collecting agency establishes (see Common Rule exemption categories below for further discussion of information in SORs used for research). 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."[435] The 21st Century Cures Act explicitly prohibits the use of FOIA to gain access to an individual's biomedical information—if there is even a very small risk that individual biomedical research data could be used to identify an individual, HHS may prevent such data from being publicly disclosed under a FOIA request.

[431] PSQIA, 42 U.S.C. § 299b-22(c)(2) (2005).
[432] The Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified at 5 U.S.C. § 552a).
[433] The Freedom of Information Act (FOIA), Pub. L. No. 89-487, 80 Stat. 250 (updated as amended by Pub. l. No. 114-185, 130 Stat. 538) (amending 5 U.S.C. § 552) (2016).
[434] 5 U.S.C. § 552a(b) (1974).
[435] 5 U.S.C. § 552(b)(6) (2016).

OVERVIEW OF FEDERAL LAWS: RESEARCH-SPECIFIC

Common Rule[436]

Purpose. The Protection of Human Subjects regulations set forth a variety of requirements to ensure that human subjects (i.e., research participants) experience minimal risk to their health, safety, and privacy during and as a result of federally supported research. There are four separate regulations (Subparts A–D), created and adopted by HHS in 1991. Subpart A is known as "the Common Rule" because it has been codified by 15 federal departments/agencies and informally adopted by three federal agencies.

In an effort to modernize the Common Rule and harmonize its provisions with other federal privacy regulations, the Common Rule departments and agencies proposed significant changes to the regulations in a 2015 NPRM.[437] 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).[438] The summary below reflects the 2017 Final Rule provisions. Future changes may be made to the regulations, and researchers and other stakeholders should continue to monitor the status of the Common Rule.

Scope. **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.[439] Research (i.e., a systematic investigation designed to develop or contribute to generalizable knowledge)[440] 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.[441] Information about behavior where an individual can reasonably expect that no observation or recording is taking place as well as information provided for specific purposes that the individual can reasonably expect will not be made public is private information.[442] Information and biospecimens are identifiable if the individual's identity is or may be readily ascertained by the investigator or associated with the information or biospecimen.[443] Note that unlike the HIPAA Privacy Rule, the Common Rule does not specify identifiable elements of information, though does require that federal departments and agencies regularly consult with experts to reexamine and, as appropriate, alter the interpretation of identifiability.[444]

[436] 45 C.F.R. Part 46, Subparts A-E (2017).
[437] "Common Rule" Departments and Agencies, Notice of Proposed Rulemaking: Federal Policy for the Protection of Human Subjects, 80 Fed. Reg. 53933 (2015).
[438] "Common Rule" Departments and Agencies, Final Rule: Federal Policy for the Protection of Human Subjects, 82 Fed. Reg. 7149 (2017).
[439] 82 Fed. Reg. 7149 at 7259 (to be codified at 45 C.F.R. § 46.101(a)).
[440] 82 Fed. Reg. 7149 at 7260-61 (to be codified at 45 C.F.R. § 46.102(l)).
[441] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(e)(1)).
[442] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(e)(4)).
[443] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(e)(5), (6)).
[444] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(e)(7)(i)).

The Common Rule specifically excludes some activities from its definition of research; these activities are not subject to any provisions of the Common Rule.[445] For example, public health surveillance activities, including the collection and testing of information or biospecimens, which are conducted, supported, requested, ordered, required, or authorized by a public health authority are not considered "research" for purposes of Common Rule applicability.[446]

The Common Rule also exempts some types of research from its requirements;[447] the Office for Human Research Protections (OHRP, an office within HHS) strongly recommends that an Institutional Review Board (IRB) or administrative review process be utilized to determine whether proposed research is considered exempt.[448] Research meeting any of the following definitions is not subject to any Common Rule requirements:

1. Research that only involves interactions using educational tests, survey procedures, interview procedures, or observation of public behavior[449] or that involves benign behavioral interventions[450] in conjunction with information collection from an adult participant (if the participant prospectively agrees to the intervention and information collection)[451] if:

    a. The researcher records information so that the participant's identity cannot be readily ascertained (directly or through linked identifiers); and/or
    b. Disclosure of a participant's responses outside the research 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 publicly available identifiable private information or identifiable biospecimens;[452]
3. Secondary research use of identifiable private information or identifiable biospecimens if the researcher records the information so that the subject's identity cannot be readily ascertained (directly or through linked identifiers), does not contact the subject, and will not re-identify the subject;[453]
4. Secondary research use of identifiable private information or identifiable biospecimens (limited to information collection and analysis) if such use is regulated under the HIPAA Privacy Rule for the purposes of "health care operations" or "research," or for "public health activities and purposes";[454]

---

[445] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(l)).
[446] 82 Fed. Reg. 7149 at 7261 (to be codified at 45 C.F.R. § 46.102(l)(2)).
[447] 82 Fed. Reg. 7149 at 7261 (to be codified at 45 C.F.R. § 46.104).
[448] HHS Office for Human Research Protections (OHRP), Exempt Research and Research That May Undergo Expedited Review [Number 95-02] (1995), *available at*: http://www.hhs.gov/ohrp/regulations-and-policy/guidance/exempt-research-and-research-expedited-review/index.html.
[449] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(2)).
[450] 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)).
[451] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(3)(i)).
[452] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(4)(i)).
[453] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(4)(ii)).
[454] 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)).

5. Secondary research use of identifiable private information or identifiable biospecimens conducted by or on behalf of a federal department or agency using government-generated or -collected information obtained for non-research activities and maintained in systems of records (SORs) subject to the Privacy Act of 1974,[455] if certain other requirements are met;[456] and
6. 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.[457]

The Common Rule also exempts some types of research from most, but not all, of its requirements. Research meeting the following definitions need only meet the requirements specified below:

1. Research that only involves interactions using educational tests, survey procedures, interview procedures, or observation of public behavior[458] or that involves benign behavioral interventions[459] in conjunction with information collection from an adult participant (if the participant prospectively agrees to the intervention and information collection)[460] if an IRB conducts a limited review of the research to determine that, when appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data;[461]
2. Storage or maintenance of identifiable private information or identifiable biospecimens for ***potential*** secondary research use if an IRB conducts a limited review and determines that:[462]

    a. Broad consent for such storage, maintenance, and secondary research use is obtained in accordance with relevant requirements;[463]
    b. Broad consent is appropriately documented or waiver of documentation is appropriate;[464] and
    c. If there is a change made in the way the information or biospecimens are stored or maintained for research purposes, there are adequate provisions to protect the privacy of participants and maintain the confidentiality of data;[465] and

---

[455] 5 U.S.C. § 552a (1974).

[456] 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*).

[457] 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).

[458] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(2)).

[459] 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)).

[460] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(3)(i)).

[461] 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).

[462] 82 Fed. Reg. 7149 at 7262-63 (to be codified at 45 C.F.R. § 46.104(d)(7)).

[463] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.111(a)(8)(i)).

[464] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.111(a)(8)(ii)).

[465] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.111(a)(8)(iii)).

3. Secondary research use of identifiable private information and identifiable biospecimens if:[466]

    a. Broad consent for the storage, maintenance, and secondary research use of the identifiable private information or identifiable biospecimens was obtained in accordance with relevant requirements;
    b. Documentation of informed consent or waiver of documentation of consent was obtained in accordance with relevant requirements;
    c. An IRB conducts a limited review and determines that the research to be conducted is within the scope of broad consent and that, when appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data; and
    d. The investigator does not include "returning individual research results to participants" as part of the study plan.

Note that research initially approved by an IRB prior to January 19, 2018, that was determined exempt or for which review was waived by a department or agency head[467] must comply with the regulations as published in the 2016 edition of the Code of Federal Regulations.[468] After the 2017 Final Rule goes into effect, institutions still engaged in such research may comply with the updated regulations if appropriate.

Subpart A specifies requirements for every entity involved in the research process, including:

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 regulations; the relevant federal department or agency will only conduct or support non-exempt research if it receives such an assurance and if the institution has properly certified that an IRB has reviewed and approved the research (unless the relevant department or agency has waived the certification requirement).[469] 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.[470]

    a. 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.[471]

2. Institutional Review Boards (IRBs). IRBs must comply with several specifications governing their membership,[472] operations,[473] recordkeeping,[474] and responsibilities.[475] An IRB must review and approve all non-exempt research protocols in accordance with Common Rule requirements,[476]

[466] 82 Fed. Reg. 7149 at 7263 (to be codified at 45 C.F.R. § 46.104(d)(8)).
[467] *See* 45 C.F.R. § 46.101(i) (2016).
[468] 82 Fed. Reg. 7149 at 7259 (to be codified at 45 C.F.R. § 46.101(l)(3)).
[469] 82 Fed. Reg. 7149 at 7259 (to be codified at 45 C.F.R. § 46.103).
[470] 82 Fed. Reg. 7149 at 7259 (to be codified at 45 C.F.R. § 46.101(a)).
[471] 82 Fed. Reg. 7149 at 7261 (to be codified at 45 C.F.R. § 46.103(e)).
[472] 82 Fed. Reg. 7149 at 7263 (to be codified at 45 C.F.R. § 46.107).
[473] 82 Fed. Reg. 7149 at 7263 (to be codified at 45 C.F.R. § 46.108).
[474] 82 Fed. Reg. 7149 at 7265 (to be codified at 45 C.F.R. § 46.115).
[475] 82 Fed. Reg. 7149 at 7263 (to be codified at 45 C.F.R. § 46.109).
[476] 82 Fed. Reg. 7149 at 7263 (to be codified at 45 C.F.R. § 46.109(a)).

including requirements related to subject selection, data monitoring, and informed consent.[477] IRBs may use an expedited review process for eligible research activities,[478] including for exempt research protocols where limited review is required as a condition of exemption.[479] IRBs must also conduct continuing review of most research at intervals appropriate to the degree of risk and no less than once a year.[480] Continuing review is not required for:[481]

a. Research eligible for expedited review (including exempt research protocols subject to limited review as a condition of exemption);
b. Research that has reached the data analysis stage and/or has progressed to accessing standard follow-up clinical data (to the extent that either or both activities were part of the IRB-approved study).

Beginning on January 20, 2020,[482] all institutions engaged in cooperative research must rely on a single IRB for study approval; the relevant federal department or agency will identify the reviewing IRB or approve it after its proposal by the lead institution.[483] Certain research is not subject to the cooperative IRB requirement, including research for which more than single IRB review is required by law (including tribal law) or for which any relevant federal department or agency determines a single IRB is not appropriate.[484] Where a cooperative research project is not subject to the cooperative IRB requirement, participating institutions may enter into a joint review arrangement, rely on the review of another IRB, or make similar arrangements to avoid effort duplication.[485]

Informed Consent

In general, an individual must give specific informed consent to participate in research before the research may begin.[486] 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.[487] IRBs may waive or alter some or all informed consent requirements under certain circumstances.[488] 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.[489] An IRB may approve a research proposal in which an

[477] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.111).
[478] 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).
[479] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.110).
[480] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.109(e)).
[481] 82 Fed. Reg. 7149 at 7263 (to be codified at 45 C.F.R. § 46.109(f)(1)).
[482] 82 Fed. Reg. 7149 at 7259 (to be codified at 45 C.F.R. § 46.101(l)(2)).
[483] 82 Fed. Reg. 7149 at 7265 (to be codified at 45 C.F.R. § 46.114(b)(1)).
[484] 82 Fed. Reg. 7149 at 7265 (to be codified at 45 C.F.R. § 46.114(b)(2)).
[485] 82 Fed. Reg. 7149 at 7265 (to be codified at 45 C.F.R. § 46.114(c)).
[486] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.111(a)(4)).
[487] 82 Fed. Reg. 7149 at 7265-67 (to be codified at 45 C.F.R. § 46.116).
[488] 82 Fed. Reg. 7149 at 7267 (to be codified at 45 C.F.R. § 46.116(f)).
[489] 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)).

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.[490] In addition to including standard elements in the informed consent, investigators must also provide specific information where it is relevant to the research protocol.[491] This includes informing the participant about the following:

1. Biospecimens may be used for commercial profit and whether the participant will or will not share in such profit;[492]
2. Whether or not clinically relevant research results, including individual research results, will be disclosed to participants and, if so, under what conditions;[493] and
3. For research involving biospecimens, whether the research will or might include whole genome sequencing.[494]

Broad Consent

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 section 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[495] and requirements for information that must be provided to the subject,[496] and includes requirements for provision of information specific to secondary use.[497]

Subparts B–D add to (or modify) Subpart A requirements for federally supported research that involves certain vulnerable populations.

1. Subpart B applies to all research that involves pregnant women, human fetuses, neonates of uncertain viability, or nonviable neonates.[498] Note that all the exemptions available under Subpart A are available to research subject to Subpart B;[499]
2. Subpart C applies to all biomedical and behavioral research where the participants include prisoners.[500] Note that none of the exemptions available under Subpart A are available to research

[490] 82 Fed. Reg. 7149 at 7267 (to be codified at 45 C.F.R. § 46.116(g))
[491] 82 Fed. Reg. 7149 at 7266 (to be codified at 45 C.F.R. § 46.116(c)).
[492] 82 Fed. Reg. 7149 at 7266 (to be codified at 45 C.F.R. § 46.116(c)(7)).
[493] 82 Fed. Reg. 7149 at 7266 (to be codified at 45 C.F.R. § 46.116(c)(8)).
[494] 82 Fed. Reg. 7149 at 7266 (to be codified at 45 C.F.R. § 46.116(c)(9)).
[495] 82 Fed. Reg. 7149 at 7265-66 (to be codified at 45 C.F.R. § 46.116(a)(1)-(4), (6)).
[496] 82 Fed. Reg. 7149 at 7266 (to be codified at 45 C.F.R. § 46.116(d)(1)).
[497] 82 Fed. Reg. 7149 at 7266-67 (to be codified at 45 C.F.R. § 46.116(d)(2)-(7)).
[498] 45 C.F.R. § 46.201(a) (2017).
[499] 82 Fed. Reg. 7149 at 7261 (to be codified at 45 C.F.R. § 46.104(b)(1)).
[500] 45 C.F.R. § 46.301(a) (2017).

subject to Subpart C (except for research aimed at a broad population that only incidentally includes prisoners);[501] and
3. Subpart D applies to all research involving children as participants.[502] Note that some of the exemptions available under Subpart A are available to research subject to Subpart C.[503]

Note that there is a **Subpart E**, which governs IRB registration with the federal government and is not technically part of the "Common Rule," as it applies government-wide. Note also that Subparts B–E were not amended in conjunction with the 2017 Final Rule that changed Subpart A. However, HHS has expressed its intent to eventually amend Subparts B-E to the extent appropriate to modernize those provisions.[504]

U.S. Food and Drug Administration (FDA) Regulations[505]

Purpose. The FDA has not adopted the Common Rule's regulations protecting human participants. Instead, the FDA has implemented multiple regulations that generally mirror the Common Rule's provisions, with some notable differences. The FDA regulations govern experiments on human participants involving products, drugs, or devices subject to FDA review and/or approval.

Note that the FDA research regulations were not amended in conjunction with the 2017 Final Rule that modified the Common Rule Subpart A. However, HHS has expressed its intent to eventually update FDA regulations to the extent appropriate to modernize its provisions and align it with changes made to the Common Rule.[506] Further, the 21st Century Cures Act requires the Secretary to harmonize the differences between Subpart A of the Common Rule and the FDA's human subject regulations.[507]

Scope. 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 50 and 56 govern all experiments involving a human participant(s) that require prior FDA approval or the results of which require FDA investigation—these, like Subpart A, are broad and generally apply to most types of research under FDA's purview. Like the Common Rule, the FDA regulations establish requirements and responsibilities for IRBs and requirements for obtaining and documenting informed consent, including requirements for children (i.e., Subpart D). Some key differences between these regulations and Subpart A include:

1. The FDA has singular authority to waive any requirements in its regulations (e.g., IRBs do not have the authority to waive or modify the review or consent process).[508]
2. Waiver of consent is permitted in emergency circumstances without prior approval;[509]

---

[501] 82 Fed. Reg. 7149 at 7261 (to be codified at 45 C.F.R. § 46.104(b)(2)).
[502] 45 C.F.R. § 46.401(a) (2017).
[503] 82 Fed. Reg. 7149 at 7261 (to be codified at 45 C.F.R. § 46.104(b)(3)).
[504] 82 Fed. Reg. 7149 at 7151 (2017).
[505] Title 21 C.F.R. Parts 50, 54, 56, 312, 812, 814 (2017).
[506] 82 Fed. Reg. 7149 at 7151 (2017).
[507] 21st Century Cures Act, Pub. L. No. 114-255, 130 Stat. 1033, 1098-99, § 2063(b) (*codified at* 42 U.S.C. § 289) (2016).
[508] Title 21 C.F.R. § 56.105 (2017).
[509] 21 C.F.R. § 50.23(a)-(c) (2017).

3. Waiver of consent for investigational drug or device trials is permitted if the proposed clinical tests pose no more than minimal risk to [human] participants and includes appropriate safeguards to protect participants' rights, safety, and welfare;[510]
4. The FDA does not use the FWA mechanism;[511] and
5. The FDA defines "human subject" as a participant in research, whether as a recipient of the "test article" or the control (i.e., FDA does not govern information about an individual obtained from a secondary source).[512]

The 21st Century Cures Act directed the FDA to allow multisite and cooperative research projects to use single IRB review, in line with the 2017 Final Rule changes made to the Common Rule Subpart A.

Part 54 governs researchers' financial disclosures to the research sponsor; Parts 312 (clinical investigations of new drugs), 812 (clinical investigations of devices), and 814 (clinical investigations of Humanitarian Use Devices (HUD)[513]) all contain requirements that are in addition to or modify the requirements of Parts 50 and 56.

HIPAA, Common Rule, and Research

Purpose. The HIPAA Rules apply only to Regulated Entities (defined and discussed above) and thus are primarily relevant in relation to healthcare treatment, payment, and operations. However, because a Covered Entity may itself conduct research or be a resource for research (such as by supplying data for researchers to use), the HIPAA Privacy Rule establishes requirements for research involving a Covered Entity.

Scope. HIPAA does not mandate informed consent for research participation, leaving those requirements to the Common Rule. In general, as with any disclosure not required, permitted, or prohibited by the Privacy Rule, most disclosures of PHI for research purposes require written authorization from the individual subject of the PHI. However, PHI disclosure without authorization is permitted for research purposes (regardless of funding, unlike the Common Rule and FDA human participants protections)[514] in the following four circumstances:

1. The researcher needs the PHI only to prepare for research (e.g., develop a research protocol) and the PHI will not be physically removed from the Covered Entity;[515]
2. The only PHI sought is decedents' PHI, the researcher can provide documentation of those individuals' death (upon request), and the PHI is necessary for the research;[516] and

[510] 21st Century Cures Act, 130 Stat. 1099, § 3024 at (a) (*amending* 21 U.S.C. § 360j(g)(3)) and (b) (*amending* 21 U.S.C. § 355(i)(4)) (2016).
[511] 21 C.F.R. § 56.103 (2017).
[512] 21 C.F.R. § 50.3 (2017).
[513] 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.
[514] 45 C.F.R. § 164.512(i) (2017).
[515] 45 C.F.R. § 164.512(i)(1)(ii) (2017) (Note that the 21st Century Cures Act requires the HHS Secretary to issue guidance clarifying that remote access to PHI for research purposes is permitted so long as applicable privacy and security safeguards are maintained and the PHI is not copied or otherwise retained by the researcher (130 Stat. 1080-81, § 2063 at (a) (*codified at* 42 U.S.C. § 1320d-2, note)).
[516] 45 C.F.R. § 164.512(i)(1)(iii) (2017).

3. The disclosure is of a limited data set (LDS),[517] which is information with 16 identifiers removed but that is still considered PHI.[518] The Covered Entity and the intended recipient of the LDS (the researcher) must first enter into a data use agreement (DUA) that meets multiple criteria regarding safeguards the researcher will employ to protect the PHI.[519] Note that an LDS may also be used or disclosed without authorization for healthcare operations purposes or public health activities and purposes.

4. An IRB or Privacy Board approves a partial or full waiver or alteration of the authorization requirement.[520] Note that a waiver or alteration can only be approved if the use of the PHI presents a minimal risk to individuals' privacy and the research could not be practicably conducted without the waiver/alteration or access to the PHI. The Privacy Rule explicitly requires IRBs to follow relevant Common Rule regulations[521] and sets forth requirements for Privacy Boards related to the review process and board structure.[522]

Non-exempt research subject to the Common Rule would still require informed consent even if HIPAA would not require the researcher to obtain an authorization to use or disclose the participant's PHI. Changes made to the Common Rule in the 2017 Final Rule created an exemption for research covered by the HIPAA Privacy Rule. Researchers may, without obtaining a subject's informed or broad consent, conduct secondary research involving the collection and analysis of the subject's private identifiable information or identifiable biospecimens when such use is regulated under the Privacy Rule for purposes of research, healthcare operations, or public health activities and purposes.[523] This exemption category is scheduled to take effect on January 18, 2018. The HIPAA Privacy Rule governs entities using information and protects an individual's information only if the information holder or user (in this case, a researcher) is a Regulated Entity. A researcher that is not affiliated with a Regulated Entity (e.g., employed by a private research institution or the non-covered component of a hybrid Covered Entity) is not subject to HIPAA, even when using information obtained from a Regulated Entity (including, but not limited to, use of a limited data set). Thus, this Common Rule provision likely only exempts secondary research use of identifiable information and biospecimens when the researcher is a Regulated Entity. However, the updated regulations are not explicit that this is the case, and institutions may interpret the provision differently. Note that there are other Common Rule exemptions for secondary research uses of identifiable information and biospecimens, which are associated with other requirements and limitations.

---

[517] 45 C.F.R. § 164.514(e)(3) (2017).
[518] 45 C.F.R. § 164.514(e)(2) (2017).
[519] 45 C.F.R. § 164.514(e)(4) (2017).
[520] 45 C.F.R. § 164.512(i)(2)(ii) (2017). (Note: waivers or alterations may only be approved if the use or disclosure of PHI involves no more than minimal risk to individuals' privacy. Minimal risk exists where the following elements exist: (1) an adequate plan to protect identifiers from improper use and disclosure; (2) an adequate plan to destroy the identifiers at the earliest opportunity consistent with the conduct of the research (absent a health or research justification for retaining the identifiers or a legal requirement to retain the identifiers); (3) adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of PHI would be permitted by the Privacy Rule; (4) the research could not practicably be conducted without a waiver or alteration; and (5) the research could not be practicably conducted without access to and use of the PHI (45 C.F.R. § 164.512(i)(2)(ii)(A) (2017))).
[521] 45 C.F.R. § 164.512(i)(2)(iv)(A) (2017).
[522] 45 C.F.R. § 164.512(i)(1)(i)(B) (2017).
[523] There are six "public health activities and purposes" for which PHI may be used or disclosed without individual authorization (*defined at* 45 C.F.R. § 164.512(b) (2017)).

Where the Common Rule requires a researcher to have obtained broad consent for secondary use of identifiable private information or identifiable biospecimens, HIPAA would also require the researcher to obtain an authorization to disclose the information (if HIPAA applies to that researcher) unless such requirement is waived or altered by an IRB or Privacy Board. However, the Privacy Rule allows researchers to obtain an authorization for future research purposes "so long as the authorization adequately describes [as the purpose of the requested use or disclosure] the future research such that it would be reasonable for the individual to expect that his or her [PHI] could be used or disclosed for such future research."[524] Thus, when a researcher is obtaining a participant's broad consent for secondary use of information or biospecimens, the researcher may simultaneously seek the participant's authorization to disclose that information for such future research. Note that a valid authorization for research-related disclosures need not include an expiration date or event (as is required for all other authorizations under the Privacy Rule).[525] However, the 21st Century Cures Act directed the Secretary of HHS to issue guidance on future research authorizations stating that such an authorization must either include a specific expiration date or event or provide instructions on how to revoke the authorization.

Another relevant provision in the Privacy Rule permits the creation of compound authorizations in research contexts; that is, an authorization for use or disclosure of PHI for a research study (where the authorization requirement has not been waived or altered) may be combined with any other written permissions for the same or another research study, including:

1. Another authorization for the same research study (e.g., authorization to disclose PHI to another entity involved in the research);
2. A consent to participate in research (i.e., informed consent required by the Common Rule or the FDA regulations);
3. An authorization to create or maintain a research database or repository.[526]

OVERVIEW OF FEDERAL LAWS: SETTING-SPECIFIC

Confidentiality of Veterans Affairs Medical Records[527]

Purpose. All medical records pertaining to treatments or services for drug abuse, alcoholism/alcohol abuse, HIV, and/or sickle cell anemia that were provided by or performed on behalf of the U.S. Department of Veteran Affairs (VA) must be kept confidential.

Scope. These regulations apply to records that contain information regarding the identity, diagnosis, prognosis, or treatment of a patient or research participant and are maintained in relation to a program or activity pertaining to drug abuse, alcohol abuse, HIV, and/or sickle cell anemia.[528] Programs or activities can include education, training, treatment, rehabilitation, and research but must be

[524] OCR. Final Rule: Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules 78 Fed. Reg. 5566 at 5612 (January 25, 2013); *see also*,OCR. "Research" (*last updated* June 5, 2013), *available at*: https://www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html.

[525] 45 C.F.R. § 164.508(c)(1)(v) (2017).

[526] 45 C.F.R. § 164.508(b)(3) (2017).

[527] 38 U.S.C. § 7332 (codified as amended in 38 C.F.R. §§ 1.460 *et seq.*) (2017).

[528] 38 C.F.R. § 1.460 (2017).

administered by or performed on behalf of the VA in order for the records to fall within the scope of the confidentiality regulations.

In general, these records remain confidential even if the patient/participant is no longer a VA patient. The regulations require patients to issue written consent to release their records, though there are exceptions to this requirement, including:

1. Disclosure to medical personnel to respond to a medical emergency;[529]
2. Disclosure to qualified personnel to conduct scientific research,[530] perform management or financial audits, or evaluate programs (if results do not directly or indirectly identify individuals);[531]
3. Disclosure to federal, state, and/or local public health authorities to comply with HIV reporting laws;[532]
4. Where a patient lacks decision-making capacity, disclosure to a personal representative to make an informed treatment decision;[533] or
5. Disclosure to state controlled substance monitoring programs in order to prevent misuse of prescription medication.[534]

42 C.F.R. Part 2 expressly exempts from its regulations services provided by or performed on behalf of the U.S. Department of Veteran's Affairs. As a result, the VA's regulations, while covering more types of patients than Part 2 (i.e., those with HIV/AIDS and/or sickle cell anemia in addition to substance abuse patients), substantially mirrors Part 2's confidentiality protections, limiting disclosure without patient consent in similar manner.

Family Educational Rights and Privacy Act (FERPA)[535]

Purpose. The purpose of FERPA is to protect the privacy of student education records.

Scope. 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.[536] FERPA governs education records, which are "records, files documents, and other materials" that "contain information directly related to a student" and that "are maintained by an education agency or institution" or an entity acting as the agent of an institution.[537] Defining an "agent" of an institution is a matter of federal law but generally includes employees, contractors, and others working on behalf of or at the direction of the institution. FERPA treats elementary and secondary student health records, including immunization records, as education records. 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

[529] 38 C.F.R. § 1.485 (2017).
[530] 38 C.F.R. § 1.488 (2017).
[531] 38 C.F.R. § 1.489 (2017).
[532] 38 C.F.R. § 1.486 (2017) (Note that physicians and counselors may also disclose HIV information to a patient's sexual partner(s) if they believe the patient will not disclose the information themselves and disclosure is necessary to protect the health of their partner(s) (38 C.F.R. § 1.487 (2017))).
[533] 38 C.F.R. § 1.484 (2017).
[534] 38 C.F.R. § 1.483 (2017).
[535] FERPA of 1974 (codified at 20 U.S.C. § 1232g; implementing regulations at 34 C.F.R. Part 99 (2017)).
[536] 34 C.F.R. § 99.1 (2017).
[537] 34 C.F.R. § 99.3 (2017).

responsibilities and is subject to school direction). The term "education records" does *not* include the following records:[538]

1. Created by instructors, teachers, or administrators accessible only by the teacher or a substitute;
2. Created for law enforcement purposes by a law enforcement unit of an education agency;
3. Regarding educational agency or institution employees that are made in the normal course of business and only pertain to their employment; and
4. 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 exception or with written consent.

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. The main and most common exception to the FERPA written consent requirement is disclosure to a dependent child's parents. Other relevant exceptions 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 the disclosure is 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 the disclosure is to the 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).[539]

HIPAA Covered Entities Subject to More Stringent Requirements

There are several types of information that may be collected or used by a HIPAA Covered Entity but which are subject to more restrictive disclosure requirements than general PHI. For example, virtually all substance abuse treatment providers subject to Part 2 would be considered HIPAA Covered Entities; however, disclosure of substance abuse patient treatment records without patient consent is much more limited as compared to HIPAA's permissive disclosure exceptions. Because Part 2 is more protective of information, its requirements supersede HIPAA's where those requirements conflict.

Another example are providers funded under certain sections of the Public Health Services Act (PHSA), including family planning projects (awarded grants under Title X of the PHSA) and Community Health Centers (CHCs) (awarded grants under § 330 of PHSA). While both Title X grantees and CHCs are HIPAA Covered Entities, the enabling regulations for each type of entity limit disclosure of patient information

[538] 34 C.F.R. § 99.3 (2017).
[539] 34 C.F.R. § 99.31 (2017).

further than would otherwise be required under HIPAA. For Title X grantees, all information as to personal facts and circumstances about individuals receiving services must be held confidential and may not be disclosed without authorization except as is necessary to provide services or as is required by law.[540] CHCs may only disclose patient information without authorization as is required by law, for HHS audits, or as is necessary to provide services.[541] Note, however, that the definition of "services" under the CHC regulations is significantly broader in scope than the definition of treatment under HIPAA.

State Laws in General and Relationship to Federal Laws

Purpose. Providers and researchers must comply with any relevant federal requirements related to information disclosure and consent. In general, they also must comply with any state laws that are more protective of patients' rights, as well as any state laws governing data, patients, or entities not regulated by existing federal law. In some cases, there is a relationship between federal requirements and state laws such that they complement, rather than preempt, the other.

Scope. States typically provide enhanced protection for sensitive information (e.g., HIV/AIDS status, mental health information) and vulnerable populations (e.g., minors, legally incompetent adults). States also generally have laws governing state-based registries, compulsory health information reporting (e.g., communicable diseases, vital statistics), health insurers, public health entities, and provider licensure—all of which may contain requirements related to data sharing, confidentiality, and patient consent. Further, states often enact laws or regulations that offer more stringent protections than federal law, or that provide specific requirements implementing federal laws. For example, HIPAA provides individuals with the right to request and receive access to (most) of their PHI held by a Regulated Entity within 30 days at a reasonable cost-based fee.[542] States will often reduce the time frame in which Regulated Entities may provide access and/or will specify a fee structure for PHI access.[543]

One example of the relationship between federal and state laws exists in their treatment of minors. Federal laws often specifically reference minors' rights to privacy but defer to states for specifics, such as defining the age or circumstances of majority, setting the circumstances that trigger a minor's ability to consent to treatment or information disclosure, or defining parental and/or guardianship relationships and rights. Primary examples of the relationship between federal and state laws include:

HIPAA and Minors

The HIPAA Privacy Rule treats an unemancipated minor's parent, guardian, or other person acting *in loco parentis* as the minor's personal representative if state law gives such person authority to act on the minor's behalf in making health care decisions.[544] A personal representative stands in the shoes of the individual, meaning that the representative may request and obtain access to PHI, provide authorization for disclosures, and exercise any and all of the rights identified in the Privacy Rule. There are three circumstances in which a minor has the authority to act on his/her behalf: (1) when the minor consents

[540] 42 C.F.R. § 59.11 (2017).
[541] 42 C.F.R. § 51c.110 (2017).
[542] 45 C.F.R. § 164.524; *see also* OCR. "Individuals' Right under HIPAA to Access their Health Information 45 C.F.R. § 164.524" (*last updated* February 25, 2016), *available at* http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html
[543] *See, e.g.* Health Information & the Law. Individual Access to Medical Records: 50 State Comparison (2013), *available at* http://www.healthinfolaw.org/comparative-analysis/individual-access-medical-records-50-state-comparison
[544] 45 C.F.R. § 164.502 (2017).

to the health care service and no other consent is required by law; (2) in cases in which a minor may lawfully obtain the health care service without parental consent (e.g., contraceptive services); and (3) in situations in which the parent agrees that the health care provider and the minor may keep the information confidential.[545]

Part 2 and Minors

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.

[545] 45 C.F.R. § 164.502 (2017).

Table 2: Federal Requirements for Consent to Disclose Identifiable Health Information

	HIPAA[546]	Common Rule[547]	GINA[548]	Part 2[549]	Privacy Act[550] (HHS)
Required elements:					
Patient's name				X	
Specific description of information[551]	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[552]	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		
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			
Must provide the individual with a copy of the form.	X	X			

[546] 45 C.F.R. § 164.508(c)(1) (2017).
[547] 82 Fed. Reg. 7149 at 7265-68 (2017) (to be codified at 45 C.F.R. Part 46 §§ 116, 117).
[548] GINA Title II, § 206(b) (2008), 42 U.S.C. § 2000ff-5(b) (2017).
[549] 42 C.F.R. § 2.31(a) (2017).
[550] 5 U.S.C. § 552a (as amended) (2016).
[551] 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)).
[552] 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 (82 Fed. Reg. 5566 at 5612 (2013)).

Table 3: Safe Harbor Method of De-Identification

In order for PHI to be considered de-identified, the following 18 elements must be removed from the information as it relates to the individual subject of the information or to the individual's relatives, employers, or household member

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.

Table 4: List of HIPAA Permissive Exceptions Available to Covered Entities[553]

General Purpose of Covered Entity Disclosure	To Whom a Covered Entity May Disclose and Relevant Limitations
For treatment purposes[554]	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
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[554]	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

[553] *See, e.g.,* 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.

[554] 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 health oversight activities	To a health oversight agency[555] 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
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,[556] 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[557]
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[557]
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

[555] 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 healthcare 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)).

[556] 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)).

[557] 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)).

Table 5: Disclosures for Purposes of Treatment, Payment, and Healthcare Operations[558]

Activity		To Whom Covered Entity May Disclose	
Treatment	Providing, coordinating, or managing health care and related services by a provider(s)	To any entity, for the disclosing Covered Entity's own activities	To any entity for a healthcare provider's (need not be a Covered Entity) own activities
	Coordinating or managing health care by a provider with a third party		
	Consultation between providers relating to a patient		
	Referring a patient for health care from one provider to another		
Payment	Activities undertaken by a health plan[559] to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan, if the activities relate to the individual to whom health care is provided.[560]	To any entity, for the disclosing Covered Entity's own activities	To a healthcare provider (need not be a Covered Entity), for the receiving provider's own activities To any Covered Entity, for the receiving entity's own activities
	Activities undertaken by a healthcare provider or health plan[559] to obtain or provide reimbursement for the provision of health care, if the activities relate to the individual to whom health care is provided.[560]		
Healthcare Operations	Conducting quality assessment and improvement activities (e.g., outcomes evaluation and development of clinical guidelines) and related functions that do not include treatment, if the primary purpose of any studies resulting from such activities is **not** to obtain generalizable knowledge.	To any entity, for the disclosing Covered Entity's own activities	To any Covered Entity, for that entity's own activities IF: (1) The disclosing entity has or had a relationship with the subject of the PHI; (2) The recipient has or had a relationship with the subject of the PHI; and (3) the PHI pertains to these relationships.
	Patient safety activities[561] and related functions that do not include treatment		
	Population-based activities relating to improving health or reducing health care costs and related functions that do not include treatment.		

[558] OCR. "Research" (*last updated* June 5, 2013), *available at*: https://www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html.

[559] Health plans may not use or disclose PHI that is genetic information for underwriting purposes (45 C.F.R. § 164.502(a)(5)(i) (2017)).

[560] Such activities include, but are not limited to: (1) Determining eligibility or coverage (including coordinating benefits or determining cost sharing amounts), and adjudicating or subrogating health benefit claims; (2) Risk adjusting amounts due based on enrollee health status and demographic characteristics; (3) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related healthcare data processing; (4) Reviewing healthcare services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; (5) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and (6) Disclosing to consumer reporting agencies any of the following PHI relating to collecting premiums or reimbursement: (A) Name and address; (B) Date of birth; (C) Social security number; (D) Payment history; (E) Account number; and (F) Name and address of the healthcare provider and/or health plan (45 C.F.R. § 164.501 at "Payment" (2017)).

[561] Patient safety activities are: (1) Efforts to improve patient safety and the quality of healthcare delivery; (2) Collecting and analyzing patient safety work product; (3) Developing and disseminating information with respect to improving patient safety (e.g., recommendations, protocols, or information regarding best practices); (4) Utilizing patient safety work product for the purposes of encouraging a culture of safety and of providing feedback and assistance to effectively minimize patient risk; (5) Maintaining procedures to preserve confidentiality with respect to patient safety work product; (6) Providing appropriate security measures with respect to patient safety work product; (7) Utilizing qualified staff; and (8) Activities related to operating a patient safety evaluation system and to providing feedback to participants in a patient safety evaluation system (45 C.F.R. § 164.501 at "Health care operations" ¶ (1) (2017) (referencing 42 C.F.R. § 3.20)).

Activity		To Whom Covered Entity May Disclose	
Healthcare Operations (continued)	Protocol development and related functions that do not include treatment.	To any entity, for the disclosing Covered Entity's own activities	To any Covered Entity, for the receiving entity's own activities IF: (1) The discloser has or had a relationship with the subject of the PHI; (2) The recipient has or had a relationship with the subject of the PHI; (3) the PHI pertains to these relationships; and (4) the intended use of the PHI is for fraud and abuse detection and/or compliance
	Case management and care coordination and related functions that do not include treatment.		
	Contacting healthcare providers and patients with information about treatment alternatives and related functions that do not include treatment.		
	Reviewing the competence or qualifications of healthcare professionals		
	Evaluating practitioner and provider performance		
	Health plan performance		
	Conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as healthcare providers[562]		
	Training of non-healthcare professionals		
	Accreditation, certification, licensing, or credentialing activities		
	Conducting quality assessment and improvement activities (e.g., outcomes evaluation and development of clinical guidelines) and related functions that do not include treatment, if the primary purpose of any studies resulting from such activities is **not** to obtain generalizable knowledge.		
	Underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.[563]		
	Ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance).[563]		
	Business planning and development[564]		
	Business management and general administrative activities[565]		

[562] Psychotherapy notes may be disclosed without authorization for use in this activity (45 C.F.R. § 164.508(a)(2)(i)(B) (2017)).

[563] Where applicable, if a health plan receives PHI for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may only use or disclose such PHI for such purpose or as may be required by law (45 C.F.R. § 164.514(g) (2017)).

[564] This includes, but is not limited to: conducting cost-management and planning-related analyses related to managing and operating the entity; formulary development and administration; and development or improvement of methods of payment or coverage policies (45 C.F.R. § 164.501 at "Health care operations" ¶ (5) (2017)).

[565] This includes, but is not limited to: (1) Management activities relating to implementation of and compliance with the requirements of the HIPAA Administrative Simplification Rules (45 C.F.R. Parts 160, 162, and 164); (2) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that PHI is not disclosed to such policy holder, plan sponsor, or customer; (3) Resolution of internal grievances; (4) The sale, transfer, merger, or consolidation of all or part of the Covered Entity with another Covered Entity, or an entity that following such activity will become a Covered Entity and due diligence related to such activity; and (5) Consistent with applicable requirements, creating de-identified health information or a limited data set, and fundraising for the benefit of the Covered Entity (45 C.F.R. § 164.501 at "Health care operations" ¶ (6) (2017)).