Seyfarth

# 50-State Survey of Health Care Information Privacy Laws

2023-2024 Edition

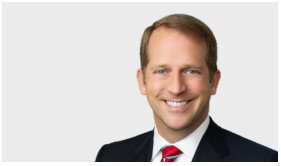
Dear Clients and Friends,

We are pleased to provide you with the 2023-2024 edition of our *50-State Survey of Health Care Information Privacy Laws*.

While there are several resources on how federal rules such as HIPAA may apply to sharing personal health information, there appear to be far fewer resources on how state privacy laws apply. Meanwhile, the challenge to maintain compliance, avoid data breaches, and make decisions on what can or should be shared with others remains ever-present and more acute than ever. For that purpose, Seyfarth attorneys created this resource to better assist you and your business identify and mitigate potential issue areas.

The information contained in this document compliments our attorneys' experience and expertise in representing clients across the full spectrum of the health care industry. Seyfarth's Health Care group is a leader in this space, as demonstrated by our ongoing recognition as a Tier 1 national Health Law practice by *U.S. News & World Report*, and as one of the top 50 largest Health Care law firms by *Modern Healthcare*. Our research for this project has been condensed and simplified, and thus, while it provides a convenient point of reference, we ask that you always consult with an attorney before making any decisions, as the law is constantly changing.

Please contact us with questions about this resource or to request additional state-specific information that may affect your organization. We also encourage you to visit Seyfarth's Health Care Privacy and Data Security Resource Center, as well as the firm's Health Care page to learn more about our cross-disciplinary industry group. Additionally, to keep you up-to-date on all of the latest health law issues and trends, Seyfarth has its Health Care Beat podcast. Episodes provide listeners with timely and insightful commentary on a variety of topics from a range of experts and thought leaders throughout the firm.



**Jesse M. Coleman**

*Partner and Health Care Industry Group Co-Chair*

**Leon Rodriguez**

*Partner and Health Care Steering Committee Member*

Project leads and members of Seyfarth's Health Care industry group.

**The following individuals contributed to this survey:** Connor Bateman (Iowa, New Mexico, Pennsylvania, Rhode Island); Alysha Bhatia (Arkansas, Indiana, Kentucky, Utah); Sierra Chinn-Liu (Missouri, Nebraska, North Dakota); Jesse Coleman (US - HIPAA); Drew del Junco (Arizona, Louisiana, Texas); Kileen Dietrich (Alabama, Oklahoma, Tennessee); Bessie Fakhri (Alaska, Colorado, Oregon, Washington); Kevin Green (California, Hawaii, Montana, Nevada); Kay Hazelwood (Delaware, New Jersey, North Carolina); Kevin Mahoney (Georgia, South Dakota, Wyoming); Andy Quesnelle (Idaho, Kansas, Minnesota, Wisconsin); Eron Reid (Maine, Massachusetts, New Hampshire); Danny Riley (Vermont, Virginia, West Virginia); Supreet Sandhu (Florida, Maryland, Mississippi); Robert Terzoli (Michigan, Ohio, South Carolina); and Owen Wolfe (Connecticut, Illinois, New York).

| State | How does the State define protected health information? | How does the state define a covered entity (i.e. who is subject to the disclosure laws)? | What additional security obligations exist (beyond HIPAA) for PHI? | What rules are there governing business associates? | What constitutes a breach or unlawful disclosure? |
|---|---|---|---|---|---|
| **US** HIPAA | Subject to certain exceptions, protective health information ("PHI") includes individually identifiable health information, transmitted or maintained in any form or medium. 45 C.F.R. §160.103 | Includes health plans, health care clearinghouses, and health care providers who transmit health information in electronic form. 45 C.F.R. §164.103 | HIPAA has a security rule to ensure the confidentiality of PHI, protect against threats and unanticipated prohibited uses or disclosures, and ensure compliance by a covered entities' work force. 45 C.F.R. §164.306 | Business associates must adhere to the same privacy and security rules applicable to covered entities, and must notify the covered entity in the event of a discovered breach. 45 C.F.R. §§164.410, .502(e),.504(e), .532(d)-(e) | A breach of the HIPAA Privacy Rule is an impermissible acquisition, access, use or disclosure that compromises the security of the protected health information; such uses and disclosures are presumed to be a breach unless the covered entity shows there is a low probability PHI was compromised based on a comprehensive risk assessment. 45 C.F.R. §164.402 |
| **AL** Alabama | State administrative code adopts HIPAA in its entirety, including definition of PHI. Ala. Dept. of Public Health Policy 2022-002 | None beyond HIPAA. Ala. Dept. of Public Health Policy 2022-002 | For general medical records, none beyond HIPAA. Heightened non-disclosure obligations for medical records regarding sexually-transmitted diseases. Ala. Code 1975 §22-11A-22 | None beyond HIPAA. | "The unauthorized acquisition of data in electronic form containing sensitive personally identifying information [including health records]." Ala. Code 1975 §8-38-2 |
| **AK** Alaska | No comprehensive statute governing PHI beyond HIPAA; privacy is addressed in separate statutes governing specific types of entities and conditions. | Restrictions on disclosure specific to certain entities:<br>• EMTs. Alaska Stat. §18.08.087<br>• Home health agencies. Alaska Admin. Code, tit. 7, §12.534.<br>• Pharmacists. Alaska Stat. §8.80.315<br>• Community health facilities. Alaska Admin. Code, tit. 7, §13.130<br>• Nursing homes. Alaska Admin. Code, tit. 7, §12.890<br>• State agencies. Alaska Stat. §40.25.120<br>• Participants of electronic health information exchange systems. Alaska Admin. Code, tit. 7 §166.040. | Restrictions on disclosure specific to certain conditions:<br>• Substance abuse. Alaska Stat. §47.37.210<br>• Cancer. Alaska Stat. §18.05.042<br>• Genetic testing. Alaska Stat. §18.13.010<br>• Infectious diseases. Alaska Stat. §18.05.042<br>• Mental health. Alaska Stat. §47.30.845<br>• Certain insurers must implement an information security program to safeguard confidential information. Alaska Admin. Code, tit. 3, §26.705. | None beyond HIPAA. | Breach of unencrypted personal information, if there is reasonable likelihood that harm to the affected individual will result. Alaska Stat. §45.48.010 |

| What safe harbors or exceptions exist (e.g., close family, death, etc.) | What form may an authorization for disclosure take (e.g., written, verbal, duration)? | What are the State's reporting and remediation requirements in the event of a breach/unlawful exposure? | What penalties exist for failure to report an unlawful exposure? | What rules are there for responding to subpoenas? |
|---|---|---|---|---|
| Per authorization, treatment payment, health care operations, personal representatives (including parents/guardians for unemancipated minors), estate executors, whistleblowers, certain government functions, certain law enforcement purposes, and per valid court subpoena and qualified protective order. 45 C.F.R. §§ 164.502, .512 | An authorization must include in written plain language: description of information, name of person making disclosure, name of person/ entity to which information will be disclosed, purpose, expiration date, signature of authorizing party, and acknowledgment of ability to revoke, and ability or inability to condition treatment, and notice for potential of redisclosure. 45 C.F.R. § 164.508 | HIPAA requires a covered entity to notify the affected party of a breach, as well as the media and Secretary of Health and Human Services, depending on the number of health records subject to unauthorized disclosure. 45 C.F.R. § 164.404-.410 | Failure to properly timely report a HIPAA breach to the correct entities (individual, media, Secretary) may result in civil penalties beyond those associated with the breach, and the Secretary may consider this failure when assessing other penalties. 45 C.F.R. § 160.402, 408 | A covered entity may produce PHI, pursuant to a valid subpoena, only with proper authorization of the individual or upon seeking and/or obtaining a qualified protective order from a court of competent jurisdiction, and may disclose only as much as necessary for purposes of the litigation. 45 C.F.R. § 164.512(e) |
| None beyond HIPAA. | None beyond HIPAA. | Report to affected individuals in most expedient manner possible and without unreasonable delay. If more than 1,000 affected individuals, notify Attorney General within 45 days. Ala. Code 1975 § 8-38-5,6 | Penalties of up to $5,000 per day for violation of notification provisions. Ala. Code 1975 § 8-38-9. Alabama Supreme Court recognizes tort claims of invasion of privacy for unlawful disclosure of medical records. | Subpoena must be HIPAA-compliant before response authorized. Particularized rules for responding to subpoenas seeking mental health records. Ala. Code 1975 § 34-26-2 |
| Child and elder abuse:<br>• Licensed counselors. Alaska Stat. § 08.29.200<br>• Licensed family therapists. Alaska Stat. § 08.63.200.<br>• Psychologists. Alaska Stat. § 08.86.200<br>• Threat of imminent serious physical harm:<br>• Licensed counselors. Alaska Stat. §§ 08.29.200<br>• Licensed family therapists. Alaska Stat. § 08.63.200 | Written or electronic form. No duration limitation. Alaska Admin. Code, tit. 3, § 26.685 | After discovering the breach, the covered person must notify each affected state resident in the most expeditious time possible. Alaska Stat. § 45.48.010 | None beyond HIPAA. | None beyond HIPAA. |

| State | How does the State define protected health information? | How does the state define a covered entity (i.e. who is subject to the disclosure laws)? | What additional security obligations exist (beyond HIPAA) for PHI? | What rules are there governing business associates? | What constitutes a breach or unlawful disclosure? |
|---|---|---|---|---|---|
| **AZ** Arizona | All medical and payment records may not be disclosed unless authorized by law or written authorization. Ariz. Rev. Stat. Ann. § 12-2292(A)<br>"Medical records" means all communications related to a patient's health that are maintained for diagnosis or treatment. Ariz. Rev. Stat. Ann. § 12-2291(6)<br>"Payment records" means all communications related to payment for health care that contain individually identifiable information. Ariz. Rev. Stat. Ann. § 12-2291(7)<br>The Arizona Insurance Information and Privacy Protection Act applies to insurance entities and includes a provision governing disclosure of "medical record information." Ariz. Rev. Stat. Ann. § 20-2113<br>"Medical record information" is any personal information that relates to an individual's medical condition and is obtained from a medical professional or medical care institution. Ariz. Rev. Stat. Ann. § 20-2102(18) | Restrictions on disclosure specific to certain entities:<br>• Health care provider. Ariz. Rev. Stat. Ann. § 12-2291(5).<br>• Health care institution. Id.<br>• Ambulance service. Id.<br>• Health care services organization. Id. | Hospitals and health care professionals must have written protocols for safeguarding medical records to prevent unauthorized access. Ariz. Rev. Stat. Ann. § 32-3211; Ariz. Admin. Code § R9-10-213(B)(1). Failure to comply may result in a civil action for damages or disciplinary action. Ariz. Rev. Stat. Ann. § 12-2296; *id.* § 20-2118; *id.* § 32-3211 | None beyond HIPAA. | Unauthorized access that materially compromises the confidentiality of unencrypted computerized personal information maintained as part of a database of personal information. Ariz. Rev. Stat. Ann. § 18-551(1) |
| **AR** Arkansas | All records "catalogued and maintained by the medical records department of a hospital, doctor's office, medical clinic, or any other medical facility." Ark. Code § 16-46-402 | Hospitals, doctors' offices, medical clinics, or any other medical facility. Ark. Code § 16-46-402 | None beyond HIPAA. | None beyond HIPAA. | Any "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business." Ark. Code § 4-110-113 |

| What safe harbors or exceptions exist (e.g., close family, death, etc.) | What form may an authorization for disclosure take (e.g., written, verbal, duration)? | What are the State's reporting and remediation requirements in the event of a breach/unlawful exposure? | What penalties exist for failure to report an unlawful exposure? | What rules are there for responding to subpoenas? |
|---|---|---|---|---|
| Medical and payment records may be disclosed by health care practitioners without patient authorization as permitted by HIPAA or to: another current or former treating provider; ambulance attendant; health care provider accrediting agency; health profession regulatory board; utilization review agent; third party payor; or deceased patient's health care decision maker or specified family members. Ariz. Rev. Stat. Ann. § 12-2294(C)-(D); *id.* § 20-2113 | Written and signed by patient or patient's health care decision maker. Ariz. Rev. Stat. Ann. §§ 12-2292, 12-2294(B); *id.* §§ 20-2106, 20-2113; Ariz. Admin. Code § R9-10-212(B)(3)(f). No duration limitation unless authorization for insurance transaction. Ariz. Rev. Stat. Ann. § 20-2106(7) | Affected individuals must be notified within 45 days of breach determination and provide certain information.<br>Ariz. Rev. Stat. Ann. § 18-552(B). This statute does not apply to HIPAA-covered entities. Ariz. Rev. Stat. Ann. § 18-552(N)(2) | The Attorney General may impose a civil penalty of up to $10,000 for each affected individual up to $500,000. Ariz. Rev. Stat. Ann. § 18-552(L). This statute does not apply to HIPAA-covered entities. Ariz. Rev. Stat. Ann. § 18-552(N)(2) | Subpoenas to health care practitioners seeking medical or payment records must be served with 10 days' notice and be accompanied by signed written authorization or court order that satisfies HIPAA qualified protective order requirements, or is a grand jury or health profession regulatory board subpoena. Ariz. Rev. Stat. Ann. § 12-2294.01; *id.* § 12-12802. Court must determine information is not available from original source and is relevant. Ariz. Rev. Stat. Ann. § 36-3808(A) |
| None beyond HIPAA. | None beyond HIPAA. | Report to affected individuals in most expedient manner possible and without unreasonable delay. If more than 1,000 affected individuals, notify Attorney General within 45 days. Ark. Code § 4-110-105 | Subject to Attorney General action for deceptive trade practice. Potential penalty of $10,000 per violation. Ark Code. § 4-88-113 | Must notify patient (or patient's attorney) by writing or fax once records are received. Ark. Code § 16-46-403 |

| State | How does the State define protected health information? | How does the state define a covered entity (i.e. who is subject to the disclosure laws)? | What additional security obligations exist (beyond HIPAA) for PHI? | What rules are there governing business associates? | What constitutes a breach or unlawful disclosure? |
|---|---|---|---|---|---|
| **CA**<br>**California** | California has a broad definition of personal information. "Personal Information" is information that has a person's first name or first initial and last name in combination with any of the following:<br>• Social security number;<br>• driver's license number or California identification card number; or<br>• account number, credit/debit card number, in combination with any required security code, access code, or password that would allow access to the person's financial account.<br>CA CIV 1798.80; see also CA CIV 1798.82(h)(1)-(2)<br>"Medical information" means any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment.<br>"Individually identifiable" means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity.<br>Confidentiality of Medical Information Act ("CMIA") CA CIV 56.05 (i)<br>"Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with | Rules for "Personal Information cover all California businesses, organizations, and state and local government agencies.<br>Rules for Medical Information cover providers of health care, health care service plans, contractors, and all recipients of that information. Any business that offers software or hardware that are designed to maintain medical information is considered a provider.<br>CA CIV 1798.82(a); CA CIV 156.05(b&m)<br>The CCPA applies to "businesses" that collect "personal information" about "consumers." There are four types of entities and persons that qualify as a "business" under the CCPA: (1) legal entities that collect consumers' personal information; (2) entities that share common control with a business; (3) joint ventures or partnerships composed of businesses; and (4) persons who voluntarily comply with the CCPA. See CA CIV 1798.140(d) (operative 1/1/23). In addition, to qualify as a "business" under CA CIV 1798.140(d)(1), the entity must do business in California and satisfy one or more of the following thresholds:<br>• as of January 1 of the calendar year, have annual gross revenues in excess of $25 million in the preceding calendar year, as adjusted pursuant to CA CIV 1798.185(a)(5);<br>• annually buy, sell or share, alone or in combination, the personal information of 100,000 or more consumers or households; or<br>• derive 50% or more of its annual revenues from selling or sharing consumers' personal information. CA CIV 1798.140(d)(1) (operative 1/1/23)<br>Note: Effective on January 1, 2023, the California Privacy Rights Act ("CPRA") amendments to the CCPA are fully operative and bring the | All health care providers, health service plans, pharmaceutical companies, contractors or other entities must preserve, store, maintain or destroy patient medical records in a way that preserves the confidentiality of the information. They shall protect and preserve the integrity of electronic medical information and automatically record and preserve any change or deletion of any electronically stored medical information. The record of any change or deletion shall include the identity of the person who accessed and changed the medical information, the date and time the medical information was accessed, and the change that was made to the medical information. CA CIV 56.101<br>Subject to certain exceptions, disclosure of a patient's, enrollee's, or subscriber's "medical information" is prohibited absent that person's authorization. CA CIV 56.10(a) | Specific patient authorization is required in order to share patient information with business associates who are not third-party payers, entities who review in liability, arbitration, peer review, quality assurance, quality assessment, medical necessity cases or otherwise not included. CA CIV 56.10 | A breach of the security of the system means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure. CA CIV 1798.82 |

| What safe harbors or exceptions exist (e.g., close family, death, etc.) | What form may an authorization for disclosure take (e.g., written, verbal, duration)? | What are the State's reporting and remediation requirements in the event of a breach/unlawful exposure? | What penalties exist for failure to report an unlawful exposure? | What rules are there for responding to subpoenas? |
|---|---|---|---|---|
| Various state laws allow use and disclosure of health information in particular instances or under particular circumstances.<br>CA CIV 5328, 5541, 1798.91, 4514, 120975-121020, 121025, 4135 | A provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization, except as provided in subdivision (b) or (c). The information may be disclosed to providers of health care, health care service plans, contractors, or other health care professionals or facilities for purposes of diagnosis or treatment of the patient.<br>The information may be disclosed to an insurer, employer, health care service plan, hospital service plan, employee benefit plan, governmental authority, contractor, or other person or entity responsible for paying for health care services rendered to the patient, to the extent necessary to allow responsibility for payment to be determined and payment to be made.<br>CA CIV 56.10 | Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, must disclose any "breach of the security of the system," following discovery, to any California patient whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.<br>The breach notification must meet all of the following requirements:<br>(A) The security breach notification shall be written in plain language.<br>(B) The security breach notification shall include, at a minimum, the following information: (1) The name and contact information of the reporting person or business subject to this section. (2) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach. (3) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice. (4) Whether notification was delayed as a result of a law enforcement investigation. (5) A general description of the breach incident. (6) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.<br>(C) At the discretion of the person or business, the security breach notification may also include any of the following: (1) Information about what the person or business has done to protect individuals whose information has been breached. (2) Advice on steps that the person whose information has been breached may take to protect himself or herself.<br>CA CIV 1798.82(a&d) | An entity or individual who negligently discloses medical information is also liable (in addition to damages paid to the patient) to pay a civil or administrative fine of $2,500 per violation.<br>CA CIV 1798.84(b)<br>CA CIV 56.36<br>In addition to any other remedies available at law, a patient whose medical information has been used or disclosed in violation of Section 56.10, 56.104, 56.107, or 56.20 or subdivision (a) of Section 56.26 and who has sustained economic loss or personal injury therefrom may recover compensatory damages, punitive damages not to exceed three thousand dollars ($3,000), attorney's fees not to exceed one thousand dollars ($1,000), and the costs of litigation<br>CA CIV 56.35 | Must list under what statute the health information being sought is covered under.<br>CA CIV 56<br>CA CIV 5328 |

| State | How does the State define protected health information? | How does the state define a covered entity (i.e. who is subject to the disclosure laws)? | What additional security obligations exist (beyond HIPAA) for PHI? | What rules are there governing business associates? | What constitutes a breach or unlawful disclosure? |
|---|---|---|---|---|---|
| | a particular consumer or household: [listing several categories of personal information]. CA CIV 1798.140(v)<br>Note: the California Consumer Privacy Act of 2018 ("CCPA") [1798.100 - 1798.199.100] expressly exempts protected health information under HIPAA and medical information governed by CMIA. CA CIV 1798.145-.146. | CCPA closer in line with the European Union's General Data Protection Regulation (GDPR, Regulation (EU) 2016/679). | | | |
| **CO**<br>Colorado | Undefined. "Personal Information" means: Resident's name plus:<br>• Social security Number;<br>• driver's license number;<br>• medical information;<br>• health insurance number; or<br>• other specified information. Col. Rev. Stat. Ann. § 6-1-716(1)(g) (West 2021). | Individual or entity that maintains Personal Information the course of his/her/its occupation or business. Excludes third-party service providers. Col. Rev. Stat. Ann. § 6-1-716(1)(b) (West 2021) | None. This state does not define Protected Health Information. This state does not mandate security obligations beyond HIPAA. Col. Rev. Stat. Ann. § 6-1-716(2) (West 2021) | None beyond HIPAA.<br>Third-party service providers are not covered entities per state statute, but can be a HIPAA business associate. Col. Rev. Stat. Ann. § 6-1-716(1)(b) (West 2021) | A "security breach" is an unauthorized acquisition of unencrypted computerized data that compromises the confidentiality of Personal Information maintained by a covered entity. Col. Rev. Stat. Ann. § 6-1-716(1)(h) (West 2021) |
| **CT**<br>Connecticut | 1) Defined in CT Statute Title 38a INSURANCE Chapter 700C Health Insurance, C.G.S.A. § 38a-591a. Health information that identifies an individual who is the subject of the information or for which there is a reasonable basis to believe that such information could be used to identify such individual. PHI is protected under both federal and state law.<br>2) Defined in CT Statute Title 38a INSURANCE Chapter Connecticut Insurance Information and Privacy Protection Act, C.G.S.A. § 38a-976. Individually identifiable health information that is maintained or transmitted by electronic media or any other form or medium. The definition excludes information that lacks personal identifiers or information that could be used to indirectly identify the individual patient, or where such information is protected by an encryption key or code. | 1) Defined in CT Statute Title 38a INSURANCE Chapter 700C Health Insurance, C.G.S.A. § 38a-472f , citing 42 U.S.C.A. § 256b. Covered entity as defined in 42 U.S.C. 256b. One of the following: Federally-qualified health center; entity receiving a grant under section 256a of this title; family planning project receiving a grant under section 300 of this title; State operated AIDS drug purchasing assistance program receiving financial assistance; black lung clinic receiving funds under section 973(a) of title 30; Federally-qualified health center; family planning project; entity providing outpatient early intervention services for HIV disease; State operated AIDS drug purchasing assistance program; comprehensive hemophilia diagnostic treatment center; Native Hawaiian Health Center; urban Indian organization; certain entity receiving funds for treatment of sexually transmitted diseases or tuberculosis; certain hospital; certain children's hospital and certain rural community hospital. | CT common law, *CT Supreme Court Case Byrne v. Avery Center for Obstetrics and Gynecology (2018)* holds that while it is true that the privacy rules in federal HIPAA do not provide patients a private right of action, health care providers in Connecticut and a significant number of other states can be sued for unauthorized disclosures of confidential patient information. | CT Statutes don't have a definition for Business Associate. It is defined by 45 C.F.R. § 160.103<br>Defer to federal HIPAA rules. | In the insurance context, disclosure with malicious intent to damage an individual's reputation or character is unlawful. C.G.S.A. § 38a-999a.<br>Otherwise, CT statutes don't define what constitutes a breach or unlawful disclosure. Defer to 45 C.F.R. § 164.402 for what is a breach.<br>In addition to protection under HIPAA, CT statutes prohibits persons from selling or offering to sell personal health information and prohibits the Department of Public Health from publicly disclosing personal identifiable information about a patient in an institution. CT statues also establishes a bill of rights for individuals admitted to nursing home, residential care home or chronic disease hospital to assure confidential treatment of patient personal medical records. *See, e.g.,* C.G.S.A. § 19a-697(12). |

| What safe harbors or exceptions exist (e.g., close family, death, etc.) | What form may an authorization for disclosure take (e.g., written, verbal, duration)? | What are the State's reporting and remediation requirements in the event of a breach/unlawful exposure? | What penalties exist for failure to report an unlawful exposure? | What rules are there for responding to subpoenas? |
|---|---|---|---|---|
| | | | | |
| Disclosure by mental health providers necessary to warn potential victims or disclose threats. Co. Rev. Stat. Ann. §13-21-117(2)(b). | None beyond HIPAA. | Notification of the affected residents and the state's attorney general within 30 days. Covered Entity must conduct a prompt investigation. Col. Rev. Stat. Ann. §6-1-716(2) (West 2021) | State AG may file a lawsuit to ensure compliance and/or recover resulting direct economic damages. Col. Rev. Stat. Ann. §6-1-716(4) (West 2021) | None beyond HIPAA. |
| Availability of patient information to certain agencies, such as the Department of Emergency Services and Public Protection, the Department of Social Services, and the United States Department of Health and Human Services. C.G.S.A. §17b-225<br>Consent not required for certain disclosures, including to persons engaged in the diagnosis or treatment of patients, or if records determine that the disclosure or transmission is needed to accomplish the objectives of diagnosis or treatment, or if a mental health provider determines there is substantial risk of imminent physical injury by the patient to himself or others, or in the course of examinations, ordered by a court, or made in connection with the appointment of a conservator, and with regard to certain payment requests by a provider of behavioral health services that contracts with the Department of Mental Health and Addiction Services. C.G.S.A. §52-146f | Content of disclosure authorization forms. The CT statute provides that no authorization form may be utilized unless it is written in plain language, dated, specifies the types of persons to disclose the information, specifies the nature of the information to be disclosed, identifies the individual who authorizes the information to be disclosed, and specifies the length of time such authorization remains valid. C.G.S.A. §38a-981<br>(What means release of confidential HIV-related information). "Release of confidential HIV -related information" requires a written authorization for disclosure of confidential HIV-related information, which is signed by the protected individual, dated, and specifies to whom the disclosure is authorized, the purpose for the disclosure, and the time period during which the release is effective. C.G.S.A. §19a-581 | HIPAA requirements on Notification in the Case of Breach of Unsecured Protected Health Information.<br>The Office of the Attorney General has authority to enforce HIPAA protections for Connecticut state residents. OCR and the Office of the Attorney General have authority to receive and investigate complaints against covered entities and business associates related to the HIPAA Privacy Rule, Security Standards, and the newly established Breach Notification Rule.<br>https://portal.ct.gov/AG/Sections/Privacy/The-Privacy-and-Data-Security-Department<br>https://portal.ct.gov/AG/Health-Issues/Health-Information--Services/Your-Rights-Under-HIPAA#:~:text=The%20Office%20of%20the%20Attorney%20General%20William%20Tong&text=The%20HIPAA%20Privacy%20and%20Security,use%20patients'%20personal%20medical%20information | For malicious intent to damage reputation in the insurance context, fine and prison time. C.G.S.A. §38a-999a.<br>Otherwise, no CT statutes. See HIPAA (45 C.F.R. §160.404 Amount of a civil money penalty) | Inspection and subpoena of hospital records. If a private hospital, public hospital, society, or corporation receiving state aid is served with a subpoena issued by a competent authority directing production of records, except where the record pertains to a mentally ill patient, deliver the record to the clerk of such court in a sealed envelope for safekeeping. C.G.S.A. §4-104<br>Records as evidence. Records of the Office of Chief Medical Examiner shall be subject to subpoena under same conditions as medical records. C.G.S.A. §19a-412 |

| State | How does the State define protected health information? | How does the state define a covered entity (i.e. who is subject to the disclosure laws)? | What additional security obligations exist (beyond HIPAA) for PHI? | What rules are there governing business associates? | What constitutes a breach or unlawful disclosure? |
|---|---|---|---|---|---|
| **DE** Delaware | "Protected health information" follows HIPAA. DEL. CODE ANN. tit. 16, §1210 (4).<br>The statute governing notice requirements for a computer security breach also includes broad definition of "Personal information." DEL. CODE ANN. tit. 6, §12B-101(7) | Restrictions on disclosure specific to certain entities, for example:<br>• Long-term care facilities. DEL. CODE ANN. tit. 16, §1121(9)<br>• skilled and intermediate care nursing facilities. 16 DEL. ADMIN. CODE §3201-9.0<br>• Free standing surgical centers. 16 DEL. ADMIN CODE §4405-4.0<br>Notice of data breach applicable to person that owns or licenses or maintains computerized data that includes personal information about a Delaware resident. DEL. CODE. ANN. tit. 6, §12B-100<br>Person comprehensively defined to include "an individual; corporation; business trust; estate trust; partnership; limited liability company; association; joint venture; government; governmental subdivision, agency, or instrumentality; public corporation; or any other legal or commercial entity." DEL. CODE. ANN. tit. 6, §12B-101(6) | "Any person who conducts business in [Delaware] and owns, licenses, or maintains personal information shall implement and maintain reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business." DEL. CODE. ANN. tit. 6, §12B-100<br>In addition, restrictions on disclosure specific to certain conditions, DEL. CODE ANN. tit. 16, §1210, including, for example:<br>• Substance abuse. 16 DEL. ADMIN. CODE § 2220<br>• Cancer. 16 DEL. ADMIN. CODE §4201-3.0<br>• Genetic testing. 16 DEL. ADMIN. CODE § 1202<br>• Infectious diseases. 16 DEL. ADMIN. CODE §<br>• Mental health. 16 DEL. ADMIN. CODE §<br>• Birth Defects. 16 DEL. ADMIN. CODE §4101-3.0<br>• Autism. 16 DEL. ADMIN. CODE §4109-3.0 | None beyond HIPAA.<br>Notice of data breach applicable to vendors with access to personal information. DEL. CODE. ANN. tit. 6, §12B-100 | A "'breach of the security of the system' means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity." DEL. CODE. ANN. tit. 6, §12B-101(1) |
| **FL** Florida | Any medical record generated after making a physical or mental examination, administration of treatment, or dispensation of legend drugs. Fla. Stat. § 456.057(1) | Any health care practitioner who generates medical records or to whom such records are transferred. Fla. Stat. § 456.057(1)-(2) | All records owners required to develop and implement confidentiality policies and train employees. Fla. Stat. § 456.057(10)<br>Record owners also required to maintain record of any requests from third parties, and destroy information after retention requirements expire. Fla. Stat. § 456.057(11); Fla. Stat. § 501.171(8) | Business associates who suffer breach of health records must notify covered entity within 10 days. Fla. Stat. § 501.171(6) | Protected health information included in state data breach law includes any unauthorized access of data in electronic form. Fla. Stat. § 501.171(1) |
| **GA** Georgia | Any record "used in assessing the patient's condition, or the pertinent portion of the record relating to a specific condition or a summary of the record." Ga. Code § 31-33-1 | Includes "all hospitals… other special care units…; intermediate care facilities; ambulatory surgical or obstetrical facilities; health maintenance organizations; and home health agencies."<br>Ga. Code § 31-33-1 | Providers are obligated to retain covered records for 10 years; particularized requirements for copying of records. Ga. Code § 31-33- | None beyond HIPAA. | State data breach law does not include health information. State recognizes tort claims for unlawful disclosure of health information. |
| **HI** Hawaii | Hawaii's Health Care Privacy Harmonization Act of 2012 harmonizes state law with HIPAA. HRS 323B-3 | None beyond HIPAA. | None beyond HIPAA. | None beyond HIPAA. | None beyond HIPAA. |

| What safe harbors or exceptions exist (e.g., close family, death, etc.) | What form may an authorization for disclosure take (e.g., written, verbal, duration)? | What are the State's reporting and remediation requirements in the event of a breach/unlawful exposure? | What penalties exist for failure to report an unlawful exposure? | What rules are there for responding to subpoenas? |
|---|---|---|---|---|
| "Good faith acquisition of personal information by an employee or agent of an individual or commercial entity for the purposes of the individual or commercial entity is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure." DEL. CODE. ANN. tit. 6, §12B-101(1) | Pursuant to "informed consent." DEL. CODE ANN. tit. 16, §1212(b).<br>"Informed consent" means a written authorization for the disclosure of PHI on a form substantially similar to one promulgated by DHS. DEL. CODE ANN. tit. 16, §1210(2) | "Notice must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system." DEL. CODE ANN. tit. 6 §12B-102(a)<br>Not later than 60 days after determination of the breach of security breach except in certain circumstances. DEL. CODE ANN. tit. 6 §12B-102(c)<br>Additional notice requirements if breach involves SSN. DEL. CODE ANN. tit. 6 §12B-102(d) | DHS shall enforce DEL. CODE ANN. tit. 16, §1210. | Attorney General may bring an action in law or equity to address the violations of statute relating to notice of data breach and may recover damages. Statute is not exclusive remedy and does not relieve a person subject to this chapter from compliance with all other applicable provisions of law. DEL. CODE ANN. tit. 6 §12B-104(a)<br>Issued through or pursuant to a court or administrative tribunal order, PHI may be disclosed without informed consent. Note that a covered entity may disclose; it does not have to disclose. See DEL. CODE ANN. tit. 16 §1212(b) |
| In cases of compulsory physical examination, to poison control centers, and to Department of Children and Families in abuse or neglect investigations. Fla. Stat. § 456.057(7)(a)(1-6) | Written authorization required. Fla. Stat. § 456.057(7)(a) | Notify affected individuals within 30 days and Florida Department of Legal Affairs for any breach affecting more than 500 individuals. Fla. Stat. § 501.171(3-4) | Penalty of $1,000 each day for first 30 days of failure to notify, thereafter $50,000 for each 30-day period in which failure continues. Fla. Stat. § 501.171(9) | Patient authorization not required as long as subpoena is from court of competent jurisdiction and proper notice given to patient or patient's representative by party seeking records. Fla. Stat. § 456.057(7)(a)(3) |
| No civil or criminal liability for provider releasing information "in good faith" pursuant to provisions of health records law. Ga. Code Ann. § 31-33-5<br>May be provided to family members or executors of estates in certain circumstances. Ga. Code § 31-33-2 | Request must be in writing by patient or authorized representative. Ga. Code Ann. § 31-33-2 | None beyond HIPAA. | None beyond HIPAA. | None beyond HIPAA. |
| None beyond HIPAA. | None beyond HIPAA. | None beyond HIPAA. | None beyond HIPAA. | None beyond HIPAA. |

| State | How does the State define protected health information? | How does the state define a covered entity (i.e. who is subject to the disclosure laws)? | What additional security obligations exist (beyond HIPAA) for PHI? | What rules are there governing business associates? | What constitutes a breach or unlawful disclosure? |
|---|---|---|---|---|---|
| **ID** Idaho | No comprehensive statute governing PHI beyond HIPAA; privacy is addressed in separate statutes governing specific types of entities and conditions. | Restrictions on disclosure specific to certain entities:<br>• Health care practitioners. Idaho Code Ann. § 37-2743(c); Idaho Admin. Code § 16.05.01.107.02<br>• Prescription information. Idaho Code Ann. § 54-1727<br>• Nurses. Idaho Admin. Code § 22.01.11.100<br>• Optometrists. Idaho Admin. Code § 24.10.01.300.02<br>• Social workers. Idaho Admin. Code § 24.14.01.450.02 | Requires pharmacies to maintain sufficient security mechanisms to protect records from unauthorized access, including electronic recordkeeping systems in certain instances. Idaho Admin. Code § 27.01.01.300; *see also* Idaho Code Ann. § 39-1394 | None beyond HIPAA. | No state-specific statute governing breach or unlawful disclosure of PHI beyond federal protections and tort law. |
| **IL** Illinois | Definitions: As specified in 45 CFR 164.103. 410 ILCS 513/10; 410 ILCS 305/3.<br>Also includes information that would identify a patient and the services provided to that patient. *See* 210 ILCS 85/6.14b; 210 ILCS 85/6.17. | Definitions: As specified in 45 CFR 160.103. 410 ILCS 513/10; 410 ILCS 305/3(d); 740 ILCS 110/2. | Confidentiality Protections in Illinois:<br>https://www.dhs.state.il.us/page.aspx?item=33520<br>https://hfs.illinois.gov/info/legal/hipaa.html | Definitions: As specified in 45 CFR 160.103. 410 ILCS 305/3(c); 410 ILCS 513/10; 740 ILCS 110/2.<br>Disclosures to "Business Associate–" permitted under the "Genetic Information Privacy Act," the "AIDS Confidentiality Act," and the "Mental Health and Development Disabilities Confidentiality Act." 410 ILCS 513/31.3; 410 ILCS 305/9.3; 740 ILCS 110/9.8.<br>–<br>Establishment and disclosure of limited data sets and de-identified information. 410 ILCS 305/9.8; 410 ILCS 513/31.7; 740 ILCS 110/9.11 | Disclosure by hospitals is violation other than to the patient or persons making decisions for the patient's health if patient is unable to do so; the persons directly involved in treatment or processing payment for the treatment; those involved in peer review, utilization review or quality assurance; or those involved in the defense of claims brought against the hospital arising out of the treatment. 210 ILC 85/6.17(d)-(e).<br>In other contexts, intentional or reckless violation of the applicable disclosures is a breach, 410 ILCS 305/12, or disclosure to individuals other than the individual in question or those persons authorized by statute, 410 ILCS 513/15(a). |
| **IN** Indiana | "As used in this chapter, PHI has the meaning set forth in 45 CFR 160.103 as in effect on November 4, 2004." IC 16-39-10-3 | "As used in this chapter, 'covered entity' has the meaning set forth in 45 CFR 160.103 as in effect on November 4, 2004." IC 16-39-10-1 16-39-10-1 | Right of access. IC 16-39-1-1<br>Provider's use of records; data aggregation; confidentiality; violations. IC 16-39-5-3 | Indiana State Department Of Health HIPAA Business Associates Policy-ISDH-COMM-006-04 | Provider's use of records; data aggregation; confidentiality; violations. IC 16-39-5-3 |
| **IA** Iowa | Defined with reference to HIPAA if created or received by an authorized participant in state health information network. IA. Code 135D.2(17) | No specific definition for covered entities beyond HIPAA, but some disclosure and record-keeping rules apply to participants in state health information network.<br>Heightened confidentiality requirements for AIDS-related records and information. IA. Code 141A.9. | Additional limitations on disclosure of mental health information. IA. Code 228.2. | None beyond HIPAA. | No set definition under state law. State data breach reporting law does not include health information unless such information is "biometric data." IA Code 715C.1 |
| **KS** Kansas | None beyond HIPAA. Kan. Stat. Ann. § 65-6825(a) (West 2021)<br>None beyond HIPAA. | Equivalent to HIPAA, as this state explicitly incorporates HIPAA regarding Protected Health Information and its unauthorized disclosure. Kan. Stat. Ann. § 65-6822(d) and (q) (West 2021) | Equivalent to HIPAA. Kan. Stat. Ann. § 65-6822(d) (West 2021) | None beyond HIPAA. Kan. Stat. Ann. § 65-6824(b) (West 2021). | A Covered Entity may disclose Protected Health Information to a health information organization without an authorization under certain conditions. Kan. Stat. Ann. § 65-6825(b) (West 2021) |

| What safe harbors or exceptions exist (e.g., close family, death, etc.) | What form may an authorization for disclosure take (e.g., written, verbal, duration)? | What are the State's reporting and remediation requirements in the event of a breach/unlawful exposure? | What penalties exist for failure to report an unlawful exposure? | What rules are there for responding to subpoenas? |
|---|---|---|---|---|
| Child abuse and domestic violence. Idaho Code Ann. § 9-203<br>Disclosure necessary to warn potential victims or disclose threats. Idaho Code Ann. § 54-3410 | Written and signed by individual or legally authorized representative. Idaho Admin. Code § 16.05.01.051. No duration limitation. | None beyond HIPAA. | None beyond HIPAA. | None beyond HIPAA. |
| Disclosure; consent "Except as provided in Sections 6 through 12.2 of this Act, records and communications may be disclosed … with the written consent of those persons who are entitled to inspect and copy a recipient's record . . . ." 740 ILCS 110/5<br>For hospitals, persons who "in good faith, act[] in accordance with the terms of" the statute" shall not be subject to an type of . . . liability or discipline . . . ." 210 ILC 85/6.17(h).<br>Disclosures to law enforcements are also permitted in some circumstances. *See, e.g.,* 410 ILCS 305/9.4a; 410 ILCS 513/31.6. | Definition of "Informed consent' " in certain contexts includes written or oral consent after receiving required information. 410 ILCS 305/3(q).<br>For mental health records, consent must be in writing and provide certain information about the intended disclosure. 740 ILCS 110/5. | Data collectors who suffer a security breach or otherwise fail to maintain confidential information must notify the individuals affected and, in the case of private companies, the Illinois Attorney General. 815 ILCS 530/10, 530/12. | For data collectors, "[a] violation of this Act constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act." IL Personal Information Protection A-t - 815 ILCS 530/20. Injunctive relief; restitution; and civil penalties. IL Consumer Fraud and Deceptive Business Practices A-t - 815 ILCS 505/7<br>For disclosure of mental health records, "[a]ny person who knowingly and wilfully violates" the statute "is guilty of a Class A misdemeanor." 740 ILCS 110/16.<br>For disclosure of AIDS information, negligence can result in damages and reasonable attorneys' fees, plus injunctive relief. 410 ILCS 305/13. Damages are also available for disclosure of genetic information. 410 ILCS 513/45. | Mental health records require subpoena accompanied by court order authorizing the subpoena. 740 ILCS 110/10(d). |
| Provider's use of records; data aggregation; confidentiality; violations. IC 16-39-5-3 | Disclosure to locate or identify a missing person. IC 16-39-10-4<br>Patient's written consent for release of records. IC 16-39-1-4 | None beyond HIPAA. See Breach Notification Rule, 45 CFR §§ 164.400-414 | See HIPAA (45 C.F.R. § 160.404 Amount of a civil money penalty) | Confidentiality; production on court order. IC 16-39-6-3 |
| None beyond HIPAA. | Authorization for disclosure of mental health information must be written, signed, and contain specific information. IA. Code 228.3 Otherwise, none beyond HIPAA. | None beyond HIPAA. State data breach reporting law does not include health information unless such information is "biometric data." IA Code 715C.1 | None beyond HIPAA. | Participants in state health information network "shall not be compelled by subpoena, court order, or other process of law to access health information through the Iowa health information network in order to gather records or information not created by the participant." IA Code 135d.7. |
| None beyond HIPAA. Kan. Stat. Ann. § 65-6825(a) (West 2021) | None beyond HIPAA. | This state does not identify any reporting and remediation requirements beyond HIPAA with respect to the unlawful disclosure of PHI. | None beyond HIPAA. | None beyond HIPAA. |

| State | How does the State define protected health information? | How does the state define a covered entity (i.e. who is subject to the disclosure laws)? | What additional security obligations exist (beyond HIPAA) for PHI? | What rules are there governing business associates? | What constitutes a breach or unlawful disclosure? |
|---|---|---|---|---|---|
| **KY**<br>Kentucky | Generally same as HIPAA. Ky. Rev. Stat. Ann. § 61.931(6)(f) (West)<br>Right of privacy extends to patient's mental health or chemical dependency, and limits disclosure to an insurer to what is necessary for the insurer to render its services. Ky. Rev. Stat. Ann. § 304.17A-555 (West)<br>All information, records, and reports relating to persons infected with or suspected of being infected with a sexually transmitted disease. Ky. Rev. Stat. Ann. § 214.420 (West) | An agency defined as the executive branch of the government, including, without limitation, public school districts and public universities;<br>Nonaffiliated third parties that have a contract or agreement with an agency and receive personal information from the agency pursuant to the contract or agreement. Ky. Rev. Stat. Ann. § 61.931 (West) | Entities are required to consult and follow policies and procedures established by the local governments or other agencies overseeing the entity, for example, Kentucky Board of Education and Counsel on Postsecondary Education. Ky. Rev. Stat. Ann. § 61.932 (West) | Nonaffiliated third parties are held to the same standards as the agencies. They are required to maintain the policies at least as stringent as those from the entity or agency that they are receiving the PHI. Ky. Rev. Stat. Ann. § 61.932 (West) | General breach notification law not applicable to breaches subject HIPAA. Ky. Rev. Stat. Ann. § 365.732 (West)<br>The unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release<br>(A) unencrypted or unredacted records or data or<br>(B) encrypted data containing PHI along with the confidential process or key to unencrypt the records that comprises or the entity reasonably believes may comprise the security, confidentiality, or integrity of personal information and result in the likelihood of harm to one (1) or more individuals. Ky. Rev. Stat. Ann. § 61.931(9) (West) |
| **LA**<br>Louisiana | Patient Identifying Information is defined as the name, address, social security number, or similar information by which a patient's identity can be determined with reasonable accuracy and speed. La. Admin Code. tit. 48, Pt I, § 503. | Restrictions on disclosure specific to certain entities:<br>• HMOs. La. Rev. Stat. Ann. § 22:2020<br>• State facilities. La. Rev. Stat. Ann. § 44:7; La. Admin. Code tit. 48, pt. I, § 503<br>• Utilization review. La. Rev. Stat. Ann. § 40:2731<br>Restrictions on disclosure specific to certain conditions:<br>• Birth defects. La. Rev. Stat. Ann. § 40:31.44<br>• Cancer. La. Rev. Stat. Ann. § 40:1299.87<br>• Communicable disease. La. Rev. Stat. Ann. § 40:3.1<br>• Genetic test results. La. Rev. Stat. Ann. § 22:213.7<br>• HIV/AIDS. La. Rev. Stat. Ann. § 40:1300.14<br>• Mental health. La. Rev. Stat. Ann. § 28:171<br>• Substance abuse. La. Rev. Stat. Ann. § 37:50.3384 | Requires hospitals to have medical records department responsible for maintaining medical records for each patient and to establish certain standards. La. Admin Code. tit. 48, Pt I, § 9387; *see also* La. Admin Code. tit. 48, Pt I, § 505. | None beyond HIPAA. | No state-specific statute governing breach or unlawful disclosure of PHI beyond federal protections and tort law. |

| What safe harbors or exceptions exist (e.g., close family, death, etc.) | What form may an authorization for disclosure take (e.g., written, verbal, duration)? | What are the State's reporting and remediation requirements in the event of a breach/unlawful exposure? | What penalties exist for failure to report an unlawful exposure? | What rules are there for responding to subpoenas? |
|---|---|---|---|---|
| None beyond HIPAA. | None beyond HIPAA. | Nonaffiliated third parties shall notify the agency in the most expedient time possibly without undue delay but no later than seventy-two (72) hours of determination of a security breach.<br>The report shall include all information that the nonaffiliated third party has with regard to the breach. Ky. Rev. Stat. Ann. § 61.932(2)(b)(1) (West)<br>Reporting may be delayed based on a notice from law a law enforcement agency. Ky. Rev. Stat. Ann. § 61.932(2)(b)(2) (West)<br>Agencies must report the breach to the state officers and departments listed in Ky. Rev. Stat. Ann. § 61.933(1)(a)(1) (West).<br>Notification of individuals affected or likely affected must be notified within 35 days after providing a report to officers listed in section (1)(a)(1) of the completion of an investigation into the breach. Ky. Rev. Stat. Ann. § 61.933(1)(b)(1)(b) (West)<br>Additional requirements must be met where the individuals to be notified exceeds one thousand. Ky. Rev. Stat. Ann. § 61.933(1)(b)(1)(c) (West)<br>Notice to individuals must include information laid out in Ky. Rev. Stat. Ann. § 61.933(2) (West) | None beyond HIPAA. | Psychiatrist-patient privilege not waived. Ky. Rev. Stat. Ann. § 422.330 (West) |
| Child and elder abuse. La. Code Evid. Ann. Art. 510<br>Child custody. La. Code Evid. Ann. Art. 510<br>Proceeding against physician. La. Code Evid. Ann. Art. 510<br>Personal injury or worker's compensation proceeding. La. Code Evid. Ann. Art. 510 | Written and signed by patient or legal representative. La. Rev. Stat. Ann. §§ 13:3734; 40:1165.1(A)(2)(b)(i); La. Admin Code. tit. 48, Pt I, §§ 507, 513. No duration limitation. | None beyond HIPAA. | None beyond HIPAA. | Subpoenaed provider must receive affidavit that subpoena is for records of party to litigation and notice has been mailed to affected patient seven days before issuance. La. Rev. Stat. Ann. § 13:3715.1(B)(1)<br>Subpoenaed provider entitled to reimbursement by person issuing subpoena. La. Rev. Stat. Ann. § 13:3715.1(G) |

| State | How does the State define protected health information? | How does the state define a covered entity (i.e. who is subject to the disclosure laws)? | What additional security obligations exist (beyond HIPAA) for PHI? | What rules are there governing business associates? | What constitutes a breach or unlawful disclosure? |
|---|---|---|---|---|---|
| **ME** Maine | Directly identifiable information relating to condition, medical history, or treatment provided to patient. 22 M.R.S. §1711-C(1)(E) | A health care practitioner or facility licensed by the state to provide health care. 22 M.R.S. §1711-C(1)(D) and (F) | If release of information to the individual would be detrimental, make copy available to authorized representative. 22 M.R.S. §1711-C(10)(C)<br>Disclosure of mental health records outside of practitioner or facility's office in nonemergency situations requires authorization. 22 M.R.S. §1711-C(6)(A)(2) | None beyond HIPAA. | None beyond HIPAA. |
| **MD** Maryland | (k) (1) "Medical record" means any oral, written, or other transmission in any form or medium of information that: (i) Is entered in the record of a patient or recipient; (ii) Identifies or can readily be associated with the identity of a patient or recipient; and (iii) Relates to the health care of the patient or recipient. MD Code, Health-General §4-301(k)(1) | (h) (1) "Health care provider" means: (i) A person who is licensed, certified, or otherwise authorized under the Health Occupations Article or §13–516 of the Education Article to provide health care in the ordinary course of business or practice of a profession or in an approved education or training program; or (ii) A facility where health care is provided to patients or recipients, including a facility as defined in §10–101(g) of this article, a hospital as defined in §19–301 of this article, a related institution as defined in §19–301 of this article, a health maintenance organization as defined in §19–701(g) of this article, an outpatient clinic, a medical laboratory, a comprehensive crisis response center, a crisis stabilization center, and a crisis treatment center established under §7.5–207 of this article. (2) "Health care provider" includes the agents, employees, officers, and directors of a facility and the agents and employees of a health care provider. MD Health-General §4-301(h)(1)-(2) | None beyond HIPAA; See MD Code, Commercial Law, §14-3507 | None beyond HIPAA. | None beyond HIPAA, except:<br>(c) "A health care provider or any other person is in violation of this subtitle if the health care provider or any other person:<br>(1) Requests or obtains a medical record under false pretenses or through deception; or<br>(2) Discloses a medical record in violation of this subtitle." MD Health-General, 4-309(c) |
| **MA** Massachusetts | None beyond HIPAA. | Hospitals and clinics must keep records of the treatment of the cases under their care for 20 years. M.G.L. c. 111, §70 | Patients can require insurance carriers to send their medical information only to them and not policyholder. M.G.L. c. 167O, §27 | None beyond HIPAA. | Under case law, providers generally must not disclose a patient's health information without the patient's written consent, subject to limited exceptions. *Alberts v. Devine*, 395 Mass. 59, 68 (1985) |

| What safe harbors or exceptions exist (e.g., close family, death, etc.) | What form may an authorization for disclosure take (e.g., written, verbal, duration)? | What are the State's reporting and remediation requirements in the event of a breach/unlawful exposure? | What penalties exist for failure to report an unlawful exposure? | What rules are there for responding to subpoenas? |
|---|---|---|---|---|
| Disclosure to another practitioner or facility for in emergency situations permitted. Disclosure to family or household member permitted unless prohibited by the individual. Facility can respond to media or public with brief confirmation of general health status unless prohibited by individual. 22 M.R.S. § 1711-C(6) | Written or oral authorization permitted, but cannot exceed 30 months. 22 M.R.S. § 1711-C(4) | Notification requirements only apply to breach of information from statewide health information exchange. 22 M.R.S. §1711-C(18)(L) | Intentional violation carries penalty up to $5,000 plus costs. Up to $10,000 for practitioners and $50,000 for facilities if repeated. 22 M.R.S. §1711-C(13)(C) | Disclosure without authorization is permitted if responding to subpoena issued by governmental entity. 22 M.R.S. §1711-C(6)(F-2) |
| Immediate family members involved with care of patient; to provide for emergency health care needs of the patient as determined by a health care provider; or appropriate organ, tissue, or eye recovery agency. See MD Health-General, 4-305 | Written; See MD Health-General, 4-303(b)(1) | None beyond HIPAA. | None beyond HIPAA. | See, MD Code –Health General, § 4-306 (Mandatory disclosures of health information) |
| Disclosure of mental health records permitted without a patient's written consent only at DMH's request, pursuant to a court order, or if in patient's best interest and consent not possible or practicable. M.G.L. c. 123, §36; 104 CMR 27.16(9) | None beyond HIPAA. | None beyond HIPAA. | No state-level penalties. State data breach law does not apply to health information. | A hospital or clinic served with a subpoena shall deliver certified copies of the subpoenaed records in its custody to the court or place of hearing designated on the subpoena. M.G.L. c. 111, §70 |

| State | How does the State define protected health information? | How does the state define a covered entity (i.e. who is subject to the disclosure laws)? | What additional security obligations exist (beyond HIPAA) for PHI? | What rules are there governing business associates? | What constitutes a breach or unlawful disclosure? |
|---|---|---|---|---|---|
| **MI** Michigan | "Medical Record" means information oral or recorded in any form or medium that pertains to a patient's health care, medical history, diagnosis, prognosis, or medical condition and that is maintained by a health care provider or health facility in the process of caring for the patient's health. Mich. Comp. Laws Ann. § 333.26263 (West) | Health care providers (licensed or registered to provide health care)<br>Health facility (organized entity where health care provider provides health care services)<br>Medical record company (person who stores, locates, or copies medical records for a health care provider or health facility under a contract or agreement). Mich. Comp. Laws Ann. § 333.26263 (West) | Shall take reasonable steps to verify the identity of the person making the request for a patient's medical data. Mich. Comp. Laws Ann. § 333.26265(g) (West) | None beyond HIPAA. | None beyond HIPAA. |
| **MN** Minnesota | Any information relating to physical or mental health, or condition of patient, or payment for same. Minn. Stat. § 144.291(2)(c) | Any person who provides health care services, including home care providers, health care facilities, assisted living facilities, and physician assistants. Minn. Stat. § 144.291(2)(i) | Provider must maintain records of any release of information without patient consent as authorized by law, within patient's health record. Minn. Stat. § 144.293(9). Health records pertaining to reproductive health care services (services related to pregnancy, contraception, or termination of a pregnancy) may not be released based on a "specific authorization in law" where that authorization is "a law in another state authorizing a civil or criminal subpoena to obtain" reproductive health care records or an order by a court sitting in another state related to enforcement of that state's law. Minn. Stat. 144.2935. Particular disclosure requirements for mental health records. Minn. Stat. § 144.294 | None beyond HIPAA. | "Negligent or intentional" request or release of health records without authorization, forging signatures on consent forms, obtaining consent or health records under false pretenses or intentional access of a record locator or patient information service without authorization. Minn. Stat. § 144.298 |

| What safe harbors or exceptions exist (e.g., close family, death, etc.) | What form may an authorization for disclosure take (e.g., written, verbal, duration)? | What are the State's reporting and remediation requirements in the event of a breach/unlawful exposure? | What penalties exist for failure to report an unlawful exposure? | What rules are there for responding to subpoenas? |
|---|---|---|---|---|
| Upon death either personal representative, heirs at law, or beneficiary of life insurance policy. Mich. Comp. Laws Ann. § 333.26263 (West) | Explicit written authorization; OR<br>Upon death either personal representative, heirs at law, or beneficiary of life insurance policy.<br>Mich. Comp. Laws Ann. § 333.26263 (West) | An entity to which the statute applies shall provide notice of the breach to each resident of MI if (a) the resident's unencrypted and unredacted personal information was accessed and acquired by an unauthorized person or (b) the resident's personal information was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key.<br>Notification is not required if the entity determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, one or more residents.<br>Notice shall be provided without unreasonable delay subject to measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database. Mich. Comp. Laws Sec. 445.72 | Disclosure of confidential medical information from the Department of Health is a misdemeanor, punishable by fine, imprisonment, or both. Mich. Comp. Laws Ann. § 333.2638 (West)<br>A person that knowingly fails to provide any notice of a security breach required under this section may be ordered to pay a civil fine of not more than $250.00 for each failure to provide notice. Mich. Comp. Laws Sec. 445.72 | Health information gathered as part of a professional review or institution of higher learning is not discoverable. Mich. Comp. Laws Ann. § 333.21515 (West); Mich. Comp. Laws Ann. § 333.20175(8) (West) |
| Consent not required for medical emergency where patient consent cannot be obtained, to other providers within related health care entities when necessary for treatment. Minn. Stat. § 144.293(5) | Consent must be in writing, signed and dated, and valid for one year unless consent states otherwise, or as otherwise provided by law. Minn. Stat. § 144.293(2) and (4) | None specified. | No specific penalties for failure to report in state law. Civil liability to patient for unauthorized disclosure, and subject to disciplinary action by licensing board. Minn. Stat. § 144.298 | None beyond HIPAA. |

| State | How does the State define protected health information? | How does the state define a covered entity (i.e. who is subject to the disclosure laws)? | What additional security obligations exist (beyond HIPAA) for PHI? | What rules are there governing business associates? | What constitutes a breach or unlawful disclosure? |
|---|---|---|---|---|---|
| **MS**<br>Mississippi | No comprehensive statute governing PHI beyond HIPAA; privacy is addressed in separate statutes governing specific types of entities and conditions.<br>The Mississippi Insurance Department adopted a privacy regulation governing disclosure of "nonpublic personal health information" by "licensees" (i.e., insurers), which are required to comply with the regulation unless they satisfy HIPAA requirements. 19 Miss. Admin. Code Pt. 1, R. § 28.20<br>Under these regulations, "nonpublic personal health information" is any information that relates to the individual's health condition, provision of health care, or payment for health care, and that can be used to identify the individual. 19 Miss. Admin. Code Pt. 1, R. § 28.04(U), 28.04(O) | Restrictions on disclosure specific to certain entities:<br>• Counselors. Miss. Code Ann. § 73-30-17<br>• Health care practitioners. Miss. Code Ann. § 13-1-21.<br>• HMOs and PPOs. Miss. Code Ann. § 83-41-355<br>• Hospice. Miss. Code Ann. § 41-85-23<br>• Hospitals. Miss. Code Ann. § 41-9-67<br>• Insurers. 19 Miss. Admin. Code Pt. 1, R. §§ 28.04(Q), 28.17(A)<br>• Nursing homes. Miss. Code Ann. § 43-11-16<br>• Mental health facilities. Miss. Code Ann. § 41-21-97<br>• Psychologists. Miss. Code Ann. § 73-31-29<br>• Social workers. Miss. Code Ann. § 73-53-29<br>• Substance abuse facilities. Miss. Code Ann. § 41-30-33<br>• Utilization review agents. Miss. Code Ann. § 41-83-17 | Restrictions on disclosure specific to certain conditions:<br>• Substance abuse. Miss. Code Ann. §§ 41-41-14, 71-7-15, 71-3-219, and 41-31-17<br>• Birth defects. Miss. Code Ann. § 41-21-205<br>• Cancer. Miss. Code Ann. § 41-91-11<br>• Communicable diseases. Miss. Code Ann. § 41-23-1.<br>• HIV/AIDS. Miss. Code Ann. § 41-34-7<br>• Mental illness. Miss. Code Ann. § 41-21-97 | None beyond HIPAA. | No state-specific statute governing breach or unlawful disclosure of PHI beyond federal protections and tort law. |
| **MO**<br>Missouri | Individual's first name or initial with last name, plus unencrypted medical or health information. Mo. Stat. § 407.1500(1)(5)-(1)(6). Among other records. Mo. Stat. § 407.1500(1)(9) | Individual or entity that: (1) conducts business in MO and possesses MO resident health information or (2) owns or licenses MO resident health information. Mo. Stat. § 407.1500(2)(1) | Restrictions on disclosure specific to certain circumstances:<br>• Testing results. Mo. Stat. § 191.317(1).<br>• Mental health and substance abuse records. Mo. Stat. § 630.140.<br>• Nursing homes. Mo. Stat. § 198.032.<br>• Health maintenance organizations. Mo. Stat. § 354.515.<br>• Genetic information. Mo. Stat. § 375.1309.<br>• Abortion reports. Mo. Stat. § 188.055(2).<br>• Newborn hearing screening results. Mo. Stat. § 191.928.<br>• HIV status. Mo. Stat. § 191.656(5).<br>• Identifying information in cancer reports submitted to DHSS. Mo. Stat. § 192.655.<br>• Brain injury records maintained by rehabilitation or treatment facilities. Mo. Stat. § 199.033(1). | Included in definition of "covered entity." | Unauthorized access to or acquisition of personal information in a manner that compromises the information's security, confidentiality, or integrity. Mo. Stat. § 407.1500(1)(1) |

| What safe harbors or exceptions exist (e.g., close family, death, etc.) | What form may an authorization for disclosure take (e.g., written, verbal, duration)? | What are the State's reporting and remediation requirements in the event of a breach/unlawful exposure? | What penalties exist for failure to report an unlawful exposure? | What rules are there for responding to subpoenas? |
|---|---|---|---|---|
| Insurance functions. 19 Miss. Admin. Code Pt. 1, R. § 28.17(B)<br>Disclosure necessary to prevent crime, violence, or suicide. Miss. Code Ann. §§ 73-30-17, 41-21-97<br>Litigation between person and HMO. Miss. Code Ann. § 83-41-355<br>Court order. Miss. Code Ann. § 41-21-97<br>Necessary for continued treatment of patient. Miss. Code Ann. § 41-21-97<br>Necessary for benefits determination. Miss. Code Ann. § 41-21-97 | Written and signed by subject of nonpublic personal health information or their representative. 19 Miss. Admin. Code Pt. 1, R. § 28.18(A); Miss. Code Ann. § 41-21-97. Valid for two years. 19 Miss. Admin. Code Pt. 1, R. § 28.18(C) | None beyond HIPAA. | None beyond HIPAA. | None beyond HIPAA. |
| Disclosure necessary for law enforcement to carry out duties. Mo. Stat. § 630.140(2)(5).<br>Entities authorized to advocate the rights of persons with developmental disabilities or mental illnesses. Mo. Stat. § 630.140(2)(6)-(2)(7).<br>Litigation between person and HMO. Mo. Stat. § 354.515(1)(4).<br>Release of genetic information necessary for body identification. Mo. Stat. § 375.1309(4).<br>Insurance functions. Mo. Stat. § 199.033(3)(3)<br>Prosecutorial purposes. Mo. Stat. § 191.656(1)(1)(d), (1)(1)(g). | None specified. | Disclose without unreasonable delay to affected consumer, and if applicable, the Attorney General and consumer reporting agencies. Mo. Stat. § 407.1500(2)(1), (2)(8). Notice must include a description of the incident, a telephone number to call for further assistance, contact information for consumer reporting agencies, and advice to remain vigilant by reviewing account statements and monitoring free credit reports. Mo Stat. § 407.1500(2)(4). Notice can be written, electronic (for those with a valid email address and who have consented to electronic communications), or telephonic. Mo. Stat. § 407.1500(2)(6). | Actual damages and up to $150,000 in civil penalties per breach. Mo. Stat. § 407.1500(4). | None beyond HIPAA. |

| State | How does the State define protected health information? | How does the state define a covered entity (i.e. who is subject to the disclosure laws)? | What additional security obligations exist (beyond HIPAA) for PHI? | What rules are there governing business associates? | What constitutes a breach or unlawful disclosure? |
|---|---|---|---|---|---|
| **MT** Montana | Enacted the Uniform Health Care Information Act in 1987 and then amended it in 2003 to only apply to those entities NOT covered by HIPAA. MCA 50-16-501. | None beyond HIPAA. | The recently enacted Montana Consumer Data Privacy Act ("MCDPA") which takes effect on October 1, 2024 is a comprehensive privacy law. While protected health information under HIPAA is exempted, the MCDPA regulates a variety of "personal data" and "sensitive data." | None beyond HIPAA. | None beyond HIPAA. |
| **NE** Nebraska | Health Information: Information or data, whether oral or recorded in any form or medium, and personal facts or information about events or relationships that relates to: (a) The past, present, or future physical, mental, or behavioral health or condition of an individual or a member of the individual's family; (b) The provision of health care services to an individual; or (c) Payment for the provision of health care services to an individual. Neb. Rev. St. § 44-1303(28).<br>Protected Health Information: Health information that identifies an individual who is the subject of the information or with respect to which there is a reasonable basis to believe that the information could be used to identify an individual. Neb. Rev. St. § 44-1303(32). | Health care professionals, health care providers, and health carriers. Neb. Rev. St. § 44-1303(24)-(27). | • Physician's must conform to the American Medical Association's Code of Medical Ethics, and must keep and maintain adequate records of treatment or service. Neb. Admin. R. & Regs. Tit. 172, Ch. 88, § 013.<br>• Hospitals must maintain confidential medical records for at least ten years after a patient's discharge or three years after a child patient reaches the age of eighteen. Medical records must include the patient's identity, diagnosis, and lab reports. Neb. Admin. R. & Regs. Tit. 175, Ch. 9, § 006.<br>• Information disclosed in the best interest of a child regarding abuse or neglect may not include protected health information. Neb. Rev. St. § 81-3126(3). | Confidentiality required. | Unauthorized acquisition of unencrypted personal information. Neb. Rev. St. § 87-802(1).<br>Knowingly disclosing confidential information except as otherwise permitted by law. Neb. Rev. St. § 38-179(8). |

| What safe harbors or exceptions exist (e.g., close family, death, etc.) | What form may an authorization for disclosure take (e.g., written, verbal, duration)? | What are the State's reporting and remediation requirements in the event of a breach/unlawful exposure? | What penalties exist for failure to report an unlawful exposure? | What rules are there for responding to subpoenas? |
|---|---|---|---|---|
| None beyond HIPAA. | None beyond HIPAA. | None beyond HIPAA. | None beyond HIPAA. | None beyond HIPAA. |
| • In the case of death or disability: Personal representative may consent to mental health information disclosure. Neb. Rev. St. § 38-2136(1).<br>• Duty to warn of patient's threatened violent behavior. Neb. Rev. St. § 38-2137.<br>• Improper disclosure made in good faith. Neb. Rev. St. § 71-8406.<br>• Disclosure necessary for the performance of insurance functions. Neb. Rev. St. § 44-916(2). | • Written request. Neb. Rev. St. § 71-8403(2).<br>• Authorization expires twelve months after the authorization was executed by the patient, unless the authorization specifies differently. Neb. Rev. St. § 71-8403(1).<br>• For disclosure for purposes of insurance, authorization may be in written or electronic form and must include the identity of the subject of the information, the signature of the consumer who is the subject of the information, and the length of time the authorization is valid, not exceeding twenty-four months. Neb. Rev. St. 44-917(1)-(2). | Disclose without unreasonable delay in Written, Electronic, or Substitute Notice form to affected consumer and Attorney General. Neb. Rev. St. § 87-802(4). | Direct economic damages for each affected NE resident. Neb. Rev. St. § 87-806. | No authorization required when responding to subpoena. Neb. Rev. St. § 87-802(1).<br>A provider complying with a subpoena may charge no more than $20 as a handling fee and no more than $0.50 per page as a copying fee. Neb. Rev. St. § 71-8404. |

| State | How does the State define protected health information? | How does the state define a covered entity (i.e. who is subject to the disclosure laws)? | What additional security obligations exist (beyond HIPAA) for PHI? | What rules are there governing business associates? | What constitutes a breach or unlawful disclosure? |
|---|---|---|---|---|---|
| **NV**<br>Nevada | [A] natural person's first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted: (1) Social security number. (2) Driver's license number or identification card number. (3) Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account. NRS 603A.040 | Any data collector that owns or licenses computerized data which includes personal information.<br>A "data collector" is "any governmental agency, institution of higher education, corporation, financial institution or retail operator or any other type of business entity or association that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates or otherwise deals with nonpublic personal information. NRS 603A.220(1) (amended on other grounds by 2023 Nevada Laws Ch. 527 (S.B. 355))<br>NRS 603A.030 | None beyond HIPAA. | None beyond HIPAA. | A "breach of the security of the system data" is the "unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the data collector." NRS 603A.020 |

| What safe harbors or exceptions exist (e.g., close family, death, etc.) | What form may an authorization for disclosure take (e.g., written, verbal, duration)? | What are the State's reporting and remediation requirements in the event of a breach/unlawful exposure? | What penalties exist for failure to report an unlawful exposure? | What rules are there for responding to subpoenas? |
|---|---|---|---|---|
| For establishing own notification method:<br>"A data collector which maintains its own notification policies and procedures as part of an information security policy for the treatment of personal information that is otherwise consistent with the timing requirements of this section shall be deemed to be in compliance with the notification requirements of this section if the data collector notifies subject persons in accordance with its policies and procedures in the event of a breach of the security of the system data." NRS 603A.220(5)(a) (amended on other grounds by 2023 Nevada Laws Ch. 527 (S.B. 355))<br>For following interagency guidelines:<br>A data collector which "[i] s subject to and complies with the privacy and security provisions of the Gramm-LeachBliley Act, 15 U.S.C. §§6801 et seq., shall be deemed to be in Compliance with the Notification requirements of this section." NRS 603A.220(5)(b) ) (amended on other grounds by 2023 Nevada Laws Ch. 527 (S.B. 355)) | None beyond HIPAA. | Method: "[T]he notification required by this section may be provided by one of the following methods: (a) Written notification. (b) Electronic notification, if the notification provided is consistent with the provisions of the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001 et seq. (c) Substitute notification, if the data collector demonstrates that the cost of providing notification would exceed $250,000, the affected class of subject persons to be notified exceeds 500,000 or the data collector does not have sufficient contact information." NRS 603A.220(4) (amended on other grounds by 2023 Nevada Laws Ch. 527 (S.B. 355))<br>Timing: Following discovery or notification of the breach, "disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in [§603A.220(3)], or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system data." NRS 603A.220(1) (amended on other grounds by 2023 Nevada Laws Ch. 527 (S.B. 355)) | Violation of Deceptive Trade Practices. "A violation of the provisions of NRS 603A.010 to 603A.290, inclusive, constitutes a deceptive trade practice" under NRS 598.0903 to 598.0999.<br>Nev. Rev. Stat. Ann. § 603A.260<br>Private Right of Action:<br>"A data collector that provides the notification required pursuant to NRS 603A.220 may commence an action for damages against a person that unlawfully obtained or benefited from personal information obtained from records maintained by the data collector. A data collector that prevails in such an action may be awarded damages which may include, without limitation, the reasonable costs of notification, reasonable attorney's fees and costs and punitive damages when appropriate. The costs of notification include, without limitation, labor, materials, postage and any other costs reasonably related to providing the notification." NRS 603A.270<br>Restitution also available: "In addition to any other penalty provided by law for the breach of the security of the system data maintained by a data collector, the court may order a person who is convicted of unlawfully obtaining or benefiting from personal information obtained as a result of such breach to pay restitution to the data collector for the reasonable costs incurred by the data collector in providing the [required] notification . . . including, without limitation, labor, materials, postage and any other costs reasonably related to providing such notification." NRS 603A.280<br>Injunction/State enforcement: "If the Attorney General or a district attorney of any county has reason to believe that any person is violating, proposes to violate or has violated the provisions of this chapter, he may bring an action against that person to obtain a temporary or permanent injunction against the violation." NRS 603A.290 | N/A |

| State | How does the State define protected health information? | How does the state define a covered entity (i.e. who is subject to the disclosure laws)? | What additional security obligations exist (beyond HIPAA) for PHI? | What rules are there governing business associates? | What constitutes a breach or unlawful disclosure? |
|---|---|---|---|---|---|
| **NH** New Hampshire | Same definition as HIPAA. RSA 332-I:1(a)(4) | Hospital, building, residence, or other place or part thereof, licensed by the state. RSA 151:21(X) | Authorization is required to disclose for marketing and fundraising, only certain distribution methods allowed. Election not to receive fundraising communication is a revocation of authorization under HIPAA. RSA 332-I:4 | None beyond HIPAA. RSA 332-I:1, II(a)(1) | Physician/patient communications are placed on the same basis as those provided by law between attorney and client. Except as otherwise provided by law, no such physician or surgeon shall be required to disclose such privileged communications. RSA 329-B:26 |
| **NJ** New Jersey | Follows HIPAA. N.J. STAT. ANN.§56:8-196 ("Identifiable health information" means individually identifiable health information as defined in 45 C.F.R. §160.103)<br>"personal information" for purposes of notice of breach separately defined at N.J. STAT. ANN. §56:8-161; N.J. STAT. ANN. §56:8-196 | New Jersey does not have a comprehensive statute which protects the privacy of confidential *medical* information. Rather, New Jersey has a comprehensive statute applicable to all businesses and personal information. *See generally* Title 56 and N.J. STAT. ANN.§ 56:8-163 (notice of data breach applicable to any business that compiles or maintains computerized records that contain personal information) There are also specific privacy protections applicable to various medical facilities: General, psychiatric and special hospitals in New Jersey. N.J. ADMIN. CODE § 8:43G-15.2<br>and<br>Practitioners. N.J. ADMIN. CODE §13:35-6.5 | Any business who conducts business in [New Jersey ] and maintains personal information shall disclose breach of security. N.J. STAT. 56.8-163. *See generally*, industry specific guidelines such as §56:8-197(a) and Title 26, Health and Vital Statistics, which includes specific privacy protections applicable to various medical facilities such as hospitals.<br>*See also*, Genetic information protected under N.J. STAT. ANN. § 10:5-45.<br>In addition, restrictions on disclosure specific to certain conditions, such as reporting of communicable diseases or gunshot wounds or suspected child abuse, etc., or when the patient's treatment is the subject of peer review. N.J. ADMIN. CODE §13:35-6.5(d); *see also* N.J. STAT. ANN.§ 30:4-24.3 (mental health) or HIV/AIDS, N.J. STAT. ANN.§ 26:5C-9.<br>Also industry-specific guidelines regarding statutory data encryption or any other method or technology rendering the information unreadable, undecipherable, or otherwise unusable by an unauthorized person of personal information. *See e.g.* N.J. STAT. ANN. §56:8-197(a) | Notice of data breach applicable to business with access to personal information if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person. N.J. STAT. ANN .§56:8-163(b)<br>Health Insurance carriers also subject to act which includes an insurance company, health service corporation, hospital service corporation, medical service corporation, or health maintenance organization authorized to issue health benefits plans in New Jersey. N.J. STAT. ANN. §56:8-196 | A "breach of security" is the "unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable." N.J. STAT. ANN.§56:8-161 |

| What safe harbors or exceptions exist (e.g., close family, death, etc.) | What form may an authorization for disclosure take (e.g., written, verbal, duration)? | What are the State's reporting and remediation requirements in the event of a breach/unlawful exposure? | What penalties exist for failure to report an unlawful exposure? | What rules are there for responding to subpoenas? |
|---|---|---|---|---|
| None beyond HIPAA. | No specific form required. | If PHI is disclosed for marketing or fundraising in a manner that complies with HIPAA, but not RSA 332-I:4, the health care provider shall promptly notify in writing the individual(s) whose PHI was disclosed. Business associate responsible for cost if it was the disclosing party. RSA 332-I:5 | If successful in civil suit, court shall award damages of not less than $1,000 for each violation, and costs and reasonable legal fees. RSA 332-I:6 | Information about HIV testing obtained by subpoena shall not be released or made public outside of the proceedings. RSA 141-F:8 |
| "Good faith acquisition of personal information by an employee or agent of the business for a legitimate business purpose is not a breach of security, provided that the personal information is not used for a purpose unrelated to the business or subject to further unauthorized disclosure." N.J. STAT. ANN.§56:8-161<br>Maintenance of and compliance with an entity's own notification process as part of a privacy or security policy and otherwise consistent with the NJ Act, shall be deemed in compliance with notice requirements. N.J. STAT. ANN.§56:8-163(e) | "in accordance with the statute" *See e.g.* N.J. STAT. ANN.§ 30:4-24.3 or with patient approval. Jersey. N.J. ADMIN. CODE § 8:43G-4.1 (21) written authorization. N.J. ADMIN. CODE §13:35-6.5(d) | Notice of breach "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system" except no disclosure necessary if misuse of the information is not reasonably possible. N.J. STAT. ANN.§56:8-163(a)<br>Industry specific enforcement. For example, N.J. STAT. ANN.§26:2H-13 provides for the imposition of administrative penalties if a hospital violates a patient's rights. Those penalties include fines and suspension or revocation of all licenses<br>Also required to Division of State Police in the Department of Law and Public Safety of the Office of the Attorney General.. If breach involves more than 100 residents, required to notify consumer reporting agencies. | No statute specifically tied to failure to report. Instead, statutes provide that it shall be an unlawful practice and a violation of [the New Jersey Consumer Fraud Act] to willfully, knowingly or recklessly violate [the breach notification law]." N.J. STAT. ANN.§56:8-166<br>"It shall be an unlawful practice and a violation of [the New Jersey Consumer Fraud Act] to violate the provisions of [title 56]." N.J. STAT. ANN.§56:8-198 | Requires HIPAA compliant release, or court order, *see e.g.* N.J. STAT. ANN.§ 30:4-24.3, or subpoena issued by Bd of Medical Examiners or Attorney General, or demand in writing, N.J. ADMIN. CODE §13:35-6.5 (d) |

| State | How does the State define protected health information? | How does the state define a covered entity (i.e. who is subject to the disclosure laws)? | What additional security obligations exist (beyond HIPAA) for PHI? | What rules are there governing business associates? | What constitutes a breach or unlawful disclosure? |
|---|---|---|---|---|---|
| **NM** New Mexico | Undefined. This state excludes individuals/ entities covered by HIPAA from its Data Breach Notification Act. Apply federal HIPAA for this category. N.M. Stat. Ann. § 57-12C-8 (West 2021) | Undefined. This state excludes individuals/ entities covered by HIPAA from its Data Breach Notification Act. Apply HIPAA for this category. N.M. Stat. Ann. § 57-12C-8 (West 2021)<br>There are additional disclosure laws that govern specific entities—*e.g.*, mental health counselors? (*See* – N.M. Code R. § 16.27.18.17)<br>There are also confidentiality requirements for HIV testing (the testing itself and the results). N.M. Stat. Ann. §24-2B-6 | Additional requirements for medical records in long-term care facilities. *See* N.M. Code R. §7.9.2.31.<br>Also, "[p]roviders who choose to send or receive confidential medical information via fax must have a dedicated fax line or fax machine. Confidential medical information should not be received at a commercial fax center where employees or customers may have access to the information. Providers who choose to send or receive confidential medical information via fax or email must follow the minimum necessary standard." N.M. Code R. §8.300.11.11B | None beyond HIPAA. N.M. Stat. Ann. § 57-12C-8 (West 2021) | Undefined. This state excludes individuals/ entities covered by HIPAA from its Data Breach Notification Act. Thus, HIPAA applies for this category. N.M. Stat. Ann. § 57-12C-8 (West 2021) |
| **NY** New York | "Patient Information": "information concerning or relating to examination, health assessment, including but not limited to health assessment for insurance or employment purposes or treatment maintained or possessed by a health care facility or health care practitioner." NY Public Health Law § 18<br>See NY HIPAA Preemption Charts for the scope of PH– in NY - NY Public Health Law § 17 and § 18<br>(https://www.health.ny.gov/regulations/hipaa/preemption_charts.htm) | "References covered entities, as defined in section 340B of the public health service act [42 U.S.C. § 256b], to facilitate their participation in such drug discount program." NY Public Health Law § 206<br>See NY HIPAA Preemption Charts for the scope of "covered entity" in NY - NY Public Health Law § 206<br>(https://www.health.ny.gov/regulations/hipaa/preemption_charts.htm) | None beyond HIPAA. | NY Statute doesn't have a definition for Business Associate, but its definition of "Authorized Third Party" includes "a third party legally authorized under state or federal law subject to a [HIPAA] business associate agreement." NY Public Health Law § 4408. | Disclosure of certain HIV information, disclosure of information required to be collected under state law, or unauthorized disclosure by a health maintenance organization or its comprehensive health services plan can constitute a breach or unlawful disclosure. See NY HIPAA Preemption Charts for the NY Public Health Law § 2782, § 2805-m, § 4410(2)<br>(https://www.health.ny.gov/regulations/hipaa/preemption_charts.htm).<br>Disclosure of certain abortion-related or venereal disease-related information for a minor cannot be disclosed to parent or guardian without consent. NY Public Health Law § 17. |
| **NC** North Carolina | N/A; HIPAA Privacy Rule governs.<br>Personal information defined in N.C. Gen. Stat. Ann. § 75-61 (10) | North Carolina does not have a comprehensive statute which protects the privacy of confidential medical information. HIPAA privacy rule governs, however some breaches may be subject to N.C. Gen. Stat. Ann. § 75-65, which governs any that business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form. N.C. Gen. Stat. Ann. § 75-65 | Notice required of any security breach without unreasonable delay or immediately following discovery. N.C. Gen. Stat. § 75-65 | None beyond HIPAA. | An incident of unauthorized access to and acquisition of unencrypted and unredacted records (or encrypted data along with the confidential process or key) or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. See, N.C. Gen. Stat. §§ 75-6165 |

| What safe harbors or exceptions exist (e.g., close family, death, etc.) | What form may an authorization for disclosure take (e.g., written, verbal, duration)? | What are the State's reporting and remediation requirements in the event of a breach/unlawful exposure? | What penalties exist for failure to report an unlawful exposure? | What rules are there for responding to subpoenas? |
|---|---|---|---|---|
| None beyond HIPAA. N.M. Stat. Ann. § 57-12C-8 (West 2021) | None beyond HIPAA. N.M. Stat. Ann. § 57-12C-8 (West 2021) | None beyond HIPAA. N.M. Stat. Ann. § 57-12C-8 (West 2021) | None beyond HIPAA. N.M. Stat. Ann. § 57-12C-8 (West 2021) | None beyond HIPAA. N.M. Stat. Ann. § 57-12C-8 (West 2021) |
| Court authorization for disclosure of confidential HIV related information. McKinney's Public Health Law § 2785<br>Certain information can be disclosed to authorized third parties, family members, or those "authorized pursuant to law to consent to health care." *See* NY Public Health Law §§ 2782, 4408 | HIV and AIDs information requires capacity to consent and a written authorization.. McKinney's Public Health Law § 2780(5), (9)<br>Confidentiality and disclosure. McKinney's Public Health Law § 2782 | NY SHIELD Act S.Sec. 5575B Chapter 117: requirements for safeguards for confidential information.<br>https://ag.ny.gov/resources/organizations/data-breach-reporting/shield-act. | Penalties; immunities. McKinney's Public Health Law § 2783: civil penalty of up to $5,000 per occurrence; willful misconduct is a misdemeanor.<br>NY SHIELD Act S.Sec. 5575B Chapter 117, civil penalties of up to $250,000 for failure to timely notify of records breach; up to $5,000 per violation for failure to maintain reasonable safeguards. | Objection to disclosure, inspection or examination; compliance. McKinney's CPLR Rule 3122 |
| None beyond HIPAA. | None beyond HIPAA. | Entity shall provide notice to the affected entity without unreasonable delay if the business owns or licenses the personal information, or immediately following discovery of the breach of if the entity does not own or license the personal information. See, N.C. Gen. Stat. §§ 75-61, 75-65<br>Notice must be conspicuous and provide, for example, information relating to the personal information accessed and contact information for assistance. N.C. Gen. Stat. Ann. § 75-65(d)<br>Notice can be provided in several forms, for example, written notice, email, telephonic, etc. N.C. Gen. Stat. Ann. § 75-65(e) | No private right of action may be brought by an individual for a violation of this section unless such individual is injured as a result of the violation. N.C. Gen. Stat. Ann. § 75-65(i).<br>Attorney General may bring action for violation. Civil penalty of up to five thousand dollars ($5,000 for each violation. N.C. Gen. Stat. Ann. § 75-15.2 | None beyond HIPAA. |

| State | How does the State define protected health information? | How does the state define a covered entity (i.e. who is subject to the disclosure laws)? | What additional security obligations exist (beyond HIPAA) for PHI? | What rules are there governing business associates? | What constitutes a breach or unlawful disclosure? |
|---|---|---|---|---|---|
| **ND** North Dakota | Individual's first name or initial with last name, plus unencrypted medical or health insurance information (as defined in N.D.C.C., 51-30-01), among other items. | Person who owns or licenses computerized personal information. N.D.C.C., as defined in 51-30-01. | None beyond HIPAA. | Included in definition of "covered entity." | Unauthorized acquisition of unencrypted personal information. N.D.C.C., 51-30-01(1) |
| **OH** Ohio | Same as HIPAA. Same definition as provided in 45 C.F.R. § 160.103. Oh. Rev. Code. Sec. 3798.01 | Same as HIPAA. Same definition as provided in 45 C.F.R. § 160.103. Oh. Rev. Code. Sec. 3798.01 | None specific to PHI.<br>However, Ohio has consumer protection laws that similarly protect consumer data.<br>Oh. Rev. Code. Sec. 3798.03 | Ohio Office of Information and Security has prepared a HIPAA Business Associate Agreement Template. See here. | None beyond HIPAA. Same as defined in 45 C.F.R. part 2. Oh. Rev. Code Sec. 3798.04 |
| **OK** Oklahoma | Undefined. "Personal Information" means: Resident's name plus:<br>• Social security number;<br>• Driver's license number;<br>• Financial account number; or<br>• Other specified information. Okla. Stat. Ann. tit. 24, § 162 (West 2021) | Undefined. This state's disclosure laws apply to all individuals or entities that own or license computerized data that includes personal information. Okla. Stat. Ann. tit. 24, § 163 (West 2021) | None beyond HIPAA. This state does not define PHI. Okla. Stat. Ann. tit. 24, § 162, et seq. (West 2021) | None beyond HIPAA. Okla. Stat. Ann. tit. 24, § 162, et seq. (West 2021) | Unauthorized data acquisition that compromises PI confidentiality and causes its maintainer to reasonably believe that fraud will occur to resident. Okla. Stat. Ann. tit. 24, § 162 (West 2021) |

| What safe harbors or exceptions exist (e.g., close family, death, etc.) | What form may an authorization for disclosure take (e.g., written, verbal, duration)? | What are the State's reporting and remediation requirements in the event of a breach/unlawful exposure? | What penalties exist for failure to report an unlawful exposure? | What rules are there for responding to subpoenas? |
|---|---|---|---|---|
| Good faith acquisition by employee or agent for authorized disclosure. N.D.C.C., 51-30-01(1) | None beyond HIPAA. | Disclose in most expedient time possible to affected consumer and if applicable, the Attorney General. N.D.C.C., 51-30-02 to 51-30-05 | Up to $5,000 per violation. N.D.C.C. 51-30-07 & 51-15-11 | None beyond HIPAA. |
| No specific safe harbors defined. Potential safe harbor from tort liability under the Ohio Data Protection Act. | Properly executed form by an individual or the individual's personal representative that meets the requirements specified in 45 C.F.R. 164.508 and if applicable 42 C.F.R. part 2. Oh. Rev. Code Sec. 3798.10 | General privacy laws that do not identify PHI. Oh. Rev. Code Sec. 1349.191 | Civil Action by attorney general pursuant to the Security Breach Notification Act. Oh. Rev. Code Sec. 1349.192 | None specific to HIPAA, however there remains privilege between a patient and their physician, advanced practice registered nurse, and dentist that may bar response. Oh. Rev. Code Sec. 2317.02(B) |
| None beyond HIPAA. Okla. Stat. Ann. tit. 24, § 163 (West 2021) | None beyond HIPAA. | Prompt notification of resident who is subject of the PI if the maintainer reasonably believes the disclosure will cause fraud. Okla. Stat. Ann. tit. 24, § 163 (West 2021) | State AG or DA may file lawsuit for actual damages or civil penalty up to $150,000 per breach. Okla. Stat. Ann. tit. 24, § 165 (West 2021) | None beyond HIPAA. |

| State | How does the State define protected health information? | How does the state define a covered entity (i.e. who is subject to the disclosure laws)? | What additional security obligations exist (beyond HIPAA) for PHI? | What rules are there governing business associates? | What constitutes a breach or unlawful disclosure? |
|---|---|---|---|---|---|
| **OR**<br>Oregon | Individually identifiable health information that is maintained or transmitted in any form of electronic or other medium by a covered entity.<br>"Protected health information" does not mean individually identifiable health information in:<br>(A) Education records covered by the federal Family Educational Rights and Privacy Act (20 U.S.C. 1232g);<br>(B) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); or<br>(C) Employment records held by a covered entity in its role as employer.<br>ORS § 192.556 | (A) A state health plan;<br>(B) A health insurer;<br>(C) A health care provider that transmits any health information in electronic form to carry out financial or administrative activities in connection with a transaction covered by ORS 192.553 (Policy for protected health information) to 192.581 (Allowed retention or disclosure of genetic information); or<br>(D) A health care clearinghouse.<br>ORS § 192-556 | None beyond HIPAA. | "Business Associate" means an individual or entity performing any function or activity on behalf of the Authority involving the use or disclosure of protected health information (PHI) and is not a member of the Authority's workforce.<br>(A) "Function or activity" includes but is not limited to program administration, claims processing or administration, data analysis, utilization review, quality assurance, billing, legal, actuarial, accounting, consulting, data processing, management, administrative, accreditation, financial services, and similar services for which the Authority may contract or obtain by interagency agreement, if access to PHI is involved.<br>(B) Business associates do not include licensees or providers unless the licensee or provider also performs some function or activity on behalf of the Authority.<br>OAR 943-014-0000 | "Breach" has the meaning given that term in 45 CFR 164.402. OAR 943-014-0410 |

| What safe harbors or exceptions exist (e.g., close family, death, etc.) | What form may an authorization for disclosure take (e.g., written, verbal, duration)? | What are the State's reporting and remediation requirements in the event of a breach/unlawful exposure? | What penalties exist for failure to report an unlawful exposure? | What rules are there for responding to subpoenas? |
|---|---|---|---|---|
| A health care provider may use or disclose protected health information of an individual without obtaining an authorization from the individual or a personal representative of the individual if the conditions in paragraph (b) of this subsection are met and:<br>(A) The disclosure is to a family member, other relative, a close personal friend or other person identified by the individual, and the protected health information is directly relevant to the persons involvement with the individuals health care; or<br>(B) The disclosure is for the purpose of notifying a family member, a personal representative of the individual or another person responsible for the care of the individual of the individual's location, general condition or death.<br>A health care provider may make the disclosures described in paragraph (a) of this subsection if:<br>(A) (i) The individual is not present or obtaining the individual's authorization is not practicable due to the individuals incapacity or an emergency circumstance; and<br>(ii) In the exercise of professional judgment and based on reasonable inferences, the health care provider determines that the disclosure is in the best interests of the individual; or<br>(B) The individual is present and the health care provider gives the individual an opportunity to object to the disclosure and the individual does not express an objection or the health care provider reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure.<br>ORS §192.567<br>Disclosure of patient records maintained by state-run public health providers permitted "to the extent necessary to meet a medical emergency." ORS §179.505(4)(a). | Authorization form template provided. ORS §192.566 | For the purposes of this rule a breach is considered "discovered" in accordance with 45 CFR 164.404(a)(2) and 45 CFR 164.410(2). OAR 943-014-0440 | None beyond HIPAA. | N/A |

| State | How does the State define protected health information? | How does the state define a covered entity (i.e. who is subject to the disclosure laws)? | What additional security obligations exist (beyond HIPAA) for PHI? | What rules are there governing business associates? | What constitutes a breach or unlawful disclosure? |
|---|---|---|---|---|---|
| **PA** Pennsylvania | Pennsylvania's Breach of Personal Notification Act (BPINA) includes breach notification requirements for entities that maintain, store, or manage computerized data that includes "personal information." 73 Pa. Cons. Stat. Ann. §2303(a). BPINA defines "personal information" to mean "an individual's first name or first initial and last name in combination with and linked to" at least one of several elements, including "medical information." 73 PA. CONS. STAT. ANN. §2302. BPINA defines "medical information" as "[a]ny individually identifiable information contained in the individual's current or historical record of medical history or medical treatment or diagnosis created by a health care professional." *Id.*<br>However, entities subject to and in compliance with privacy and security standards for the protection of electronic personal health information under HIPAA are deemed to be in compliance with BPINA. 73 PA. CONS. STAT. ANN. §2305c.<br>Pennsylvania also addresses privacy of confidential medical information in separate statutes governing specific types of entities and conditions. | Any "individual or a business doing business in" Pennsylvania is subject to BPINA's breach notification requirements if that individual or business "maintains, stores or manages computerized data that includes personal information." 73 PA. CONS. STAT. ANN. §§ 2302, 2303(A).<br>However, entities subject to and in compliance with privacy and security standards for the protection of electronic personal health information under HIPAA are deemed to be in compliance with BPINA. 73 PA. CONS. STAT. ANN. §2305c.<br>There are also restrictions on disclosure specific to certain entities. *See generally*, specific privacy protections applicable to various medical facilities such as Title 28, Health and Safety, which includes various medical facilities such as hospitals. 28 PA. CODE § 115.27 (hospitals); 28 PA. CODE § 563.9 (ambulatory surgical centers); 28 PA. CODE § 5.53 (Clinical laboratories); *See also* Title 49, Professional and Vocational Standards, which includes specific privacy protections applicable to various medical professions. | Restrictions on disclosure specific to certain conditions, such as child abuse. *See generally* Title 28 and 49.<br>Also, under BPINA, entities that maintain, store, or manage computerized data that constitutes "personal information" on behalf of Pennsylvania must implement encryption or other appropriate security measures. 73 PA. CONS. STAT. ANN. §2305a.<br>However, entities subject to and in compliance with privacy and security standards for the protection of electronic personal health information under HIPAA are deemed to be in compliance with BPINA. 73 PA. CONS. STAT. ANN. §2305c. | None beyond HIPAA. Under BPINA, a "vendor that maintains, stores or manages computerized data on behalf of another entity" must notify the entity of the breach. 73 PA. CONS. STAT. ANN. §2303 (c). However, entities subject to and in compliance with privacy and security standards for the protection of electronic personal health information under HIPAA are deemed to be in compliance with BPINA. 73 PA. CONS. STAT. ANN. §2305c. | BPINA defines "breach of the security of the system" as "[t]he unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of [Pennsylvania]." 73 PA. CONS. STAT. ANN. §2302. |
| **RI** Rhode Island | Rhode Island's Confidentiality of Health Care Information Act defines "confidential healthcare information" as "all information relating to a patient's healthcare history, diagnosis, condition, treatment, or evaluation obtained from a healthcare provider who has treated the patient." 5 R.I. Gen. Laws § 5-37.3-3. | Any person licensed to provide or lawfully providing healthcare services. 5 R.I. Gen. Laws § 5-37.3-3 | None beyond HIPAA. | None. Statute technically applies to "any person," but is limited to information obtained from a health care provider. | Any release or transfer not described in 5 R.I. Gen. Laws 5-37.3-4(b). For all data, any disclosure of personal information that poses a significant risk of identity theft. 11 R.I. Gen. Laws 11-49.3-4 |

| What safe harbors or exceptions exist (e.g., close family, death, etc.) | What form may an authorization for disclosure take (e.g., written, verbal, duration)? | What are the State's reporting and remediation requirements in the event of a breach/unlawful exposure? | What penalties exist for failure to report an unlawful exposure? | What rules are there for responding to subpoenas? |
|---|---|---|---|---|
| Entities subject to and in compliance with privacy and security standards for the protection of electronic personal health information under HIPAA are deemed to be in compliance with BPINA. 73 PA. CONS. STAT. ANN. §2305c.<br>Moreover, an entity shall deemed to be in compliance with BPINA's notification requirements if it maintains its own notification procedures as part of a privacy or security policy, those procedures are consistent with the notice requirements of BPINA, and the entity notified persons in accordance with its policies in the event of a breach. 73 PA. CONS. STAT. ANN. §2307(a).<br>A notification under BPINA may be delayed if a law enforcement agency advises the entity that the notification will impede a criminal or civil investigation. The notice must be in a writing that references the exception under BPINA. 73 Pa. Cons. Stat. Ann. §2304.<br>"Good faith acquisition of personal information by an employee or agent of the entity for the purposes of the entity is not a breach of the security of the system if the personal information is not used for a purpose other than the lawful purpose of the entity and is not subject to further unauthorized disclosure." 73 PA. CONS. STAT. ANN. §2302<br>Maintenance of an entity's own notification process as part of a privacy or security policy shall be deemed in compliance with notice requirements. 73 PA. CONS. STAT. ANN. §2307(b) | None beyond HIPAA -- for example, there is no specific provision allowing the release of information from medical records for research purposes. | A covered entity shall provide notice of any breach following determination of the breach of the security of the system to any resident of Pennsylvania whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. The entity must take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system. The notice shall be made without unreasonable delay. 73 PA. CONS. STAT. ANN. §2303.<br>Notifications must mailed to the last known address, by telephone if the individual can be reasonably expected to be contacted by phone and are not required to provide personal information for verification, or via email, if a previous business relationship exists and a valid email address is known for that individual. Electronic notice is permitted if it directs the individual to promptly change their password and security question or answer or to take other steps appropriate to protect that individual's online account, provided sufficient contact information is held to allow the electronic notice to be served. 73 PA. CONS. STAT. ANN. §§ 2302, 2303.<br>When an entity provides notification under BPINA to more than 1,000 persons at one time, the entity must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in section 603 of the Fair Credit Reporting Act. 73 Pa. Cons. Stat. Ann. §§ 2305. | The Attorney General shall have exclusive authority to bring an action for violation of the data breach statute. 73 PA. CONS. STAT. ANN. §2308 | N/A |
| Disclosure without consent permitted for medical or dental emergency, for professional disciplinary or peer-review boards, to law enforcement in certain circumstances, or for claims adjudication. 5 R.I. Gen. Laws § 5-37.3-4 | Must be in writing and contain statutory disclosure language. 5 R.I. Gen. Laws § 5-37.3-4(d) | Notification to affected residents of the state (if more than 500 individual affected), the Attorney General, and major credit reporting agencies. No later than 45 calendar days of discovery. 11 R.I. Gen. Laws 11-49.3-4 | Reckless violation - $100 per record.<br>Knowing and willful violation - $200 per record<br>AG may bring action<br>(11 R.I. Gen. Laws 11-49.3-5) | May disclose if subpoena and certification of service on affected individual, and passage of 20 days or court order after challenge. 5 R.I. Gen. Laws 5-37.3-6.1 |

| State | How does the State define protected health information? | How does the state define a covered entity (i.e. who is subject to the disclosure laws)? | What additional security obligations exist (beyond HIPAA) for PHI? | What rules are there governing business associates? | What constitutes a breach or unlawful disclosure? |
|---|---|---|---|---|---|
| **SC** South Carolina | "Protected Health Information" means any information, whether oral, written, electronic, visual, pictorial, physical, or any other form, that relates to an individual's past, present, or future physical or mental health status, condition, treatment, service, products purchased, or provision of care, and that reveals the identity of the individual whose health care is the subject of the information, or where there is a reasonable basis to believe such information could be utilized (either alone or with other information that is, or reasonably should be known to be, available to predictable recipients of such information) to reveal the identity of that individual. S.C. Code Ann. § 44-4-130(O) | N/A; HIPAA Privacy Rule governs | N/A | None beyond HIPAA. | "breach in the security of the data to a resident of this State whose personal identifying information that was not rendered unusable through encryption, redaction, or other methods was, or is reasonably believed to have been, acquired by an unauthorized person when the illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident." S.C. Code Ann. § 39-1-90 |
| **SD** South Dakota | Person's first name or initial with last name, plus HIPAA-defined health information, among other items. SDL 22-40-19(4) | Person or business that: (A) conducts business in SD and (B) owns or retains computerized personal information of an SD resident. SDL 22-40-19(3) | None beyond HIPAA. | Included in definition of "covered entity." | Unauthorized acquisition of unencrypted personal information. SDL 22-40-19(1) |

| What safe harbors or exceptions exist (e.g., close family, death, etc.) | What form may an authorization for disclosure take (e.g., written, verbal, duration)? | What are the State's reporting and remediation requirements in the event of a breach/unlawful exposure? | What penalties exist for failure to report an unlawful exposure? | What rules are there for responding to subpoenas? |
|---|---|---|---|---|
| N/A | A patient or his legal representative has a right to receive a copy of his medical record, or have the record transferred to another physician, upon request, when accompanied by a written authorization from the patient or his legal representative to release the record. S.C. Code Ann. § 44-115-30<br>Requests muse be made by "express written consent of the patient or person authorized to act on behalf of patient." S.C. Code Ann. § 44-115-40<br>Physician is immune from civil liability or disciplinary action for release of records in reliance on representations of a health and life insurance carrier or administrator of health and life insurance claims that the authorization of the patient or of a person upon whose status the patient's claim depends for release of the medical record is on file with the carrier as an authorization to release medical information under this chapter. S.C. Code Ann. § 44-115-50. Physician is similarly immune from civil or criminal liability or disciplinary action for releasing records on written authorization of patient or patient's representative. S.C. Code Ann. § 44-115-140.<br>Physician may limit the release of the *entire* medical record an furnish only a portion if they have a reasonable belief that entire release would cause harm to emotional or physical well being of the patient or others giving information about the patient. However, physician must release the full record to authorized representatives, attorneys representing the patient, or legal guardian with express written consent. | The disclosure must be made to a resident whose data was breached in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or with measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. S.C. Code Ann. § 39-1-90 | Knowing and willful violations may be subject to an administrative fine of $1,000 for each resident whose information has been breached. S.C. Code Ann. § 39-1-90(H_) | Other provisions pertaining to medical records or actions involving medical negligence not invalidated by this chapter. S.C. Code Ann. § 44-115-150 |
| Good faith acquisition by employee or agent for authorized disclosure. SDL 22-40-19(1) | None beyond HIPAA. | Disclose within 60 days to affected consumer, and if applicable, the Attorney General – some exceptions if after investigation and notice to Attorney General the breach "will not likely result in harm…" SDL, 22-40-22. Separate requirement to notify credit reporting agencies "without unreasonable delay." SDL, 22-40-24 | Prosecution for deceptive practice or act. Up to $10,000 per day for violation. SDL 22-40-25 | None beyond HIPAA. |

| State | How does the State define protected health information? | How does the state define a covered entity (i.e. who is subject to the disclosure laws)? | What additional security obligations exist (beyond HIPAA) for PHI? | What rules are there governing business associates? | What constitutes a breach or unlawful disclosure? |
|---|---|---|---|---|---|
| **TN** Tennessee | Same as HIPAA. Defined the same as the meaning given in 45 C.F.R. § 160.103<br>(Note this relates to solicitation, but provides a definition of PHI.) Tenn. Code. Ann. § 47-18-3001 | Health care providers, further defined as "any person required to be licensed under [Tennessee Code Annotated Title 63]" Tenn. Code. Ann. § 63-2-101 | N/A | None beyond HIPAA. | None beyond HIPAA. |
| **TX** Texas | Has the same meaning assigned by HIPAA. Tex. Health & Safety Code Ann. § 181.001(a); Tex. Ins. Code Ann. § 602.001(3); 28 Tex. Admin. Code § 22.52<br>The Texas Administrative Code defines as any information that relates to the individual's health condition, provision of health care, or payment for health care, and can be used to identify that individual. *See, e.g.*, 10 Tex. Admin. Code § 1.24(b)(12); 25 Tex. Admin. Code § 1.501(b)(5); Tex. Bus. & Com. Code Ann. § 521.002(a)(2)(B) | Any person who collects, uses, stores, transmits, or possesses PHI. Tex. Health & Safety Code Ann. § 181.001(b)(2); Tex. Ins. Code Ann. § 602.001(1). Covered entities must comply with HIPAA privacy requirements. Tex. Health & Safety Code Ann. § 181.004 | Hospitals must safeguard all health care information they maintain. Tex. Health & Safety Code Ann. § 241.155. Patients harmed by the release of confidential health information may sue for injunctive relief or damages. Tex. Health & Safety Code Ann. § 241.156 | None beyond HIPAA. | The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information. Tex. Bus. & Com. Code Ann. § 521.053(a) |
| **UT** Utah | Undefined. "Personal Information" means: Resident's name plus:<br>• Social security number ;<br>• driver's license number;<br>• financial account number; or<br>• other specified information. Utah Code Ann. § 13-44-102 (West 2020) | Undefined. This state's disclosure laws apply to any individual/entity who/ that conducts business in the state and maintains Personal Information. Utah Code Ann. § 13-44-201 (West 2020) | None beyond HIPAA. This state does not define PHI. Utah Code Ann. § 13-44-201 (West 2020) | None beyond HIPAA. Utah Code Ann. § 13-44-102, et seq. (West 2020) | Unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality, or integrity of personal information. Utah Code Ann. § 13-44-102 (West 2020) |

| What safe harbors or exceptions exist (e.g., close family, death, etc.) | What form may an authorization for disclosure take (e.g., written, verbal, duration)? | What are the State's reporting and remediation requirements in the event of a breach/unlawful exposure? | What penalties exist for failure to report an unlawful exposure? | What rules are there for responding to subpoenas? |
|---|---|---|---|---|
| Disclosure of student records to a member of the state threat assessment team is allowed if information holder believes disclosure is necessary to prevent a serious or imminent threat. Tenn. Code. Ann. § 49-6-2702<br>Upon death, next of kin is considered authorized representative. Tenn. Code. Ann. § 63-2-101 | Written authorization including core elements of 45 C.F.R. Parts 160 and 164.<br>Allows health care provider to determine form of authorization based on circumstance and maintain a policy.<br>Tenn. Code. Ann. § 63-2-101 | None beyond HIPAA. | None beyond HIPAA. | None beyond HIPAA. |
| Disclosure is: for treatment, payment, health care operations, or performing insurance functions; directory information; to another treating physician, EMS provider, or prospective provider; to certain clergy; to an organ procurement organization; for peer review; to a government agency; to a hospital's successor in interest; to the American Red Cross; to a poison control center; to a utilization review agent; for research; for reimbursement for medical services; to an HMO; for medical records of a deceased or incompetent; pursuant to court order or subpoena. Tex. Health & Safety Code Ann. §§ 181.153, 241.153; *see also* Tex. Occ. Code Ann. § 159.003(a); Tex. R. Evid. 509(e), 510(d) | Written or electronic form, or in oral form if it is documented in writing by the covered entity. No duration limitation. Tex. Health & Safety Code Ann. § 181.153(b) | Within 60 days after breach, covered entities must provide written notice to last known address of any affected state resident. Tex. Bus. & Com. Code Ann. § 521.053(b), (e) | Failure to report unlawful exposure is liable to State for civil penalty between $2,000 and $50,000 for each violation. Tex. Bus. & Com. Code Ann. § 521.151(a) | Patient is party to judicial proceeding and disclosure is pursuant to subpoena issued under: (1) the Texas Rules of Civil or Criminal Procedure; or (2) Chapter 121 of the Texas Civil Practice and Remedies Code. Tex. Health & Safety Code Ann. § 241.153(20); Tex. Occ. Code Ann. § 159.002(f) |
| None beyond HIPAA. Utah Code Ann. § 13-44-202 (West 2020) | None beyond HIPAA. | Notification of the subject of the PI if the maintainer determines that the PI may or will be fraudulently used. Utah Code Ann. § 13-44-202 (West 2020) | State AG may file a lawsuit for up to $2,500 per resident up to certain aggregate limits determined by specified circumstances. Utah Code Ann. § 13-44-301 (West 2020) | None beyond HIPAA. |

| State | How does the State define protected health information? | How does the state define a covered entity (i.e. who is subject to the disclosure laws)? | What additional security obligations exist (beyond HIPAA) for PHI? | What rules are there governing business associates? | What constitutes a breach or unlawful disclosure? |
|---|---|---|---|---|---|
| VT Vermont | "Protected health information" shall have the same meaning as in 45 C.F.R. § 160.103. 18 V.S.A. § 1881(a)(4) | "Covered entity" has the same meaning as in 45 C.F.R. § 160.103. 18 V.S.A. § 1881(a)(2) | The state of Vermont provides patients with more privacy protections than HIPAA. The following VT laws provide additional protection beyond HIPPA: 18 V.S.A. §7103 (fines and possible imprisonment for wrongful disclosure of mental health treatment information), 12 V.S.A. §1612 (provides privilege for patient-provider communications), 18 V.S.A. §1852(a)(7) (confidentiality provisions for hospital patients), 18 V.S.A. §4211 (rights to inspect prescription records only granted to federal and state drug enforcement officers), 18 V.S.A. §1001 (confidentiality requirements for mandatory reporting records) | "Business Associate" has the same meaning as in 45 C.F.R. § 160.103. 18 V.S.A. § 1881(a)(21 | "A covered entity or business associate shall not disclose protected health information unless the disclosure is permitted under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)." 18 V.S.A. § 1881 (b)<br>HIPAA (45 CFR §§ 164.402) Definition of Breach |

| What safe harbors or exceptions exist (e.g., close family, death, etc.) | What form may an authorization for disclosure take (e.g., written, verbal, duration)? | What are the State's reporting and remediation requirements in the event of a breach/unlawful exposure? | What penalties exist for failure to report an unlawful exposure? | What rules are there for responding to subpoenas? |
|---|---|---|---|---|
| "To the extent permitted under federal law, this section does not affect the requirements for mental health professionals to communicate with individuals involved in a patient's care in a manner that is consistent with legal and professional standards, including section 7103 of this title." Disclosures of protected health information to avert a serious risk of danger. 18 V.S.A. § 1882(d)<br>"Nothing in this section shall preclude disclosure, upon proper inquiry, of information concerning medical condition to the individual's family, clergy, physician, attorney, the individual's agent under an advance directive executed in accordance with chapter 231 of this title, a person to whom disclosure is authorized by a validly executed durable power of attorney for health care, or to an interested party." 18 V.S.A. § 7103(b)<br>12 V.S.A. § 1612(b) & (c)<br>18 V.S.A. §1852(a)(7) | The law states that patient identification and records shall be kept confidential absent the patient's written consent or a court order. 18 V.S.A. § 7103 | None beyond HIPAA. See Breach Notification Rule, 45 CFR §§ 164.400-414 | None beyond HIPAA. | Vermont Rules of Civil Procedure, Rule 45. SUBPOENA |

| State | How does the State define protected health information? | How does the state define a covered entity (i.e. who is subject to the disclosure laws)? | What additional security obligations exist (beyond HIPAA) for PHI? | What rules are there governing business associates? | What constitutes a breach or unlawful disclosure? |
|---|---|---|---|---|---|
| VA Virginia | "Medical information" means the first name or first initial and last name with any of the following data elements that relate to a resident of Virginia, when the data elements are neither encrypted nor redacted: (1) any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or (2) an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records. Medical Information does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public. Va. Code § 32.1-127.1:05(A)<br>"Health record" means any written, printed, or electronically recorded material maintained by a health care entity in the course of providing health services to an individual concerning the individual and the services provided. "Health record" also includes the substance of any communication made by an individual to a health care entity in confidence during or in connection with the provision of health services or information otherwise acquired by the health care entity about an individual in confidence and in connection with the provision of health services to the individual. Va. Code Ann. § 32.1-127.1:03(B) | Any health care provider, health plan, or health care clearinghouse. See Code of Virginia; § 32.1-127.1:03(B) | None beyond HIPAA. | None beyond HIPAA. | "Breach of the security of the system" means access and acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality, or integrity of medical information maintained by an entity. Va. Code Ann. § 32.1-127.1:05(A) |

| What safe harbors or exceptions exist (e.g., close family, death, etc.) | What form may an authorization for disclosure take (e.g., written, verbal, duration)? | What are the State's reporting and remediation requirements in the event of a breach/unlawful exposure? | What penalties exist for failure to report an unlawful exposure? | What rules are there for responding to subpoenas? |
|---|---|---|---|---|
| See Va. Code Ann. § 32.1-127.1:03 (D). – health records minors, worker's comp cases, release to a correctional facility, or secure juvenile shelter, and to comply with subpoena). | Written authorization including information provided in the sample form at Va. Code Ann. § 32.1-127.1:03(G) | HIPAA reporting requirements control if an entity is covered as a "covered entity" or "business associate" or a non-HIPAA-covered entity subject to the Health Breach Notification Rule. Va. Code Ann. § 32.1-127.1:05(F)<br>Notice shall be written, telephonic, or electronic, substitute (available under certain circumstances) to include: email notice, conspicuous posting on a website of the entity, notice to major statewide media. Notice shall include (1) the incident in general terms, (2) type of medical information subject to unauthorized access or acquisition, (3) general acts of the entity to protect the personal information from further unauthorized access, and (4) a telephone number that the person may call for further information and assistance, in one exists.<br>Notice must be provided to Office of the Attorney General and the Commissioner of Health if more than 1,000 individuals are provided notice at any time. Va. Code Ann. § 32.1-127.1:05 | None beyond HIPAA. | Health care entities may, and, when required by other provisions of state law, shall, disclose health records in compliance with a subpoena issued in accord with subsection H, pursuant to a search warrant or a grand jury subpoena, pursuant to court order upon good cause shown or in compliance with a subpoena issued pursuant to subsection C of § 8.01-413. Regardless of the manner by which health records relating to an individual are compelled to be disclosed pursuant to this subdivision, nothing in this subdivision shall be construed to prohibit any staff or employee of a health care entity from providing information about such individual to a law-enforcement officer in connection with such subpoena, search warrant, or court order. See Va. Code Ann. § 32.1-127.1:03 (D)(2) |

| State | How does the State define protected health information? | How does the state define a covered entity (i.e. who is subject to the disclosure laws)? | What additional security obligations exist (beyond HIPAA) for PHI? | What rules are there governing business associates? | What constitutes a breach or unlawful disclosure? |
|---|---|---|---|---|---|
| **WA** Washington | "Health care information" means any information, whether oral or recorded in any form or medium, that identifies or can readily be associated with the identity of a patient and directly relates to the patient's health care, including a patient's deoxyribonucleic acid and identified sequence of chemical base pairs. The term includes any required accounting of disclosures of health care information. RCW § 70.02.010<br>The Washington My Health My Data Act defines protected "consumer health data" as "personal information that is linked or reasonably linkable to a consumer that identifies the consumer's past, present, or future physical or mental health status," including but not limited to information related to diagnoses, treatments, medication use, gender-affirming care, reproductive health, biometric data, and genetic data, as well information used to identify the above that is "derived or extrapolated from non-health information," such as information derived through algorithms or machine learning. HB 1155 § 3(7).<br>The Act does not apply to protected health information under HIPAA or health care information collected, used or disclosed in accordance with RCW § 70.02. HB 1155 § 12.<br>[Note: Most sections of the My Health My Data Act are set to take effect March 31, 2024]. | Health care provider, health care facility, or third-party payor, to the extent that activities are related to functions that make an entity a health care provider, health care facility or third-party payor. RCW § 70.02.020<br>Additionally, state law requires many agencies that are exempt from HIPAA to meet similar administrative requirements. Executive Order 16-01<br>The Washington My Health My Data Act define a "regulated entity," subject to the Act, as an entity that (a) conducts business in Washington or provides products or services targeted to consumers in Washington and (b) "alone or jointly with others, determines the purpose and means of collecting, processing, sharing, or selling consumer health data." HB 1155 § 3(23)<br>[Note: Most sections of the My Health My Data Act are set to take effect March 31, 2024]. | Special security rules exist for information contained in a patient medication record system or in regards to hospital patient discharge data.<br>RCW § 246-875-070<br>RCW § 246-455-080<br>Under the Washington My Health My Data Act, regulated entities:<br>• May not collect or share any consumer health data, except (i) with the consumer's consent or (ii) to the extent necessary to provide a product or service that the subject consumer has requested from such regulated entity. HB 1155 § 5(2)<br>• Must restrict access to consumer health data to employees or contractors for which access is necessary to further the purposes for which the consumer provided consent. HB 1155 § 7(1)(a)<br>• Must establish and maintain security practices to protect the confidentiality of consumer health data that, at minimum, "satisfy reasonable standard[s] of care" within the entity's industry. HB 1155 § 7(1)(a)<br>• May not sell or offer to sell any consumer health data without first obtaining valid authorization from the consumer. HB 1155 § 9<br>• May not implement a "geofence"—e.g., technology that uses cell tower connectivity or WiFi data—around an in-person health facility to track or collect consumer health data or to send advertisements to consumers related to their consumer health data or health care services. HB 1155 § 10.<br>[Note: Most regulated entities must comply with the above sections beginning March 31, 2024]. | None beyond HIPAA. | Washington's public records act prohibits disclosure of the following health care information:<br>• Information obtained by the board of pharmacy from a manufacturer or their representative.<br>• Information obtained by the board of pharmacy from an individual or entity (e.g. pharmaceutical manufacturer, practitioner) that purchases or distributes drugs.<br>• Information and documents created and maintained by quality improvement committees, peer review committees, quality assurance committees, and hospitals in relation to the reporting and notification of adverse events and hospital acquired infections.<br>• Records related to the impaired physician program.<br>• Complaints regarding health professional discipline.<br>• Information related to the prescription monitoring program.<br>• Information obtained by the department of health pursuant to the death with dignity act.<br>• Cardiac and stroke performance data submitted to national, state, or local data collection systems.<br>• Information obtained from the employee wellness program. However, statistical reports that do not contain identifying information may be disclosed.<br>RCW § 42.56.360 |
| **WV** West Virginia | None beyond HIPAA, except for specific areas (e.g. – mental health records) | None beyond HIPAA. | None beyond HIPAA. | None beyond HIPAA. | None beyond HIPAA. |

| What safe harbors or exceptions exist (e.g., close family, death, etc.) | What form may an authorization for disclosure take (e.g., written, verbal, duration)? | What are the State's reporting and remediation requirements in the event of a breach/unlawful exposure? | What penalties exist for failure to report an unlawful exposure? | What rules are there for responding to subpoenas? |
|---|---|---|---|---|
| Individuals, or their legal representatives, may authorize, in writing, a state agency to disclose records containing their individually identifiable information for research purposes. RCW 42.48.020<br>A health care provider or facility has the option of disclosing health care information about a patient without the patient's authorization if the disclosure fits in one of the following categories:<br>• To a person who the provider or facility reasonably believes is providing health care to the patient<br>• To other persons in the facility or office to provide planning, quality assurance, peer review, or administrative, legal, financial or other health care operations on behalf of the provider or facility<br>• To another provider reasonably believed to have previously provided health care to the patient, unless the patient has specifically instructed otherwise<br>• To a person the provider or facility reasonably believes will help avoid or minimize an imminent danger to the health or safety of the patient or any other individual<br>• To immediate family members, domestic partners, and close personal relationships of the patient, unless the patient has stated otherwise<br>• For use in certain research projects that contain reasonable safeguards to protect the information from direct identification and redisclosure<br>• To a person who obtains information for purposes of an audit<br>• To officials of a correctional facility<br>• To provide directory information, unless the patient has instructed the health care provider or health care facility not to make the disclosure<br>• To fire, police, sheriff, or other public authorities that brought the patient to the provider or facility<br>• To law enforcement authorities if evidence of criminal conduct is present<br>• For payment<br>RCW § 70.02.0500 | A patient may authorize a health care provider or facility to disclose the patient's health care information. The provider or facility must honor an authorization, and if requested, provide a copy of the recorded information. A reasonable fee may be charged for providing the information, and the record is not required to be sent until the fee is paid. The provider must keep either the original or a copy of the information being disclosed. To be valid, a disclosure authorization must:<br>• Be in writing, dated, and signed by the patient<br>• Identify the information to be disclosed<br>• Identify the name of the person to whom the information is to be disclosed<br>• Identify who is to make the disclosure<br>• Contain an expiration date or event for that disclosure<br>A patient may revoke in writing a disclosure authorization at any time. Patients may not maintain an action against the provider for disclosures made in good-faith reliance on an authorization if the provider had no actual notice of the revocation.<br>RCW § 70.02.030<br>Under the Washington My Health My Data Act, consent for collection or disclosure of consumer health data must be "a clear affirmative act that signifies a consumer's freely given, specific, informed, opt-in, voluntary, and ambiguous agreement" to collection or disclosure, "which may include written consent provided by electronic means." HB 1155 §3(5).<br>Under the Washington My Health My Data Act, a valid authorization from a consumer permitting the sale of consumer health data must be "written in plain language," signed by the consumer, "separate and distinct" from other consumer consent required by the Act, and must contain specific information, including identification of the specific consumer health data the entity intends to sell, the name and contact information of the purchaser, a description of the purpose of the sale, and a statement that the consumer has the right to revoke the authorization at any time. HB 1155 §9(2).<br>[Note: Most sections of the My Health My Data Act are set to take effect March 31, 2024]. | None beyond HIPAA. | A person who has complied with the relevant requirements governing health care information access and disclosure may bring an action for relief against a health care provider or facility who has not complied with relevant requirements within two years after the cause of action is discovered. The court may order the provider or other person to comply with requirements, and may award actual damages. The court must award reasonable attorneys' fees and all other expenses reasonably incurred to the prevailing party. RCW § 70.02.170<br>Conduct prohibited by the Washington My Health My Data Act is considered a violation of the Washington Consumer Protection Act, RCW § 19.86, et seq., which empowers the Attorney General to bring an action on behalf of the people and also provides a private right of action for consumers. HB 1155 § 11.<br>[Note: Most sections of the My Health My Data Act are set to take effect March 31, 2024]. | None beyond HIPAA. |
| None beyond HIPAA. | Upon written request of a patient or his or her personal representative, as defined by HIPAA. W. Va. Code Ann. § 16-29-1(a) | None beyond HIPAA. | None beyond HIPAA. | None beyond HIPAA. |

| State | How does the State define protected health information? | How does the state define a covered entity (i.e. who is subject to the disclosure laws)? | What additional security obligations exist (beyond HIPAA) for PHI? | What rules are there governing business associates? | What constitutes a breach or unlawful disclosure? |
|---|---|---|---|---|---|
| **WI** Wisconsin | Has the meaning given in 45 CFR 160.103. W.S.A. 146.816 (1)(f) | Has the meaning given in 45 CFR 160.103. W.S.A. 146.816 (1)(b) | Confidentiality of patient health care records. W.S.A. 146.82 | 'Business associate' has the meaning given in 45 CFR 160.103. W.S.A. 146.816 (1)(a) | None beyond HIPAA. |
| **WY** Wyoming | No specific definition for PHI but "Personal Identifying Information" means: Resident's name plus:<br>• Social security number;<br>• river's license number;<br>• medical/health insurance information; or<br>• other specified information. Wyo. Stat. Ann. § 40-12-501; Wyo. Stat. Ann. § 6-3-901 | No specific definition, but state disclosure laws apply to any individual/ entity who/that conducts business in-state and maintains Personal Identifying Information. Wyo. Stat. Ann. § 40-12-502) | None beyond HIPAA. | None beyond HIPAA. | Unauthorized acquisition of data that compromises the confidentiality of Personal Identifying Information or is reasonably believed to cause resident loss. Wyo. Stat. Ann. § 40-12-501) |

| What safe harbors or exceptions exist (e.g., close family, death, etc.) | What form may an authorization for disclosure take (e.g., written, verbal, duration)? | What are the State's reporting and remediation requirements in the event of a breach/unlawful exposure? | What penalties exist for failure to report an unlawful exposure? | What rules are there for responding to subpoenas? |
|---|---|---|---|---|
| Patient health care records may be released to "other persons" with the "informed consent" of the patient or someone authorized by the patient. W.S.A. 146.82(1). The statute also contains a very long list of authorized disclosures without informed consent, which can be found at W.S.A. 146.82(2)(1-22). | Confidentiality of patient health care records. W.S.A. 146.82<br>WI DHS - Consent must be informed. | Not specified. See HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414. | HIPPA (45 C.F.R. § 160.404 Amount of a civil money penalty) | W.S.A. 805.07. Subpoena. The subpoena rules contain nothing specifically applicable to health care information. |
| None beyond HIPAA. | None beyond HIPAA. | Notification of affected person if the information is likely to be misused. Wyo. Stat. Ann. § 40-12-502(a) and (h) | State AG may file a lawsuit to recover damages and/or ensure compliance. Wyo. Stat. Ann. § 40-12-502(f) | None beyond HIPAA. |



www.seyfarth.com