Part I Questions and Answers:
Health Insurance Portability Accountability Act
and Minnesota Health Records Act

Index

Question 10: **p. 9**
Under HIPAA, what would be the "minimum necessary requirement" for the various entities that would have access to a patient's health records for treatment, payment, and operations?

Question 11: **p. 11**
What are other states doing regarding citizens who do not wish to have their health records shared?

Question 12: **p. 26**
How would elimination of the Minnesota consent requirement impact sharing through the state or other health information exchanges, or the national health information exchange, called the eHealth Exchange?

Question 1:

Who defines "coordination of care"?
What does it mean to those who claim a "breakdown of coordination of care"?
What are the contributors to a breakdown in coordination of care?

There is no single definition for coordination of care. It is not defined by Minnesota law or HIPAA. The Agency for Healthcare Research and Quality (AHRQ) has found that there are over 40 definitions for coordination of care.[1] The U.S. Department of Health and Human Services (HHS) does not adopted a universal definition for coordination of care, but has used the following definition:

> "Care coordination is the deliberate organization of patient care activities between two or more participants (including the patient) involved in a patient's care to facilitate the appropriate delivery of health care services. Organizing care involves the marshalling of personnel and other resources needed to carry out all required patient care activities and is often managed by the exchange of information among participants responsible for different aspects of care."[2]

What is considered a "breakdown" in the coordination of care will be different to each individual and will be specific to their experience. However, patients, health care professionals, and system representatives, all agree that most often the breakdown occurs when there is a transition in health care, requiring an exchange of information.

- Most often patients and health care professionals are burdened by the inconvenience and delay during the process of exchanging information, and when they believe the burden has becomes too much is when patients and professionals believe they experience a "breakdown" in the coordination of care.[1]
- From the **patient perspective**, "care coordination is any activity that helps ensure that the patient's needs and preferences for health services and information sharing across people, functions, and sites are met over time." However, patients believe when they've exerted more effort than should be required of them, there is a breakdown in the coordination of their care.
- From the **health care professional prospective**, coordination of care focuses on the patient; where to send them, what information must be transferred among health care entities, and managing responsibilities among all health care professionals and entities. Professionals believe a breakdown occurs when there is a delay in shared information among professionals or a lack of accountability among professionals, affecting patient treatment.
    - Discrepancies among health care professional regarding their roles may also lead to ineffective communication and misguiding patients. Therefore, there is a responsibility of doctors, nurses, specialist, physician assistants, etc. to understand their role and to take accountability for that role, including the exchange of information. For example, physicians reported that 72% of the time relative

[1] https://www.ahrq.gov/professionals/prevention-chronic-care/improve/coordination/atlas2014/chapter2.html
[2] https://www.ahrq.gov/downloads/pub/evidence/pdf/caregap/caregap.pdf

medical information was not available at the time of the appointment, and only 34% of physicians' reports receiving timely information from referrals.[3]
    - Additionally, health care providers cite a lack of time, infrastructure, and resources to respond to patient needs, as major barriers to patient care and coordination.
- The **system representative's perspective** differs from patients and professionals. From the perspective of the system representative, coordination of care is the deliberate integration of "personnel, information, and other resources needed to carry out all required patient care activities between and among care participants." They believe a "breakdown" occurs when there is a failure within their system affecting the exchange of information. They are concerned with the functionality of their systems. However, they struggle to create cost-effective coordination systems, which are adaptable to changes in definitions and models.
    - From their perspective, a breakdown in the coordination of care occurs when the system does not bridge gaps in information flow, which occurs most often because there is no single model of coordination. Due to the "lack of consensus regarding definitions and measures, and the paucity of data on the cost effectiveness of different interventions" the ability to compare care coordination models is limited, making it difficult to find the most effective care coordination systems.[4]

The more complex a case or health care plan, the more health care professionals involved, the more exchanges of information, the more likely there will be a breakdown in the coordination of care. Therefore, the most significant contributor to a breakdown in coordination of care is the involvement of numerous health care professionals and increase in the exchange of information.[4]

Question 2:

Do patients have a right to limit the hospital/health plan's definition of "coordination of care" according to their personal privacy and consent preferences?

Neither MHRA nor HIPAA adopt a definition of coordination of care, nor do they mention altering a definition of coordination of care. MHRA is silent on a patient's right to limit or alter the hospital or health plan's definition of coordination of care. Therefore, it is assumed that patients do not have a right to limit a hospital's or health plan's definition of coordination of care.

There does not appear to be an adopted definition of coordination of care under HIPAA. However, the definition of treatment would imply that patients do not have a right to limit the definition of coordination of care. According to HIPAA's Privacy Rule, otherwise protected health information (PHI) may be disclosed without consent for the purpose of treatment.

[3] https://www.ahrq.gov/professionals/prevention-chronic-care/improve/coordination/atlas2014/chapter2.html
[4] https://www.ahrq.gov/professionals/prevention-chronic-care/improve/coordination/atlas2014/chapter2.html

Treatment is defined to include the coordination or management of health care. Therefore, the definition of treatment and applicable rules include the coordination of care. Generally, the Privacy Rule is limited by the principle of "minimum necessary," meaning a covered entity may only disclose the information needed to accomplish the intended purpose for the use, disclosure, or request. However, the minimum necessary standard does not apply to disclosures or requests for the purpose of treatment; this effectively gives patients no control over limiting the definition of treatment or coordination of care.[5] For the purpose of treatment, a health care provider is not limited in their use, disclosure, or request for a patient's PHI.

Question 3:

Can coordination of care and an individual's rights to control who can see their health records co-exist in state law?

On its face, it seems entirely possible that coordination of care and an individual's right to privacy in health records can co-exist in state law. However, whether there is an attainable solution, which both streamlines coordination of care and protects an individual's privacy, is entirely up to the stakeholders—health care professionals, system/IT representatives, and patients.

- Health care professionals must be knowledgeable in privacy laws, and take responsibility for their role in exchanging information.
- Patients must be willing to either consent, or face delays and take responsibility for exchanging information in their health care.
- System or IT representatives must also be knowledgeable in state privacy laws and create systems that incorporate those laws and protect information, all while facilitating the exchange of information, a complex task.

As mentioned, coordination of care is simplified when PHI is easily accessible and exchangeable. HIPAA allows for exchanges of information without consent in many circumstances, most notably consent is not required for the purpose of treatment, payment, and health care operations. Exceptions to consent under HIPAA are governed by 45 CFR § 164.512, and can be found here, https://www.law.cornell.edu/cfr/text/45/164.512. Although HIPAA allows for an easy exchange of information and tends to streamline coordination of care, it leaves gaps in a patient's privacy rights and hinders a patient's ability to control how and when their information is shared. A select number of states have created laws to close these gaps and enhance privacy protections in health care. However, more stringent laws may have a negative impact on coordination of care.

- It has been suggested that stringent state laws delay or prevent the sharing of PHI, thereby impacting, sometimes negatively, a patient's care.
    - However, according to the IBM Watson Health System Study, the Mayo Clinic ranks in the top five of large health systems in the United States. Also, Health Partners in Bloomington ranks among the top five for medium health systems.[6]

[5] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html

[6] https://www.prnewswire.com/news-releases/ibm-watson-health-finds-nations-top-performing-health-systems-deliver-more-consistent-care-across-member-hospitals-300634204.html

- It is important to note that HIPAA has also been found to prevent the use or disclosure of PHI. Due to a lack of understanding and fear of liability for violating HIPAA, health care professionals are often overly cautious, and in some cases do not make disclosures in circumstances in which it is perfectly acceptable to do so. This issue was discussed in detail at a 2013 congressional hearing, in which it was also suggested that education and outreach are essential to the effectiveness of HIPAA.[7]
    - Due to state preemption, comprehensible state laws that are more restrictive than HIPAA could arguably help resolve health care professionals issues with understanding HIPAA and fearing liability, so long as educational tools and resources are provided to health care professionals.

Question 4:

Could a "universal" consent form, used across the state, by all providers, allow for necessary itemized consent AND itemized sharing of health records?

Under Minnesota Statute §144.292 subdivision 8, the Department of Health developed a form that allows patients to request access to health care records.[8] The form allows patients to specify the facility they are requesting records from and the facility, organization, or person they wish to have the records sent to. Additionally, the form allows for patients to specify the information they want to be released.

Based on this form, it is arguably possible for the legislature to direct the Minnesota Department of Health to produce a different form that would be used by every provider. For example, New Mexico, for the purpose of their electronic health information exchange (HIE) network, currently uses a uniform consent form, found here, https://www.nmhic.org/sites/default/files/Opt-out-form_2016.pdf This form adds a patient to the state HIE, where only authorized users can view a patient's records.[9] Authorized users include the following:

- Providers whom are licensed, certified, or otherwise permitted by law to provide health care in the ordinary course of business or practice of a profession; and
- Health care organizations and facility administrative and clerical staff.

By signing the consent form, patients are allowing all clinical information, including protected information, to be included on the HIE. There is no itemization that would allow patients to prohibit certain records from being disclosed. Patients in New Mexico can opt out of the HIE network, either by filling out a consent form and opting out, or by not submitting a form. If a patient opts out without filling out a consent form and selecting "opt out" their information is available in emergency circumstances. However, if a patient opts out by submitting the form, their information is not available, even in an emergency. Although the system does not allow itemized consent, the system technology provides a number of safeguards to patient privacy, including:

- Allowing access for only authorized used;

[7] https://www.gpo.gov/fdsys/pkg/CHRG-113hhrg82190/html/CHRG-113hhrg82190.htm
[8] https://www.revisor.mn.gov/statutes/?id=144.292
[9] https://www.nmhic.org/sites/default/files/patient-consent-form.pdf

- Levels of restriction for authorized staff;
- A log of every instance in which someone accessed the HIE.

A system representative should determine whether it would be effective to include itemized consent on a universal consent form, and whether a system using that form would be effective.

Question 5:

What would it look like for Minnesota to give up the stronger state privacy laws allowed under HIPAA?

Eliminating MHRA would leave HIPAA as the only protection from disclosing protected health information (PHI) without a patient's authorization. This would affect the following situations:

- Patients would lose control over their health information. Under HIPAA, an individual may make privacy requests to the covered entities holding their health information. However, in most circumstances, a covered entity is not obligated to agree with or fulfill the patient's privacy request.[10]
- Minnesotans would lose their right to private action under § 144.298.
- Minnesotans only recourse for challenging wrongful disclosures would be filing complaints with the Office of Civil Rights (OCR), or relying on the State Attorney General to bring civil action.[11]
    - Filing complaints with the OCR is consistently criticized as an ineffective means for reporting violations and getting relief.
        - "In the majority of cases, OCR determined that the complaint did not present an eligible case for enforcement, either because OCR lacked jurisdiction, the complaint was untimely, or the activity did not violate the Privacy Rule."[12]
    - Relying on the Attorney General to bring action puts a burden on the patient to file complaints with the Attorney General, and to investigate their claims in order to convince their Attorney General to pursue civil action.

Question 6:

How many Minnesotans would/could have their health records shared without their consent for treatment, payment, and health care operations?
What could the unintended consequences be?
What would it mean for privacy rights in Minnesota?

If Minnesota conforms to HIPAA, consent would not be required for a covered entity to disclose protected health information (PHI) for the purpose of treatment, payment, or health care operations. This would affect every Minnesotan that has received health care in the state of Minnesota. This would severely limit protections in the following ways:

[10] https://www.privacyrights.org/consumer-guides/hipaa-privacy-rule-patients-rights#right-request-special-privacy-protection
[11] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/state-attorneys-general/index.html
[12] https://www.ncbi.nlm.nih.gov/books/NBK9573/

- It would remove protection Minnesotans currently have that require consent in order to share PHI with researchers;
- It would remove patient control over their PHI, leaving discretion to disclose or use PHI up to a patient's health care providers; and
- Again, it would eliminate the private right to action.

Question7:

What is the definition of "treatment"?
Under treatment, who would/could have access to a patient's health care records?

Generally, treatment means the "provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another."[13]

For the purpose of treatment, otherwise protected health information (PHI) can be shared among health care professionals or providers. There are a plethora of scenarios in which PHI may be exchanged. Most often PHI will be exchanged between professionals, specialists, pharmacists, caretakers, etc. for the purpose of diagnosing, treating, and caring for the patient. Under this rule, PHI may freely be exchanged without a patient's consent between the following, among others:

- Hospitals, clinics, health care facilities, and the professionals, specialists, nurses, coordinating staff employed there;
- Health plan providers;
- Pharmacies, pharmacists, pharmacist technicians;
- Emergency medical technicians;
- Contact lens distributors;
- Nursing homes, professionals, nurses, staff;
- Laboratory technicians and staff;
- Medical device company representatives;[14]and
- Social service agency coordinating or managing patient's health care.[15]

It is important to note that the "minimum necessary" standard, which ordinarily limits the disclosure to only the information necessary to achieve the purpose, does not apply when the disclosure is for treatment purposes.[16]

[13] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/disclosures-treatment-payment-health-care-operations/index.html
[14] https://www.hhs.gov/hipaa/for-professionals/faq/490/when-may-a-covered-health-care-provider-disclose-protected-health-information-without-authorization/index.html
[15] https://www.hhs.gov/hipaa/for-professionals/faq/2073/may-covered-entity-collect-use-disclose-criminal-data-under-hipaa.html
[16] https://www.hhs.gov/hipaa/for-professionals/faq/208/wont-minium-necessary-restriction-impede-delivery/index.html

Question 8:

What is the definition of "payment"?
Under payment, who would/could have access to a patient's health care records?

Payment includes the various activities of health care providers to obtain payment or be reimbursed for the services, and activities of health plan providers or representatives to obtain premiums, fulfill their coverage responsibilities, provide benefits under health plans, and obtain or provide reimbursement for health care.[4]

Under 45 CFR § 164.501, Payment includes any of the following:

- The activities undertaken by:
    - A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or
    - A covered health care provider or health plan to obtain or provide reimbursement for the provision of health care; and
- The activities in paragraph (1) of this definition related to the individual to whom health care is provided and include, but are not limited to:
    - Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
    - Risk adjusting amounts due based on enrollee health status and demographic characteristics;
    - Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
    - Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
    - Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and
    - Disclosure to consumer reporting agencies of any of the following protected health information (PHI) relating to collection of premiums or reimbursement:
        - Name and address;
        - Date of birth;
        - Social Security number;
        - Payment history;
        - Account number; and
        - Name and address of the health care provider and/or health plan.

Under this definition health plan representatives and health care providers all have access to PHI for the purpose of obtaining payment. Beyond PHI, this rule also permits the disclosure of location information, as such information would facilitate the collection of payment.

This information can be shared with virtually anyone who is responsible for billing patients. This includes anyone within health care facilities, health care plan providers, outside labs, ambulance providers, and business associates. Business associates would include debt collection agencies,

acting on behalf of a covered entity, and pharmaceutical manufacturers adjudicating claims.[1718] Additionally, state Medicaid agencies are permitted to disclose PHI to pharmaceutical manufacturers and third party data vendors that are validating claims under the Medicaid Drug Rebate program.[19] However, payment disclosures are limited to sharing only the minimum necessary information for the purpose of payment.

Additionally, covered entities and their business associates are permitted to contact persons other than the patient for the purpose of obtaining payment for health care services.[20] The covered entity is required to limit disclosure to only the minimum necessary information.

Question 9:

What is the definition of "health care operations"?
Under health care operations, who would/could have access to a patient's health care records?

Health care operations includes administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment. This includes activities that are considered a part of case management and care coordination and business management and general administrative activities.

Under 45 CFR § 164.501, this includes:

- Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination;
- Reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities;
- Underwriting and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to health care claims
- Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs;
- Business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and
- Business management and general administrative activities, including those related to implementing and complying with the Privacy Rule and other Administrative

[17] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/disclosures-treatment-payment-health-care-operations/index.html
[18] https://www.hhs.gov/hipaa/for-professionals/faq/455/does-hipaa-permit-health-plans-to-disclose-information-to-pharmaceutical-manufacturers/index.html
[19] https://www.hhs.gov/hipaa/for-professionals/faq/456/does-hipaa-permit-state-medicaid-agencies-to-disclose-information-to-pharmaceutical-manufacturers/index.html
[20] https://www.hhs.gov/hipaa/for-professionals/faq/266/does-the-privacy-rule-permit-a-covered-entity-to-communicate-with-other-parties-regarding-a-bill/index.html

Simplification Rules, customer service, resolution of internal grievances, sale or transfer of assets, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

Under health care operations, nearly anyone within the health care or health plan entity can access a patient's private health information (PHI).[21] This includes legal departments or hired attorneys; billing or accounting departments; medical or professional liability insurance providers or representatives; independent contractors providing business management, care coordination, or administrative services; medical device company representative; and Food and Drug Administration representatives; among others.[22] The otherwise protected health information may be exchanged without a patient's consent between any of the above mentioned groups, so long as they are accessing the information for the purpose of health care operations. Again, these disclosures, under HIPAA, are subject to the minimum necessary standard, meaning only the information necessary for the purpose of health care operations may be disclosed.

Question 10:

Under HIPAA, what would be the "minimum necessary requirement" for the various entities that would have access to a patient's health records for treatment, payment, and operations?

Under HIPAA's Privacy Rule, protected health information (PHI) may be disclosed without a patient's consent, if disclosure is for the purpose of treatment, payment, or health care operations. When disclosed for the purpose of payment or health care operations, the disclosure is limited to the minimum information necessary to achieve that purpose. There is no limit to the information that can be disclosed for the purpose of treatment. This standard requires a covered entity to make reasonable efforts to limit the use, disclosure of, and requests for PHI to the minimum necessary to accomplish the intended purpose.[23] The responsibility to use, disclose, and request the minimum necessary information, falls on the covered entity making the request. The requesting party is responsible for only requesting the minimum information necessary to fulfill their purpose. This is known as the reasonable reliance standard, and permits a covered entity to rely on the judgment of the requesting party, as to the minimum amount of information that is needed. Reliance on the requesting party must be reasonable, and is permitted when made by:

- another covered entity;
- a public official or agency who states the information requested is the minimum necessary for a purpose permitted under 45 CFR 164.512;
- a professional who is a workforce member or business associate of the covered entity holding the information, and who states that the information requested is the minimum necessary for the stated purpose; or

[21] https://www.hhs.gov/hipaa/for-professionals/faq/treatment,-payment,-and-health-care-operations-disclosures/index.html
[22] https://www.hhs.gov/hipaa/for-professionals/faq/490/when-may-a-covered-health-care-provider-disclose-protected-health-information-without-authorization/index.html
[23] https://www.hhs.gov/hipaa/for-professionals/faq/207/how-are-covered-entities-to-determine-what-is-minimum-necessary/index.html

- a researcher with appropriate documentation from an Institutional Review Board or Privacy Board.

However, if the covered entity receiving the request, does not agree that the amount of information requested is reasonably necessary, it is up to both covered entities to negotiate a resolution as to the amount of information needed.[24]

The minimum necessary standard is considered a reasonableness standard that calls for an approach consistent with the policies and procedures of a health care providers; or the best practices and guidelines used by many providers and plans, to limit the unnecessary sharing of medical information.[25] This requires covered entities to evaluate their practices and enhance safeguards to limit unnecessary or inappropriate access to and disclosure of PHI.[26] Under the Privacy Rule, a covered entity must have a policy and procedure addressing the following:

- identify the persons or classes of persons within the covered entity who need access to the information in order to carry out their job duties;
- the categories or types of PHI needed; and
- conditions appropriate for access.

However, these policies and procedures are often created by health care professionals, and are meant to provide flexibility to accommodate numerous circumstances, relying on professional judgment and standards to determine the minimum information necessary. Specifically, this rule requires covered entities to make their own assessment of what PHI is reasonably necessary for a particular purpose, given the characteristics of their business and workforce, and to implement policies and procedures accordingly. Therefore, what is reasonable, even if consistent with health care policies and procedures, is determined only by health care professionals, which may be problematic. For example, if a covered entity has it documented in their policies and procedures that disclosure of an entire medical record is reasonably necessary for certain identified purposes, the health care professional may disclose the persons' entire medical history, without consent and without justifying the disclosure, in those circumstances.[27] Currently, there does not appear to be an outside authority that must determine whether a health care entity's policies and procedures are reasonable, or whether a disclosure consistent with those policies and procedures is reasonable. Whether a health care entity's policies and procedures are reasonable, and whether a disclosure is consistent with those policies and procedures, is only scrutinized through enforcement procedures, which at the federal level only includes the OCR complaint process.

Again, it is important to note that the minimum necessary standard does not apply to disclosures for treatment purposes. Therefore, there is essentially no limit to the information that can be

[24] https://www.hhs.gov/hipaa/for-professionals/faq/216/does-minimum-necessary-standard-apply-to-disclosures/index.html
[25] https://www.hhs.gov/hipaa/for-professionals/faq/207/how-are-covered-entities-to-determine-what-is-minimum-necessary/index.html
[26] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html
[27] https://www.hhs.gov/hipaa/for-professionals/faq/213/what-conditions-may-health-care-provider-use-entire-medical-record/index.html

exchanged for the purpose of treatment. In addition to treatment purposes, the minimum necessary standard does not apply to any of the following disclosures:

- Disclosures to the individual who is subject of the information;
- Disclosures made pursuant to an individual's authorization;
- Disclosures required for compliance with HIPPA's administrative simplification rules;
- Disclosures to HHS when disclosure is required under the Privacy Rule for enforcement purposes;
- Disclosures that are required by other law.

Question 11:

What are other states doing regarding citizens who do not wish to have their health records shared?

Below is a glimpse at each state's requirements for patient consent or authorization for the use or disclosure of medical records. Most states are consistent with HIPAA. Some claim to provide more protections to protected health information (PHI) than HIPAA. However, most of these states provide for the same exceptions to consent as HIPAA.

- Alabama—there does not appear to be additional state protections concerning the disclosure of medical records.
- Alaska—there does not appear to be additional state protections concerning the disclosure of medical records.
    - Alaska statute states that access to medical records is limited to patient, patient's parents or guardians, Department of Social Services, and Medical Review Organization. However, these statutes governing medical records are found under chapters dealing with custody, medical assistance, and a patient's access to their own medical records. There does not appear to be any chapter dedicated to privacy of medical records, and/or language prohibiting others from accessing a patient's record. Therefore, it is assumed that Alaska defaults to HIPAA rules and standards.
        - Department of Social Service has access to financial records of medical assistance beneficiaries, does not have access to personally identifying information.
        - Medical Review Organization does not have access to personally identifying information.
- Arizona—there does not appear to be additional state protections concerning the disclosure of medical records.
    - § 12-2294, under Chapter 13 Evidence, addresses the release of medical and payment records to third parties. However, it specifically includes instances in which health care providers may provide records; references to HIPAA and federal law; exceptions for treatment, accreditation, and quality assurance. The statute, although it covers medical records, does not outline any additional state protections and is found within the chapter concerning evidence in court. Therefore, without mention of further state restriction, it appears that Arizona uses HIPAA as its default "privacy" law.

        - "Health care provider SHALL disclose medical records or payment records, or the information contained in medical records or payment records, without the patient's written authorization, as otherwise required by law or when ordered by a court or tribunal of competent jurisdiction."
        - "A health care provider MAY disclose medical records or payment records, or the information contained in medical records or payment records, pursuant to written authorization signed by the patient or the patient's health care decision maker."
        - "A health care provider MAY disclose medical records or payment records or the information contained in medical records or payment records and a clinical laboratory MAY disclose clinical laboratory results without the written authorization of the patient or the patient's health care decision maker as otherwise authorized by state or federal law, including the health insurance portability and accountability act privacy standards."
- Arkansas— there does not appear to be additional state protections concerning the disclosure of medical records.
    - Medical records are addressed in Chapter 46 of Arkansas Code. However, is only in reference to admissibility at trial.
- California—it is stated that California's Confidentiality of Medical Information Act (CMIA) provides more protections of medical records than HIPAA.[28] However, it is not clear how CMIA provides more protection, as their law has the same exceptions to consent for disclosure as HIPAA.
    - Generally, California law requires written authorization for use or disclosure of medical records. However, there are several exceptions to this requirement. The most notable exception includes the HIPAA Privacy Rule exceptions for treatment, payment, and health care operations.
    - Exceptions to authorization requirement:[29]
        - HIV status and test results may be disclosed for diagnosis, care, treatment, and mandatory state and federal public health reporting;
        - Researchers using medical records that have de-identified data or a limited data set;
        - Health plans can communicate to members about plan benefits, plan services, and availability of cheaper prescription drugs;
        - Providers and plans can advise or educate individuals about treatment options;
        - Mandatory disclosures include court orders, civil and criminal legal proceedings, and when required by law;
        - Disclosure for the purpose of treatment or diagnosis;
        - Disclosures for the purpose of payment;
        - Disclosures for the purpose of health care operations;
        - Access may be granted to business associates;

[28] https://www.privacyrights.org/consumer-guides/health-and-medical-privacy-laws-california-medical-privacy-series

[29] https://www.privacyrights.org/consumer-guides/how-your-medical-information-used-and-disclosed-and-without-consent-california

        - Health care professionals may share information with family, friends, and others involved in a patient's health care or payment; and
        - In several circumstances government agencies and law enforcement may be granted access to medical records without authorization;
- Colorado—there does not appear to be additional state protections concerning the disclosure of medical records.
    - § 25-1-801 of Colorado Statutes governs medical records in Colorado. Paragraph (b)(I)(A) states that a health facility must provide a patient's medical records. . . in accordance with the Health Insurance Portability and Accountability Act, as amended and any rules promulgated pursuant to the act, or to a third person who requests the records upon submission of a HIPAA compliant authorization, valid subpoena, or court order and upon the payment of the reasonable fees."
- Connecticut—there does not appear to be additional state protections concerning the disclosure of medical records.
- Delaware—there does not appear to be additional state protections concerning the disclosure of medical records.
    - In Delaware, patient medical records are governed by §16-12-1212 of Delaware Code.
    - Generally, Delaware law requires informed consent for the disclosure of medical records. However, there are several exceptions to this requirement. The most notable exception includes the HIPAA Privacy Rule exceptions for treatment, payment, and health care operations.
    - Exceptions to informed consent when disclosure is:[30]
        - Directly to the individual;
        - Required by federal or state law and for law enforcement purposes in accordance with 45 C.F.R. Parts 160, 162, and 164 [HIPAA];
        - To public safety authority during a public health emergency;
        - In the course of any judicial or administrative proceeding in accordance with 45 C.F.R. Parts 160, 162, and 164 [HIPAA], or pursuant to a court order to avert danger to individual or public health;
        - To the Child Death Review Commission or Child Protection Accountability Commission;
        - To the Division of Long Term Care Residents' Protection where there is an investigation or survey involving care or treatment of an individual at a facility licensed by the Division, and the individual has been admitted to or discharged from a hospital to the facility.
        - Pursuant to § 2005 of this title;
        - For research, provided the researcher provides documentation that the use or disclose of information has been approved by a privacy board in accordance with HIPAA regulations.
        - For patient treatment and care coordination, including the coordination between health care providers and third parties, consultation between health care providers, and referral of a patient between health care providers;

[30] https://law.justia.com/codes/delaware/2017/title-16/chapter-12/subchapter-ii/section-1212/

        - To a health plan, health care clearinghouse, business associate, or health care provider for the purpose of carrying out financial or administrative activities; and
        - To the Drug Overdose Fatality Review Commission.
- Florida—the only additional protection under Florida law appears to be that there is no exception to consent for the purpose of payment or health care operations.
    - Medical records are governed by § 456.057 of Florida Statutes
    - Generally, Florida law requires written authorization for disclosure. However, there are several exceptions to this requirement. The most notable exception includes an exception for treatment. However, there does not appear to be an exception for payment or health care operations.
    - Exceptions to written authorization under the following circumstances:[31]
        - To any person, firm, or corporation who has procured or furnished such care or treatment with the patient's consent;
        - When compulsory physical examination is made pursuant to Rule 1.360 of Florida Rules of Civil Procedure;
        - In any civil or criminal action, upon the issuance of a subpoena from the court and proper notice to the patient or patient's legal representative by the party seeking records;
        - For statistical and scientific research provided the information does not identify the patient;
        - To a regional poison control center; and
        - To Department of Children and Families, its agent or its contracted entity, for the purpose of investigations or services for cases of abuse, neglect, or exploitation of children or vulnerable adults.
    - "Information disclosed to a health care practitioner by a patient in the course of the care and treatment of such patient is confidential and may be disclosed only to other health care practitioners and providers involved in the care or treatment of the patient, if allowed by written authorization from the patient, or if compelled by subpoena at a deposition, evidentiary hearing, or trial for which proper notice has been given."
- Georgia—governed by § 31-33 of Georgia Code
    - Generally, Georgia law requires written authorization for disclosure. However, there is the good faith exception, meaning that so long as the person violating a patient's privacy acted in good faith, they cannot be found liable.
    - Under § 31-33-2, "any provider or person who in good faith releases copies of medical records in accordance with this Code section shall not be found to have violated any criminal law or to be civilly liable to the patient, the deceased patient's estate, or to any other person."
    - Interestingly, there does not appear to be any exceptions or circumstances in which a health care provider, plan, or other may disclose a patient's medical record without written authorization.[32]

[31] https://law.justia.com/codes/florida/2017/title-xxxii/chapter-456/section-456.057/
[32] https://law.justia.com/codes/georgia/2017/title-31/chapter-33/section-31-33-2/

- Hawaii— there does not appear to be additional state protections concerning the disclosure of medical records.
    - Based on § 323B-3 of Hawaii Statute, it appears that Hawaii has adopted 45 C.F.R. part 164 (HIPAA) as state law governing a patient's health information with personally identifiable information.[33]
- Idaho— there does not appear to be additional state protections concerning the disclosure of medical records.
    - Medical records are addressed in §§ 9-203, 9-340, and 9-420 of Idaho statute. However, these laws are only in reference to admissibility at trial.
- Illinois— there does not appear to be additional state protections concerning the disclosure of medical records.
- Indiana—Governed by § 16-39 of Indiana Code
    - Based on § 16-39-1-4, a patient's consent is required for the release of medical records. However, there are several exceptions in which patient consent is not required.
    - Exceptions include, but are not limited to:
        - Providers are allowed to exchange health records with one another, without patient consent, for the purpose of providing health care services.[34]
        - A person with authorization to consent for a patient has the same right of receiving information and consenting to the release of medical records.[35]
- Iowa— there does not appear to be additional state protections concerning the disclosure of medical records.
    - Under § 653-13.7, it states that patient information may be disclosed with authorization by the patient, law, or for the purpose of treatment.[36]
    - There are mentions of medical records under § 217.30 of Iowa Code. However, this is in reference to privacy policy for medical records for services obtained through Iowa's Department of Human Services.[37] This does not appear to apply to anyone accessing health care outside of Iowa's Department of Human Services.
- Kansas— there does not appear to be additional state protections concerning the disclosure of medical records.
    - Kansas Health Information Technology Act is governed by § 65-6821 — § 65-6835 of Kansas statutes. However under §65-6823 of the Act it states that the purpose is to harmonize state law with HIPAA privacy rule.[38]
    - Reiterates HIPAA, § 65-6825 covers use and disclosure of PHI and specifically references that use and disclosure consistent with 45 C.F.R. Part 164 is permitted.

[33] https://law.justia.com/codes/hawaii/2017/title-19/chapter-323b/section-323b-3/
[34] http://www.healthinfolaw.org/state-law/inter-provider-exchange-records-without-patient%E2%80%99s-consent-%E2%80%93-ind-code-ann%C2%A7-16-39-5-1
[35] http://www.healthinfolaw.org/state-law/requirements-disclosure-medical-information-individuals-authorized-consent-%E2%80%93-ind-code-ann%C2%A7
[36] http://www.healthinfolaw.org/state-law/iowa-admin-code-653-137
[37] https://www.legis.iowa.gov/docs/code/2014/217.30.pdf
[38] https://law.justia.com/codes/kansas/2017/chapter-65/article-68/

- Kentucky— there does not appear to be additional state protections concerning the disclosure of medical records.
- Louisiana— there does not appear to be additional state protections concerning the disclosure of medical records.
    - Hospital Records and Retention Act is governed by § 40:2144 of Louisiana Law, but does not appear to protect a patient's medical records. It appears that this is only meant to define terms and outline process for a patient requesting copies of their records.[39]
- Maine— there does not appear to be additional state protections concerning the disclosure of medical records.
- Maryland—governed by §§ 4-301—309 of Maryland Code.[40]
    - §4-302(a) states that a health care provider shall keep records confidential and disclose only as provided by that statute, or as required by law. There is no further language concerning the term "confidential" under this portion of the statute. The following are the only circumstances for disclosure as outlined by §4-302.
        - Paragraph (c) states that directory information may be disclosed unless expressly prohibited by patient.
        - Paragraph (d) prohibits a person from disclosing records that are disclosed to them unless authorized by the "person in interest"
        - Paragraph (e) states that records may not be transferred as a part of a sale, rental, or bartering of a health care practice/facility; unless, the transfer is in accord with ethical guidelines, in which the records may be transferred.
    - § 4-302.2(d) provides circumstances in which the exchange of health information is not "regulated". These circumstances are similar to HIPAA's Privacy Rule, and include:
        - Between a hospital and credentialed member of the hospital medical staff;
        - Among credentialed members of the hospital medical staff; and
        - Between a hospital and ancillary clinical service providers that are affiliated with the hospital and have signed a business associate agreement.
    - § 4-303 requires health care providers to gain the authorization of a person in interest before disclosing a medical record. However, §4-305 provides for circumstances in which authorization is not required, which closely mimics the exceptions outlined in HIPAA's Privacy Rule. This statute allows for disclosures in the following circumstances, among others:[41]
        - To health care provider's employees, agents, staff, medical students, or consultants for the purpose of payment;
        - To the health care provider's legal counsel relating to the subject matter of the representation;
        - To the provider's insurer or legal counsel for the purpose of handling a claim against the provider;

[39] https://law.justia.com/codes/louisiana/2017/code-revisedstatutes/title-40/rs-40-2144/
[40] https://law.justia.com/codes/maryland/2017/health-general/title-4/subtitle-3/
[41] https://law.justia.com/codes/maryland/2017/health-general/title-4/subtitle-3/section-4-305/

        - Educational research purposes, subject to requirements of institutional review board, so long as they agree to not redisclose personally identifiable information;
        - For the purpose of evaluating management of health care delivery systems, so long as they agree to not redisclose personally identifiable information;
        - For the accreditation of a facility, so long as the professional standard setting entity performing the accreditation agrees to not redisclose personally identifiable information;
        - If disclosure is determined necessary to provide emergency health care needs to recipient; and
        - For the purpose of coordinating services and record retention with Montgomery County Department of Health and Human Services.
    - Additionally, under § 4-309, there are criminal penalties for wrongly disclosing or obtaining a medical record. If wrong disclosure is done knowingly and willfully, person can be charged with a misdemeanor, and may face fines up to $50,000 and imprisonment up to one year. Penalties exceed if disclosure is done under false pretenses, and exceed again if disclosure is done with intent to sell, transfer, or use for commercial advantage, personal gain, or malicious harm.[42]
- Massachusetts— there does not appear to be many additional state protections concerning the disclosure of medical records. The recent passing of the PATCH act limits disclosures for the purpose of payment, but does not address disclosures for the purpose of treatment or operations.
    - § 70E of Massachusetts law states that patients have a right to "confidentiality of all records and communications to the extent provided by law." However, without providing further information, it is assumed that "to the extent provided by law" refers to HIPAA. There does not seem to be an additional laws providing protection, so the default rule would be HIPAA.
    - On March 30, 2018 the Governor of Massachusetts signed the PATCH (an Act to Protect Access to Confidential Healthcare) bill into law, which does provide some additional protections to patient privacy. However, it mostly focuses on how patient privacy can be protected throughout the payment process.
        - For example paragraph (a) creates a common summary of payment forms and paragraph (e) states that carriers shall not specify or describe sensitive health care services in the common summary of payments form.[43]
- Michigan— there does not appear to be additional state protections concerning the disclosure of medical records.
    - Michigan's Medical Records Access Act seems to only govern how a patient may request copies of their own records, and additional standards providers have in fulfilling their patient's requests.
- Mississippi— there does not appear to be additional state protections concerning the disclosure of medical records.

[42] https://law.justia.com/codes/maryland/2017/health-general/title-4/subtitle-3/section-4-309/
[43] https://malegislature.gov/Laws/SessionLaws/Acts/2018/Chapter63

- Missouri— there does not appear to be additional state protections concerning the disclosure of medical records.
    - However, there may be more remedies, under state law, for residents who have had their records wrongfully disclosed under HIPAA.[44]
- Montana—there does not appear to be additional state protections concerning the disclosure of medical records.
    - Medical records are governed by § 50-16-525 of Montana Code
    - Generally, a health care provider cannot disclose health care information without the patient's written authorization. However, there are several circumstances in which a patient's authorization is not required. These exceptions are consistent with HIPAA's Privacy Rule.
    - The following are some of the circumstances in which a patient's information may be disclosed without patient authorization:
        - To a person providing health care to the patient;
        - To provide planning, quality assurance, peer review, or administrative, legal, financial or actuarial services to the health care provider for assisting in the delivery of health care;
        - To immediate family members of the patient or another person with a close personal relationship with the patient, unless the patient has instructed the provider not to make the disclosure;
        - For use in a research project, as determined by an institutional review board;
        - To a person obtaining the information for the purpose of an audit;
        - To an official or a penal or custodial institution in which the patient is detained; and
        - To any contact, if the health care provider reasonably believes the disclosure will avoid or minimize an imminent danger to the health or safety of the contact or another individual.
- Nebraska— there does not appear to be additional state protections concerning the disclosure of medical records.
    - § 71-961 of Nebraska Code states that all records are confidential, with certain exceptions.
    - Exceptions to confidentiality include:[45]
        - the subject of the records;
        - the subject's legal counsel;
        - the subject's guardian or conservator;
        - persons authorized by a court order;
        - agents or employees of the Department of Human Services, upon subpoena from the Department in connection to an investigation;
    - Although there doesn't appear to be exceptions for treatment, payment, and health care operations, there also doesn't appear to be any explicit protections. Therefore, it is not clear what is meant by confidential, and it is assumed the default rule would be HIPAA's Privacy Rule.

[44] http://bdslaw.com/2015/06/missouri-medical-records-privacy-and-hipaa/
[45] https://law.justia.com/codes/nebraska/2017/chapter-71/statute-71-961/

- Nevada— there does not appear to be additional state protections concerning the disclosure of medical records.
    - Health records are governed by Chapter 629 of Nevada Statute. However, there does not appear to be a specific statute that outlines how a patient's medical records are protected.
    - § 629.051 covers the retention and destruction periods for records.
    - § 433.332 requires copies to be forwarded, without patient's consent, upon transfer to a new medical facility
    - §49.215 outlines confidential communications between health care professionals and patient, and §49.245 outlines exceptions to confidential communications.
- New Hampshire— there does not appear to be additional state protections concerning the disclosure of medical records.
    - Patient privacy is governed by Chapter 332-I of New Hampshire Code.[46]
    - § 332-I:2 states that health care providers shall not reveal confidential communication or information without the consent of the patient, unless permitted by law or the need to protect the welfare of the individual or public interest.[47]
    - Not only does "permitted by law" presumably include HIPAA, there are several exceptions to confidentiality under New Hampshire law that are consistent with HIPAA.
        - § 332-I:3 states that "a health care provider or a business associate of a health care provider or a patient or patient's legal representative may transmit the patient's protected health information through the health information organization. Only a health care provider, for purposes of treatment, care coordination, or quality assurance, or a patient or a patient's legal representative with respect to the patient's protected health information, may have access to protected health information transmitted."
    - § 332-I:5 also states that in the event that PHI is disclosed in violation of New Hampshire law, but in circumstances permitted by federal law, the health care provider or business associate shall notify the individual in writing.
        - § 332-I:6 states that aggrieved individuals may bring a civil action and shall be awarded damages of no less than $1,000 for each violation + costs and reasonable legal fees.
    - Although New Hampshire law is consistent with HIPAA's Privacy Rule, New Hampshire law also establishes the requirement of an audit log for transactions involving health information.
        - Paragraph III of § 331-I:3 states that "The health information organization shall maintain an audit log of the transactions transmitted through the health information organization. The parties transmitting or receiving information through the health information organization shall maintain audit logs in accordance with nationally accepted interoperability standards, practices, regulations, and statutes, including but not limited to: (a) The identity of the health care provider accessing the information; (b) The identity of the individual whose protected health

[46] https://law.justia.com/codes/new-hampshire/2017/title-xxx/chapter-332-i/
[47] https://www.dhhs.nh.gov/hie/documents/laws.pdf

information was accessed by the health care provider; (c) The date the protected health information was accessed; and (d) The area of the record that was accessed."
        - At the very least, this provides patient's with the ability to review who has accessed their records.
- New Jersey— there does not appear to be additional state protections concerning the disclosure of medical records.
    - Under § 26:2B-20 a patient's records are considered confidential and only available upon proper judicial order. However, there is no additional information outlining the proper procedures for disclosure of medical records, or exceptions to confidentiality. Therefore, it is assumed New Jersey law would default to HIPAA.
- New Mexico— there does not appear to be additional state protections concerning the disclosure of medical records.
    - § 24-1-15.4 states that disclosures without the authorization are subject to state and federal law. However, it does not appear there are any other state laws addressing the subject, so it is assumed HIPAA is the law by default.
    - § 24-1-20 states that records are confidential, but does not provide additional information on disclosure of medical records.
    - § 24-14A-8 concerns the confidentiality of health information systems, it states that data shall be "public records if the release of these data does not violate state or federal law relating to the privacy and confidentiality of individually identifiable health information." Again, it seems New Mexico defaults to federal law. [48]
    - § 24-14B-6 states that electronic health information shall not be disclosed without a patient's authorization unless otherwise permitted by state or federal law. Again, it seems New Mexico defaults to federal law.[49]
- New York—there does not appear to be additional state protections concerning the disclosure of medical records.
    - NY Pub Health L §§ 17-18 govern the release of medical records, and require the written request of a patient to release records. There is no mention, in either section, of exceptions to patient consent for the purpose of treatment, payment, or operations.[50]
- North Carolina— there does not appear to be additional state protections concerning the disclosure of medical records.
    - The North Carolina Health Information Exchange Act, was adopted to improve the delivery of health information, in a "manner that is consistent with the Health Insurance Portability and Accountability Act, Privacy Rule, and Security Rule." Therefore, it provides the same "protection" as HIPPA. However, there is an option to opt out of the health information exchange.[51]

[48] https://law.justia.com/codes/new-mexico/2017/chapter-24/article-14a/section-24-14a-8/
[49] https://law.justia.com/codes/new-mexico/2017/chapter-24/article-14b/section-24-14b-6/
[50] https://law.justia.com/codes/new-york/2017/pbh/article-1/title-2/
[51] https://law.justia.com/codes/north-carolina/2016/chapter-90/article-29a/section-90-413.2/

    - Once a person opts out, the PHI belonging to that individual may not be disclosed to covered entities through the HIE Network for any purpose[52]
    - If a person opts out, it is not clear what laws are in place to protect their physical records from being disclosed.
- North Dakota— there does not appear to be additional state protections concerning the disclosure of medical records.
- Ohio— there does not appear to be additional state protections concerning the disclosure of medical records.
    - § 3701 of Ohio Code governs medical records.
    - § 3701-83-07 and 3701-84-07 require that every health care facility develop and follow patient care policies that include rights for each patient to have their medical and financial records kept confidential. The statute does not further elaborate on how records are kept confidential or if there are exceptions. It is assumed that because there is no language indicating stricter protections than HIPAA, that this statute provides the same "protection" as HIPAA. [53]
- Oklahoma— there does not appear to be additional state protections concerning the disclosure of medical records.
- Oregon— there does not appear to be additional state protections concerning the disclosure of medical records.
    - § 192.553 of Oregon Statute states that an individual has the right to have PHI safeguarded from unlawful use or disclosure. Again, however, there is no indication on how records are kept confidential, or whether there are exceptions to disclosure. Additionally, HIPAA is referenced in the statute, stating that in addition to safeguards from disclosure, the rights and obligations under HIPAA apply. Therefore, it appears that this statute provides the same "protection" as HIPAA.[54]
- Pennsylvania—it appears that under Pennsylvania Code medical records are confidential and that disclosure requires the written authorization of the patient.
    - Medical records are governed by Chapters 25 and 563 of Pennsylvania Code
    - Under § 563.9, records shall be treated as confidential. Only authorized personnel shall have access to the records. The written authorization of the patient shall be presented and then maintained in the original record as authority for release of medical information outside the ASF.
        - However, there is the exception for treatment purposes, in which written authorization is not required.
        - § 25.213 outlines what is included in medical records and retention periods. It also states that records shall be kept confidential, unless disclosure is required for treatment.
- Rhode Island—Confidentiality of Health Care Communications and Information Act § 5-37.3 of Rhode Island General Laws[55]

[52] https://law.justia.com/codes/north-carolina/2016/chapter-90/article-29a/section-90-413.6/
[53] https://law.justia.com/codes/ohio/2017/title-37/chapter-3701/
[54] https://law.justia.com/codes/oregon/2017/volume-05/chapter-192/section-192.553/
[55] https://law.justia.com/codes/rhode-island/2017/title-5/chapter-5-37.3/section-5-37.3-4/

- Paragraph (a)(1) states that "a patient's confidential health care information shall not be released or transferred without the written consent of the patient, or his or her authorized representative, on a consent form meeting the requirements of subsection (d) of this section."
    - Paragraph (a) also provides remedies and damages for violations of this statute.
- However, there are several exceptions to the written authorization requirement. These exceptions are outlined in paragraph (b) of the Act, and include:
    - To a physician, dentist, or other medical personnel who believes, in good faith, that the information is necessary for diagnosis or treatment of that individual in a medical or dental emergency;
    - To medical and dental peer review boards, or the board of medical licensure and disciplines, or to the board of examiners in dentistry;
    - To qualified personnel for the purpose of conducting scientific research, audits, evaluations, actuarial, insurance underwriting, or similar studies; provided, that personnel shall not identify or otherwise disclose patient identities in any manner;
    - By a health care provider to appropriate law enforcement personnel;
    - By a health care provider to a person if the provider believes the person (or his/her family) is in danger of the patient;
    - To the health care provider's own lawyer or medical liability insurance carrier, if there is a medical liability action against the health care provider.
- According to paragraph (d) consent forms must include:
    - A statement of the need for and proposed uses of that information;
    - A statement that all information is to be released or clearly indicating the extent of the information to be released; and
    - A statement that the consent for release or transfer of information may be withdrawn at any future time and is subject to revocation.

- South Carolina—Physicians' Patient Records Act, § 44-115 of South Carolina Code of Laws.
    - Under § 44-115-40, a physician shall not release records without the receipt of express written consent of the patient or a person authorized by law to act on the patient's behalf.
    - § 44-115-60 permits physicians to disclose a summary of a patient's medical record, in lieu of the full record. Instances in which a physician may disclose a summary include:
        - when he has a reasonable belief that release of the information contained in the entire record would cause harm to the patient's emotional or physical well-being, the emotional or physical well-being of another person who has given information about the patient to the physician;
        - or where release of the information is otherwise prohibited by law.
    - It appears that there are no exceptions to written consent, but that a summary can be provided in circumstances where providing the entire medical record would be prohibited under the Act, or other laws.

- South Dakota—there does not appear to be additional state protections concerning the disclosure of medical records.
- Tennessee—the only additional protection under state law, is that there is no exception to patient consent for the purpose of payment. However, there are exceptions to consent for the purpose of treatment and operations.
    - § 68-11-15 of Tennessee Code outlines the Patient's Privacy Protection Act, which establishes the right to patient privacy at health care facilities. However, there are several exceptions in which there is no apparent right to privacy. These exceptions include:[56]
        - When reporting to health or government authority is statutorily required;
        - For the purpose of utilization reviews, case management, peer reviews, or other administrative functions;
        - Access by health care providers from whom the patient receives or seeks care;
        - Directory information, so long as the patient has been notified and does not object;
        - Any request by the office of inspector general or the Medicaid fraud control unit with respect to ongoing investigation.
    - Additionally, according to § 68-11-312, there is no implied covenant of confidentiality that prohibits health care providers from communicating with one another in the course of treatment. It also states that health care providers may respond to a request from a hospital regarding treatment. Arguably, this last exception for requests from the hospital is consistent with HIPAA's exception for operations.
        - Paragraph (c) of §68-11-312 also states that it is not to be construed to authorize disclosure of information otherwise prohibited by HIPAA.
    - It does not appear that Tennessee law allows for disclosure of medical records, absent patient consent or authorization, for the purpose of payment. However, there is nothing in Tennessee law that directly addresses this HIPAA exception, and states that it is not permitted.
- Texas—there does not appear to be additional state protections concerning the disclosure of medical records.
    - § 181.153(a) states that a covered entity may not disclose an individuals PHI except for the purpose of treatment, payment, health care operations, or performing an insurance or health maintenance organization function.[57]
- Utah—there does not appear to be additional state protections concerning the disclosure of medical records.
- Vermont—there does not appear to be additional state protections concerning the disclosure of medical records.
    - Accord to 18 V.S.A. § 1881 a covered entity is prohibited from disclosing PHI unless disclosure is permitted under HIPAA.

[56] https://law.justia.com/codes/tennessee/2017/title-68/health/chapter-11/part-15/section-68-11-1503/

[57] https://law.justia.com/codes/texas/2017/health-and-safety-code/title-2/subtitle-i/chapter-181/

    - 18 § 9351 of Vermont Statute covers Health Information Technology. It states that privacy standards shall be no less stringent than applicable state and federal guidelines, including HIPAA. However, the state seems to follow HIPAA, so there are no additional protections to electronic records.
- Virginia— the only additional protection under state law, is that there is no exception to patient consent for the purpose of treatment. However, there are exceptions to consent for the purpose of operations and payment.
    - § 32.1-127.1:03 of Virginia Code covers privacy of medical records, and states that records are confidential, unless stated otherwise by law. According to paragraph (c) medical records are not confidential and can be disclosed without a patient's authorization in the following circumstances, among others:[58]
        - In compliance with subpoena, search warrant, or court order;
        - When disclosure is reasonably necessary to establish or collect a fee;
        - To defend a health care entity and employees or staff, against accusations of wrongful conduct;
        - As required in the course of an investigation, audit, review, or proceeding conducted by law enforcement, licensure, accreditation, or professional review entity;
        - In connection with the health care entity's operations or another health care entity's operations; and
        - To third party payors and their agents for purposes of reimbursement;
    - It is interesting to note, there does not appear to be an exception to patient consent for the purpose of treatment. Other than this, paragraph (c) provides for the same exceptions as HIPAA's Privacy Rule.
- Washington—there does not appear to be additional state protections concerning the disclosure of medical records.
    - Governed by § 70.02 of Washington Code.
    - Generally, disclosure of health care information requires a patient's written authorization. However, there are several exceptions in which a patient's written authorization is not required.[59]
    - These exceptions include the following, among others:
        - To third party payors for the sole purpose of payment;[60]
        - To persons reasonably believed to be providing health care to the patient;[61]
        - To any person who requires health care information for health care education, providing planning, quality assurance, peer review, or administrative, legal, financial, actuarial, or other health care operations.
    - Essentially Washington has the same exceptions to patient authorization as HIPAA's Privacy Rule.
- West Virginia—there does not appear to be additional state protections concerning the disclosure of medical records.

[58] https://law.justia.com/codes/virginia/2017/title-32.1/chapter-5/section-32.1-127.1-03/
[59] https://law.justia.com/codes/washington/2017/title-70/chapter-70.02/section-70.02.020/
[60] https://law.justia.com/codes/washington/2017/title-70/chapter-70.02/section-70.02.030/
[61] https://law.justia.com/codes/washington/2017/title-70/chapter-70.02/section-70.02.050/

- Wisconsin—there does not appear to be additional state protections concerning the disclosure of medical records.
    - Public health is governed by Chapters 145—160 of Wisconsin Code. Laws regulating health care records can be found in Chapters 146 and 153.
    - § 146.816 states that a covered entity must comply with the privacy obligations of 45 CFR 164.520, which is HIPAA's notice requirement.
    - § 146.82 states that a patient's medical records are confidential, requiring a patient's informed consent prior to disclosure, except in the circumstances outlined by 45 CFR Part 164 Subpart E.[62]
        - 45 CFR Part 164 Subpart E is the portion of HIPAA that outlines all instances of disclosure in which patient authorization is not required.
    - There does appear to be increased penalties for violations of a patient's privacy related to their medical records.[63]
- Wyoming—there does not appear to be additional state protections concerning the disclosure of medical records.
    - Governed by § 35-2-606 through 609 of Wyoming statutes.
    - Generally, Wyoming law requires written authorization for disclosure. The written authorization must be in writing, signed, dated, identify what can be disclosed, and the person to whom the information is to be disclosed. However, there are several exceptions to this requirement, which are consistent with HIPAA.
    - Exceptions to written authorization under the following circumstances:[64]
        - To a person providing health care to the patient;
        - To any other person who requires health care information for health care education or to provide planning, quality assurance, administrative, legal, financial, or actuarial services to the hospital, or assist the hospital in delivery of health care;
        - To any health care provider who has previously provided health care to the patient, to the extent necessary to provide health care to the patient, unless the patient has instructed the hospital not to make the disclosure;
        - To any person if the hospital reasonably believes that the disclosure will avoid or minimize an imminent danger to the health or safety of the patient or any other individual;
        - To immediate family members of the patient, or any other individual with whom the patient is known to have a close personal relationship, if made in accordance with good medical or other professional practice, unless the patient has instructed the hospital not to make the disclosure;
        - To a health care facility who is the successor in interest to the hospital maintaining the health care information;
        - For use in certain research projects as determined by an institutional review board;
        - For purposes of an audit; and

[62] https://law.justia.com/codes/wisconsin/2017/chapter-146/section-146.82/
[63] https://law.justia.com/codes/wisconsin/2017/chapter-146/section-146.84/
[64] https://law.justia.com/codes/wyoming/2017/title-35/chapter-2/article-6/section-35-2-609/

- To an official of a penal or other custodial institution in which the patient is detained.

Question 12:

How would elimination of the Minnesota consent requirement impact sharing through the state or other health information exchanges, or the national health information exchange, called the eHealth Exchange?

In comparison to many other states, Minnesota's Health Records Act (MHRA) has fewer exceptions for gaining consent prior to disclosing otherwise protected health information (PHI). Weakening these consent requirements and/or increasing the exceptions to consent, would align Minnesota with the practices of a majority of other states, and HIPAA. It also could simplify and increase the effectiveness of the information exchange process. However, by increasing exceptions to consent requirements, Minnesota would be removing standards that were designed to protect patient privacy and provide Minnesotans control over their medical records.

Electronic Health Records (EHR) are "real-time, patient centered records . . . [that] bring together in one place everything about a patient's health."[65] The Office of the National Coordinator for Health Information Technology (ONC) is part of the U.S. Department of Health and Human Services, and helps to administer the national eHealth Exchange. All 50 states participate in the eHealth Exchange. However, the records of each patient included on the eHealth Exchange depends on state law. The less rigid a state law is on patient privacy, the more information will appear in that persons EHR on the eHealth Exchange. Given that MHRA is one of the most restrictive state policies, the information on the eHealth Exchange for Minnesotans should be limited and would contain less PHI than other states with fewer consent requirements. Eliminating consent requirements for Minnesotans would increase the information available for exchange on the eHealth Exchange.

The website for the National Coordinator for Health Information Technology (ONC) suggests that by making health records electronic and accessible on the national eHealth Exchange, the exchange of information will be more efficient and cost effective. ONC lists the following as positive outcomes of the eHealth Exchange:[66]

- eHealth Exchange will contain information about a patient's medical history, diagnoses, medications, immunization dates, allergies, radiology images, and lab and test results.
- Offers access to evidence based tools that provider can use to make decisions about a patient's care;
- Automates and streamlines providers' workflow;
- Increases organization and accuracy of patient information;
- Supports key market changes in payer requirements and consumer expectations;
- Reduces transcription costs;
- Reduces chart pull, storage, and re-filing costs;

[65] https://www.healthit.gov/topic/health-it-and-health-information-exchange-basics/what-are-electronic-health-records-ehrs

[66] https://www.healthit.gov/topic/health-it-basics/medical-practice-efficiencies-cost-savings

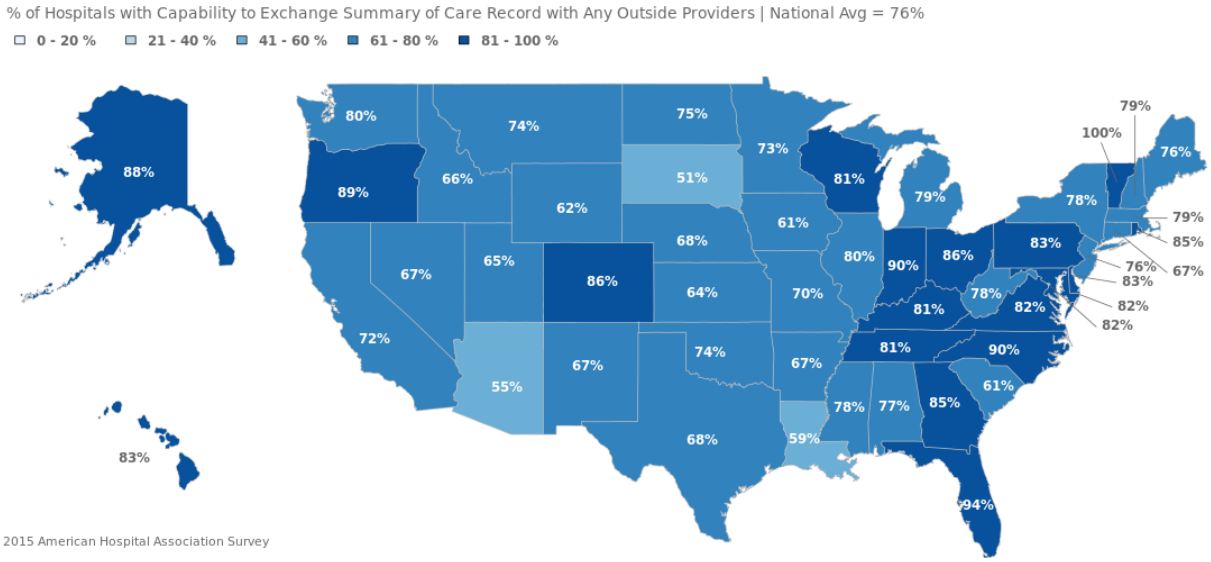
- Improves patient health/quality of care through better disease management and patient education;
- Improves medical practice management through an integrated scheduling system linking appointments directly to progress notes, automate coding, and managed claims;
- Saves time with a centralized chart management system, condition-specific queries, and other shortcuts;
- Enhances communication with other clinicians, labs, and health plans through access to patient information from anywhere; tracking electronic messages between other clinicians, hospitals, labs, etc.;
- Enhances ability to meet important regulation requirements through alert system that notifies physicians to complete key regulatory data elements;
- Reduces time and resources needed for manual charge entry resulting in more accurate billing and reduction in lost charges;
- Reduces charge lag days and vendor/insurance denials associate with late filing;
- Alerts providers to obtain advance beneficiary notice, minimizing claim denials and lost charges related to Medicare procedures performed without an advance beneficiary notice.

Although ONC suggests that the eHealth Exchange will improve the exchange of information and reduce the cost of exchanging information, the ONC does not include the extent of those savings, and whether those savings will positively impact health care providers, health plans, or patients.

In 2017, the Minnesota Department of Health found that MHRA cost patients only .83 per encounter.[67] Although this does not demonstrate how much Minnesotans may save by increasing PHI on the eHealth Exchange, it does demonstrate that MHRA is not a large cost to patients per encounter. Therefore, it is hard to conclude that patients would see any noticeable decrease in health care cost by reducing consent requirements in Minnesota. Arguably, the mostly likely benefit a patient will experience is a reduction in their role or responsibility for exchanging information. Based on this information, it appears that any reduction in consent requirements would largely benefit health care providers and professionals, and their business associates.

Below is a map depicting the percentage of hospitals that can exchange a summary of care record with outside providers. As shown, 73 percent of hospitals in Minnesota can exchange a summary of care record with outside providers, which is only three percent below the national average.[68] This demonstrates that although Minnesota has one of the most stringent health care record laws, it has not prohibited hospitals from exchanging information with outside providers.

[67] http://www.health.state.mn.us/e-health/legrpt/docs/rfi-health-record-act2017.pdf
[68] https://dashboard.healthit.gov/apps/hospital-health-it-adoption.php


% of Hospitals with Capability to Exchange Summary of Care Record with Any Outside Providers | National Avg = 76%
0 - 20 %
21 - 40 %
41 - 60 %
61 - 80 %
81 - 100 %
88%
80%
74%
75%
73%
79%
100%
76%
89%
66%
51%
81%
79%
78%
62%
61%
79%
68%
83%
85%
67%
65%
86%
64%
70%
80%
90%
86%
76%
83%
78%
82%
72%
81%
82%
82%
74%
67%
81%
90%
55%
67%
61%
78%
77%
85%
68%
59%
94%
83%
2015 American Hospital Association Survey