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

Prepared by Maren Bardal, Research Assistant, Legislative Commission on Data Practices

Index

Question 10: **p. 20**

How many hospital and clinic consent forms include consent for data-sharing on the same form as the consent for treatment? Is there one signature or separate signatures?

Question 11: **p. 21**

Who were the "national organizations" contacted for the Care Coordination Measures Atlas (and the updated Atlas) and what information did they provide?

Did any Minnesota providers or companies participate/provide info toward development of the Atlas?

Question 1:

What is the Administrative Simplification provision?
What is the Security Rule?
Are either used to determine the minimum necessary standard?

The Administrative Simplification provision was created to improve efficiency and effectiveness of health care systems, by publishing and adopting national standards for electronic health care transactions and code sets, unique health identifiers, and security.[1] These standards include:

- Electronic health transaction standards and code sets — the implementation of a national standard for transmitting health data electronically and using standard code sets to describe diseases, injuries, and other health problems.
- Unique identifiers — a system that uses one identification number per employer, health plan or payer, and health care provider to simplify administration.
- Security — safeguarding the storage of, access to, and transmission of electronic patient information.
- Privacy — generally, limiting the use or disclosure of protected health information to a minimum necessary standard. It also gives patients the right to see and get copies of their records, request amendments to their records, and learn details of certain disclosures of their records.

The security standard, required by the Administrative Simplification regulation, is further described under HIPAA's Security Rule, 45 CFR § 164.[2]

Generally, the Security Rule requires covered entities and business associates to do four things:

- Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part; and
- Ensure compliance with this subpart by its workforce.[3]

As part of this, the Security Rule requires covered entities to maintain reasonable administrative, technical, and physical safeguards for protecting electronic protected health information (e-PHI).

- "Administrative safeguards are administrative actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to safeguard electronic protected health information and manage the conduct of the covered entity's workforce in relation to the protection of that information."
- "Physical safeguards are physical measures, policies and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards and unauthorized intrusion."
- "Technical safeguards are the technology, policy and procedures for its use that safeguard electronic protected health information and control access to e-PHI."

[1] https://www.hhs.gov/hipaa/for-professionals/index.html
[2] https://www.law.cornell.edu/cfr/text/45/part-164
[3] https://www.law.cornell.edu/cfr/text/45/164.306

Additionally, the administrative safeguards provision, 45 CFR § 164.308, includes standards designed to limit the use and access to e-PHI. According to § 164.308(a)(4), which is part of the Security Rule, a covered entity or business associate must implement policies and procedures for authorizing access to e-PHI. This requires that those policies and procedures are consistent with the applicable requirements of subpart E, which includes the minimum necessary standard. It also requires that a covered entity or business associate establish role based access policies and procedures. Paragraph (a)(3)(ii) states that a covered entity must implement procedures to determine that "the access of a workforce member to electronic protected health information is appropriate."

Question 2:

What are duplicate tests, are there legitimate needs for duplicate testing? Would eliminating patient privacy and consent rights eliminate duplicate testing in Minnesota?

Duplicate testing is the repeating of labs or other diagnostic evaluations. When a duplicate test is performed without a legitimate need, it needlessly costs patients their time and money, and may negatively impact their health. A 2014 study, published by the American Journal of Clinical Pathology, found that duplicate testing often occurs when a second physician is unaware of the first physician's existing testing order, and mistakenly orders a second test.[4] This study does not assert why a second physician would be unaware of an existing testing order. However, several causes for the ordering of duplicate testing have been identified, several of which show that a delay or void in accurate information may be to blame. These causes of duplicate testing include, but may not be limited to:

- legitimate medical need or clinical reason;
- the practice of defensive medicine;
- overlay in medical records creating one record for multiple people;
- patients having multiple or duplicate partial medical records;
- error during patient registration;
- error in transcription or data entry; and, or
- absences in the patient's medical records.

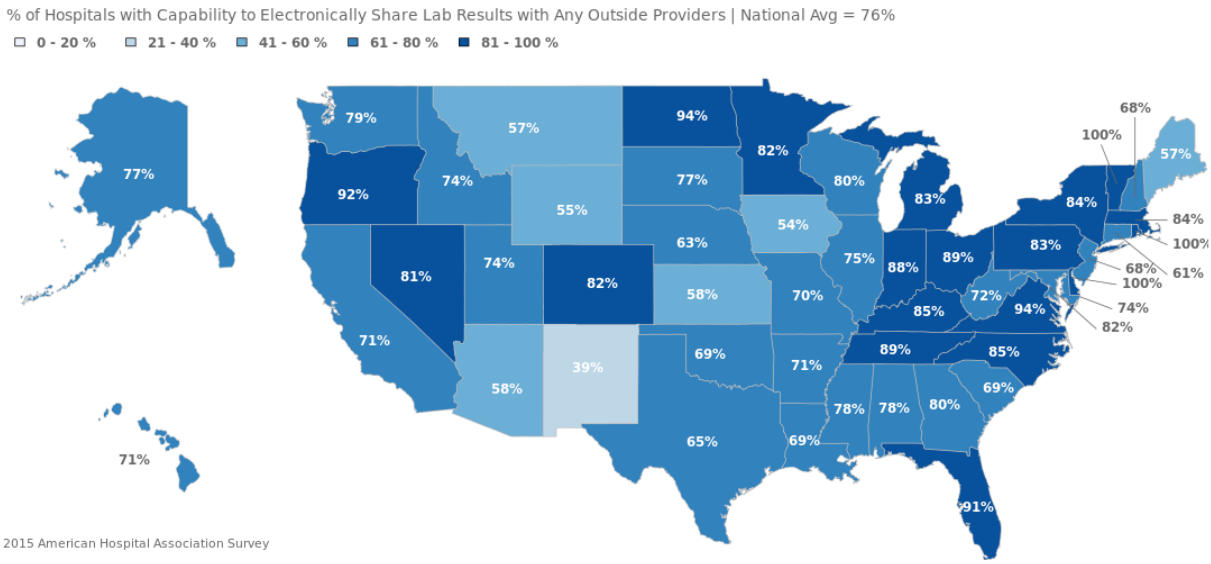
A 2009 article estimated that eliminating duplicate tests would have saved hospitals in the United States $8 billion in the year 2004.[5] Other articles report $20 billion is wasted on duplicate testing every year.[6] One article even claims $200 billion is wasted annually on excessive testing and treatment.[7] It has been suggested that each duplicate test costs $1,099.[8] Based on the costs to patients and payers, reducing or eliminating duplicate testing may provide savings to patients and payers.

---

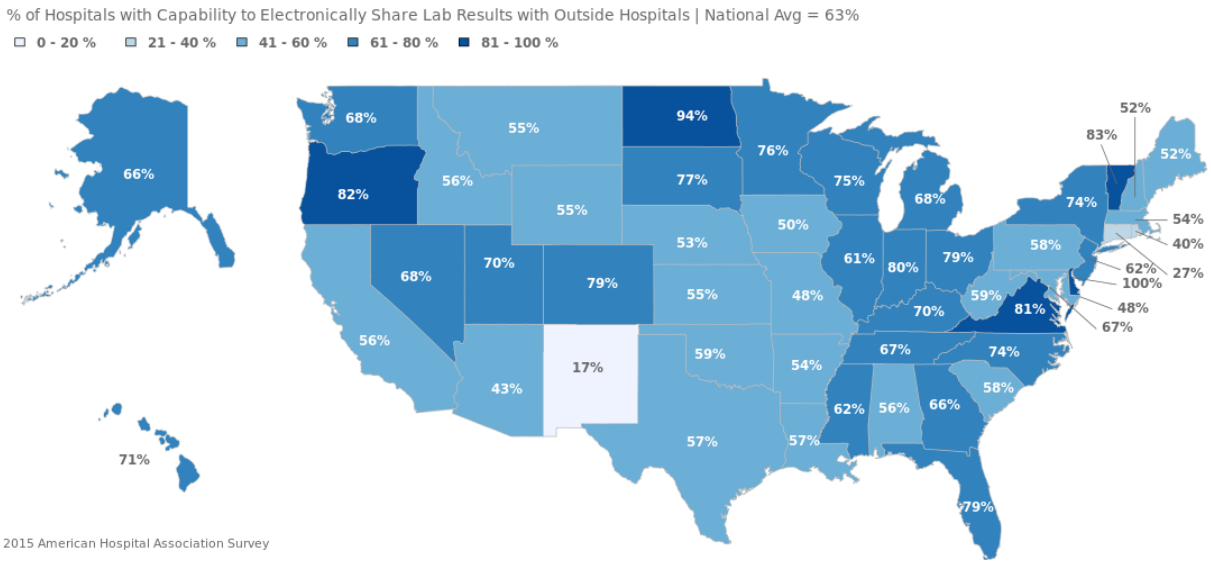
[4] https://academic.oup.com/ajcp/article/143/5/623/1760774
[5] https://www.healthaffairs.org/doi/pdf/10.1377/hlthaff.28.5.1475
[6] https://www.unh.edu/healthyunh/blog/healthcare-consumerism/2015/05/doing-away-duplicate-testing-can-cut-healthcare-costs
[7] https://money.cnn.com/2017/05/20/news/economy/medical-tests/index.html
[8] http://healthitmhealth.com/health-infographic-week-duplicates-hidden-cost-healthcare/

It has been theorized that duplicate testing may be avoided by reducing a patient's privacy rights and, or increasing the use and efficiency of electronic health records (EHR).[9] Using an electronic medical record system or health information exchange (HIE), like the eHealth Exchange, likely improves health care providers and professionals access to records; dependent upon state law. As a result, professionals with quick access to complete and accurate records may be less likely to order duplicate testing.[10]

As described in Part I, Minnesota currently ranks just three percent below the national average for the capability to electronically share summary of care records with outside providers. Additionally, Minnesota currently exceeds the national average by six percent, for the capability to electronically share lab results with outside providers.[11] This is demonstrated in the first graphic below. Furthermore, Minnesota currently exceeds the national average by 13 percent, for the capability to electronically share lab results with outside hospitals. This is demonstrated in the second graphic, which can be found on the following page, page four.



[9] https://pdfs.semanticscholar.org/8b95/dc6a2970e0b61bb56f5bd560b4956aef34c7.pdf
[10] https://www.brookings.edu/blog/techtank/2017/05/26/health-information-exchanges-reduce-redundant-medical-procedures/
[11] https://dashboard.healthit.gov/apps/hospital-health-it-adoption.php



As these maps depict, Minnesota hospitals consistently rank above average in their capability to electronically share information.

A study of western New York's networks, found that an HIE lowers the repetition of therapeutic procedures aimed at improving a patient's condition. However, it also found that the HIE did not affect diagnostic procedures that determine the extent of a patient's illness.[12] Another study also found that that HIEs are often not used to exchange lab and diagnostic test results, and that many of these systems do not allow for communication among health care professionals.[13] As a result, it is suggested that systems use what is known as Computerized Provider Order Entry (CPOE) to reduce the number of duplicate image tests, and what is known as Picture Archival and Communication Systems (PACS) to reduce duplicate radiology imaging examinations.

CPOEs have been found to reduce transcription error, provide real-time information to health care providers, and can be adapted to alert or block duplicate test orders for select tests.[14] A two year study at the Cleveland Clinic showed that a CPOE system, when combined with a Clinical Decision Support Tool (CDST), blocked 12,204 duplicate orders, and allowed only 414 duplicate tests, making the CDST 96% effective and saving the Clinic $183,586.[15] This study used a CDST with a "hard block" that required a health care provider to call client services to override the blocking of a duplicate test order.

A second study of seven Cleveland area hospitals analyzed the use of a CDST using a "smart alert". A smart alert is different from a hard block. It does not require calling client services to override a block on duplicate testing. The study showed that the smart alert CDST approach was much less effective. Over the course of a year it was only effective 43% of the time, blocking

[12] https://www.brookings.edu/blog/techtank/2017/05/26/health-information-exchanges-reduce-redundant-medical-procedures/
[13] https://pdfs.semanticscholar.org/8b95/dc6a2970e0b61bb56f5bd560b4956aef34c7.pdf
[14] https://academic.oup.com/ajcp/article/141/5/718/1761633
[15] https://academic.oup.com/ajcp/article/141/5/718/1761633

only 5,669 of the 12,990 duplicate tests, and saving the seven hospitals a combined $94,225, less than $13,500 in savings to each hospital.

Additionally, it has been found that due to incompatible systems, the electronic records received may often be incomplete, and can also lead to duplicate testing.[16] It is suggested that interoperable systems with integrated decision support will be able to prevent incomplete transfers and reduce or eliminate duplicate testing. An interoperable system should have the ability to interpret and convey shared data, which contains prior rest results, notification, alerts, decision support, and imaging studies.

In regards to interoperability, Minnesota hospitals' interoperability systems consistently rank above average; with the exception of one circumstance, in which Minnesota ranks just one percent below the national average. For example, 63% of hospitals in Minnesota can electronically find patient health information from outside providers, which is 12% above the national average. Additionally, 58% of Minnesota's hospitals electronically integrate any patient information from outside providers. The national average is 50% of hospitals. As mentioned, the only circumstance in which Minnesota falls below average is among hospitals that can electronically send patient summary of care records to outside providers. On average 85% of hospitals nationwide can electronically send patient summary of care records to outside providers. In Minnesota, 84% of hospital systems can electronically send patient summary of care records to outside providers.

Based on these studies, HIE systems without a hard block CPOE/CDST, PACS, or interoperability, are likely not as effective in reducing duplicate testing as HIE systems using hard blocks or interoperable systems. It is suggested that interoperable systems with decision support will prevent incomplete record transfers that result in lab orders or results not being transferred.

In conclusion, the theory that stringent state laws, like MHRA, are the predominant factor contributing to duplicate testing may not be accurate. Theoretically, given that duplicative testing is a national problem, restrictive state laws, like MHRA, would likely not be a significant contributor to duplicate testing in other states. As a result, it is possible that a predominant factor may be HIE systems, or a state's lack thereof. Without knowing the predominant factors contributing to duplicate testing, it may not be possible to ascertain the impact that MHRA alone has on costs associated with duplicate testing.

Question 3:

According to the federal government, how many entities could have access to a patient's medical record information without their consent?

While it is not known exactly how many entities may have access to a patient's PHI, it is possible to know the types of entities that could potentially have access to a patient's PHI. In general, covered entities and their business associates are permitted to receive PHI. In 2010,

[16] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2995707/

HHS issued a HIPAA regulation that listed more than 700,000 covered entities and 1.5 million business associates.[17] Covered entities include health plans, health care providers, and health care clearinghouses. HHS has developed materials to determine whether an entity is a covered entity under HIPPA. Those materials can be found using this link:

- https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/Downloads/CoveredEntitiesChart20160617.pdf

A covered entity's business associates will also have access to a patient's PHI. A business associate is a "person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information"[18] Business associates can include any entity that provides a covered entity with any of the following services: legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. This includes covered entities that are business associates of another covered entity.

A covered entity is permitted to use and disclose PHI in the following six circumstances:

- To the individual who is subject of the information;
- For treatment, payment, or health care operations;
- After asking the individual's informal permission, allowing the opportunity to agree or object, and receiving permission;
    - Requesting informal permission to include patient's contact information in the health care facility directory, which can be disclosed to anyone asking for the individual by name
        - Directory information would include name, general condition, religious affiliation, and location in the facility.
    - Requesting informal permission to disclose PHI to the individual's family, relatives, friends, or other persons whom the individual identifies.
        - Allows for others to fill prescriptions; the facility to notify those regarding the individuals care, general condition, or death; and for notifying purposes to public or private entities to assist in disaster relief efforts.
- Incident to an otherwise permitted use and disclosure;
- Public interest and benefit activities; and
    - Disclosures are permitted, without an individual's authorization or permission, under 12 circumstances considered "national priority purposes":
        1. Required by Law—covered entities may disclose PHI without authorization when required by law.
        2. Public Health Activities—covered entities may disclose PHI to: (1) public health authorities authorized by law to collect such information for preventing or controlling disease, injury, or disability; and to public health or other government authorities authorized to receive reports of child abuse and neglect; (2) entities subject to FDA regulation regarding FDA regulated products or activities for purposes such as adverse event

[17] http://forhealthfreedom.org/Newsletter/September2010.html#Article3
https://cdn.cnsnews.com/documents/HIPAAPrivacyRegs_EconomicStimulusChanges.pdf
[18] https://www.hhs.gov/sites/default/files/privacysummary.pdf

reporting, tracking of products, product recalls, and post-marketing surveillance; (3) individuals who may have contracted or been exposed to a communicable disease when notification is authorized by law; and (4) employers, regarding employees, when requested by employers, for information concerning a work-related illness or injury or workplace related medical surveillance, when such information is needed by the employer to comply with the OSHA, the Mine Safety and Health Administration, or similar state law

3. Victims on Abuse, Neglect, or Domestic Violence—covered entities may disclose PHI to appropriate government authorities regarding victims of abuse, neglect, or domestic violence
4. Health Oversight Activities—covered entities may disclose PHI to health oversight agencies for purposes of legally authorized health oversight activities, such as audits and investigations
5. Judicial and Administrative Proceedings—covered entities may disclose PHI in a judicial or administrative proceeding if through a court order or by request of an administrative tribunal.
6. Law Enforcement Purposes—covered entities may disclose PHI to law enforcement as: (1) required by law under court orders, warrants, subpoenas, and administrative requests; (2) to identify or locate a suspect, fugitive, material witness, or missing person; (3) to a law enforcement official's request for information about a victim or suspected victim; (4) to alert law enforcement of a person's death if criminal activity is suspected; (5) when PHI is believed to be evidence of a crime that occurred on a covered entity's premise; and (6) when necessary to inform law enforcement about commission and nature of a crime, the location of a crime or crime victims, and the perpetrator of a crime.
7. Decedents—covered entities may disclose PHI to funeral directors, coroners, or medical examiners, for the purpose of identify deceased, determining cause of death, or performing other functions authorized by law.
8. Cadaveric Organ, Eye, or Tissue Donation—covered entities may use or disclose PHI to facilitate the donation and transplantation of cadaveric organs, eyes, and tissues.
9. Research—covered entities may disclose PHI for research purposes, without an individual's authorization, provided they obtain either: (1) documentation that an alteration or waiver of individuals' authorization for the disclosure of their PHI for purpose of research has been approved by the Institutional Review Board or Privacy Board; (2) representations from the researcher that the use or disclosure of PHI is solely to prepare a research protocol or for similar purpose preparatory to research, and that research will not remove PHI from covered entity, and that PHI sought is necessary for the research; or (3) representations from the researcher that the use or disclosure sought is solely for research on the PHI of decedents, that the PHI sought is necessary for the research, and that at the request of the covered entity, documentation of the death of the individuals.

10. Serious Threat to Health or Safety—covered entities may disclose PHI they believe is necessary to prevent or lessen a serious and imminent threat to a person or the public, when such disclose is made to someone they believe can prevent or lessen the threat. This includes disclosing PHI to law enforcement when needed to identify or apprehend an escapee or violent criminal.
11. Essential Government Functions—authorization is not required to disclose PHI for certain essential government functions, including: assuring proper execution of military mission, conducting intelligence and national security activities authorized by law, providing protective services to the President, making medical suitability determinations for U.S. State Department employees, protecting the health and safety of inmates or employees in a correctional institution, and determining eligibility for or conducting enrollment in certain government benefit programs.
12. Workers' Compensation—covered entities may disclose PHI as authorized by, and to comply with, workers' compensation laws and other programs providing benefits for work-related injuries or illnesses.

- Limited data sets for the purpose of research, public health or health care operations.
    - Includes PHI from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed.
    - May be used and disclosed for research, health care operations, and public health purposes, provided the recipient enters into a data use agreement promising specified safeguards for PHI within the limited data set.

Question 4:

Is HIPAA a privacy rule or a disclosure rule?
Under HIPAA, for what kind of sharing is consent required?

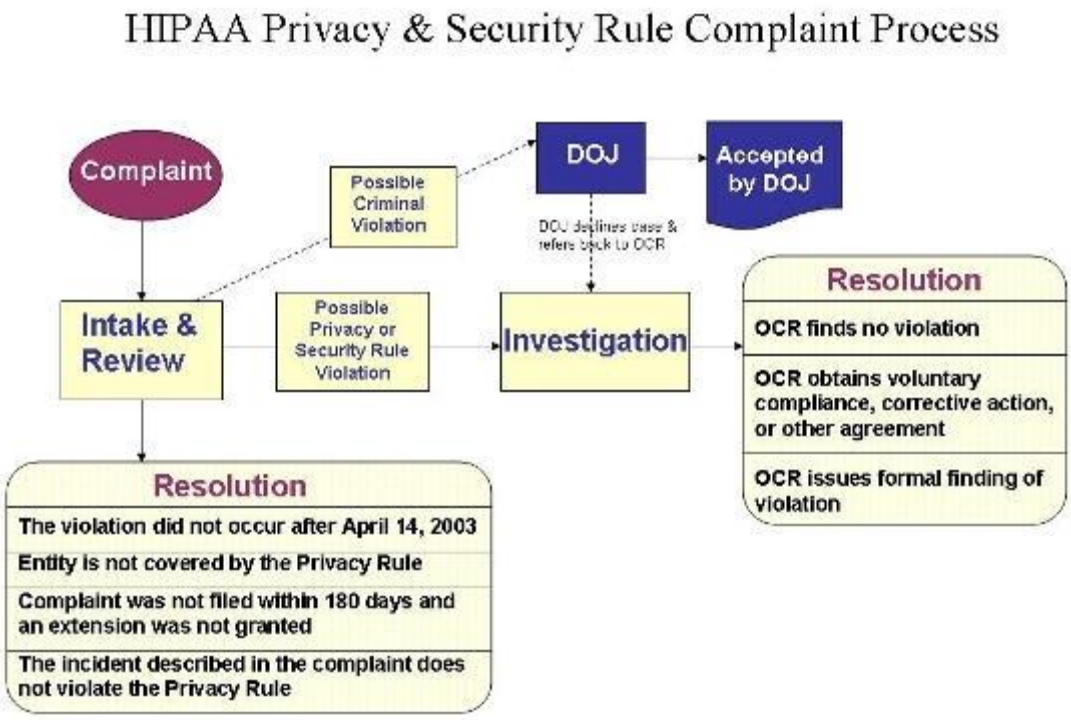
Generally, HIPAA is considered and referred to as a privacy rule. HIPAA's privacy rule allows for disclosure of PHI for the purpose of treatment, payment, or operations. This rule eliminated the need for consent in many instances of disclosure.

Consent or authorization is still required to disclose PHI in some circumstances. Most notably, consent is required if PHI is being disclosed to a person's employer. Additionally, individual authorization is required if PHI is being shared for the purpose of marketing or advertising.

Question 5:

How can penalties and rights for patients be more enhanced/enforced on a state level when there are violations of privacy rather than relying on making a complaint to the Office for Civil Rights?

The U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) is responsible for enforcing HIPAA and investigating complaints filed with OCR. The complaint process is as follows:



[19]

- Any person who believes their rights under HIPAA have been violated may file a complaint with the Secretary of Health and Human Services.[20]
    - Complaints must be in writing and filed within 180 days of when complainant knew or should have known that the act or omission complained of occurred.
        - This time limit may be waived by the Secretary if good cause is shown.
- Following a complaint, a preliminary review occurs.
    - The complaint process ends if the review shows any of the four problems above, listed under "Resolution." For example, if the entity (employer, life insurers, law enforcement agency, etc.) is not covered by the privacy rule, the complaint is rejected.
    - If the review indicates a possible violation, the OCR will conduct an investigation or compliance review to determine if the covered entity or business associate is in compliance.

[19] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html

[20] https://www.worldprivacyforum.org/2013/09/hipaaguide-right-to-complain-to-the-secretary-of-hhs-46-50/

        - OCR may request additional specific information from the covered entity or person filing the complaint.[21]
        - If the complaint describes what may be a violation of criminal provisions of HIPAA, the OCR may refer the complaint to the Department of Justice (DOJ) for investigation.
        - If the OCR review finds that a violation occurred, but that it was not criminal, the OCR will attempt to resolve the complaint in three possible ways:
            - Voluntary compliance;
            - Corrective action; and/or
            - Resolution or agreement.
- If a penalty is enforced as part of the resolution, the OCR will determine the amount of the penalty.
    - Secretary of Health and Human Services may waive civil penalties, except for violations that show a willful neglect.
    - Secretary considers 5 factors in determining amount of civil penalty, these include:
        - Nature and extent of the violation;
        - Nature and extent of the harm resulting from the violation;
        - History of prior compliance with administrative simplification provisions, including violations;
        - Financial condition of the covered entity or business associate; and
        - Such other matters as justice may require.
    - Penalty amounts are awarded based on reason/type of violation and frequency of violations
        - Unknowingly = $100 - $50,000
            - A violation, of an identical provision, in a calendar year is fined $1,500,000
        - Reasonable Cause = $1,000 - $50,000
            - A violation, of an identical provision, in a calendar year is fined $1,500,000
        - Willful Neglect (Corrected) = $10,000 - $50,000
            - A violation of an identical provision, in a calendar year is fined $1,500,000
        - Willful Neglected (Not Corrected) = $50,000
            - A violation of an identical provision, in a calendar year is fined $1,500,000
    - Criminal penalties may be imposed if person knowingly violates the following provisions of HIPAA:
        - Uses or causes to be used a unique health identifier;
        - Obtains individually identifiable health information relating to an individual; or
        - Discloses individually identifiable health information to another person.

[21] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/how-ocr-enforces-the-hipaa-privacy-and-security-rules/index.html

- Criminal penalties include:
  - Fine of no more than $50,000 and/or imprisonment of no more than 1 year;
  - If offense is committed under false pretenses, a fine of no more than $100,000 and/or imprisonment of no more than 5 years; and
  - If offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a fine of no more than $250,000 and/or imprisonment of no more than 10 years or both.

While the complaint process may provide some victims a remedy, it does very little to compensate them for any losses. In the rare circumstances in which a fine is levied against a covered entity, it is collected by the OCR for the purpose of enforcing provisions of HIPAA.[22] A percentage of the penalty is to be distributed to those harmed by the violation. The method and circumstances for distributing penalties to victims was to be determined no later than 18 months after February 17, 2009. However, HHS has not been able to establish the methodology for or circumstances in which a harmed individual would be paid a percentage of the penalty. As a result, those harmed do not receive compensation for any of their time or money lost pursuing the complaint process. For this reason, until a percentage of penalties is paid to those harmed, private causes of action are essential to compensating those harmed.

Under HIPAA, there is no private cause of action that would allow an individual to sue for a violation. As demonstrated, individuals are instead required to file complaints through the OCR. From the patient perspective, this process is flawed, not only because of the lack of a penalty structure, but also because the law permits many disclosures and can protect those who have violated HIPAA. If a patient can overcome the burden of establishing that a violation of HIPAA occurred, there are laws and rules in place that make it nearly impossible to find legal recourse for a HIPAA violation. For example, if neglect of HIPAA laws results in a violation of HIPAA, but the neglect was not willful and was corrected within 30 days, the OCR cannot enforce a civil penalty. As a result, the patient will not receive any redress. Nevertheless, there are a small number of states in which law provides patients a right of action, and enhances penalties for violations of a patient's privacy rights. The following is a list of several states with penalties for violations of patient privacy laws (note: this list is not exhaustive):

- California—Confidentiality of Medical Information Act (CMIA), Chapter 7 Violations
  - § 56.35 In addition to other remedies, a patient whose medical information has been used/disclosure in violation of §§ 56.10, 56.104, 56.20, or 56.26(a), and who has sustained personal injury or economic loss may recover compensatory damages, punitive damages (not to exceed $3,000), attorney's fees (not to exceed $1,000), and cost of litigation.
  - §56.36(a) a violation that results in economic loss or personal injury is punished as a misdemeanor, and may result in monetary damages, as outlined in § 56.36 (b) and (c)

[22] https://www.law.cornell.edu/uscode/text/42/17939#c

- § 56.36 (b) an individual may bring action against a person or entity who has ***negligently*** released confidential information or records of the person, for the following:
  - Nominal damages ($1,000), in which it is not necessary that the plaintiff suffered or was threatened with actual damages; and/or
  - Actual damages
- § 56.36 (c) A person or entity that ***negligently*** discloses medical information shall also be liable, regardless of the amount of damages suffered, for an administrative fine or civil penalty (not to exceed $2,500 per violation).
  - A person or entity, other than a licensed health care professional, who ***knowingly and willfully*** obtains, discloses, or uses medical information shall be liable for an administrative fine or civil penalty (not to exceed $25,000 per violation).
  - A licensed health care professional, who ***knowingly and willfully*** obtains, discloses, or uses medical information shall be liable for:
    - First violation = administrative fine or civil penalty (not to exceed $2,500 per violation).
    - Second violation = administrative fine or civil penalty (not to exceed $10,00 per violation)
    - Third and any subsequent violations = administrative fine or civil penalty (not to exceed $25,000 per violation)
  - A person or entity, other than a licensed health care professional, who knowingly or willfully obtains or uses medical information in violation of this part for the ***purpose of financial gain*** shall be liable for an administrative fine or civil penalty (not to exceed $250,000 per violation) and shall be subject to disgorgement of any proceeds/considerations obtained as a result of the violation.
  - A licensed health care professional who knowingly and willfully obtains, discloses, or uses medical information in violation of this part ***for financial gain*** shall be liable for the following, as well as disgorgement of any proceeds or consideration obtained as a result of the violation:
    - First violation = administrative fine or civil penalty (not to exceed $5,000 per violation)
    - Second violation = administrative fine or civil penalty (not to exceed $25,000 per violation)
    - Third and any subsequent violation = administrative fine or civil penalty (not to exceed $250,000 per violation) and shall also be subject to disgorgement of any proceeds or other consideration obtained as a result of the violation.
  - A person or entity, other than a licensed health care professional, who knowingly or willfully obtains or uses medical information in violation of this part ***for the purpose of financial gain*** shall be liable for an administrative fine or civil penalty (not to exceed $250,000 per violation) and shall also be subject to disgorgement of any proceeds or other consideration obtained as a result of the violation.

        - A person or entity ***who is not permitted to receive medical information*** pursuant to this part and who knowingly and willfully obtains, discloses, or uses medical information without written authorization from the patient shall be liable for a civil penalty (not to exceed $250,000 per violation).
    - The California State Department of Public Health, licensing agency, or certifying board or court determines the amount of an administrative fine or civil penalty by assessing the following:
        - Whether the defendant has made reasonable, good faith attempt to comply with this part;
        - The nature and seriousness of the misconduct;
        - The harm to the patient, enrollee, or subscriber;
        - The number of violations;
        - The persistence of the misconduct;
        - The length of time over which the misconduct occurred;
        - The willfulness of the misconduct; and
        - The defendant's assets, liabilities, and net worth.
    - § 56.36 (e) Defendants are entitled to an affirmative defense, so long as they establish:
        - The defendant is a covered entity or business associate;
        - The defendant has complied with any obligations to notify all persons entitled to receive notice regarding the release of information or records;
        - The release of confidential information or records was solely to another covered entity or business associate;
        - The release of confidential information or records was not an incident of medical identity theft;
        - The defendant took appropriate preventative actions to protect the confidential information or records against release consistent with the defendant's obligations under state law and HIPAA;
        - The defendant took reasonable and appropriate corrective action after the release of confidential information or records, and the covered entity or business associate that received the information or records destroyed or returned the information in the most expedient time possible and without unreasonable delay;
        - The covered entity or business associate that received confidential information or records, or any of its agents, independent contractors, or employees, did not retain, use, or release the information or records;
        - After release of the confidential information or records, the defendant took reasonable and appropriate action to prevent a future similar release of confidential information or records;
        - The defendant has not previously established an affirmative defense, or the court determines that the application of the affirmative defense is compelling and consistent with the purpose of this section to promote reasonable conduct in light of all the facts.
    - Civil penalties shall be assessed and recovered in a civil action brought in the name of the people of California in any court of competent jurisdiction by any of the following: Attorney General, District Attorney (DA), county counsel

authorized by DA, city attorney, city attorney in a city of 750,000 or more with the consent of the DA, city prosecutor with consent of the DA.
    - The State Public Health Officer or his/her designees may recommend that one of the above mentioned people bring a civil action.
- Delaware—like many states, Delaware does not have laws concerning the wrongful disclosure of a patient's medical records or information. Instead, patients harmed by a wrongful disclosure would need to bring their own lawsuit. Whether a plaintiff can bring a lawsuit will depend on the facts of the case, state laws, and case law. For example, there are some states that do not acknowledge the tort of invasion of privacy based on unreasonable public disclosure of private fact.[23] Absent state law prohibiting such legal action, there are some possible legal claims available, which will depend on case facts and often the statute of limitations. These claims may include, but are not limited to:
    - Tort of invasion of privacy;
        - Unreasonable public disclosure of private facts
        - Intrusion upon physical solitude or seclusion
        - Wrongful appropriation of a person's name or likeness
        - Publicity that unreasonably places a person in a false light before the public
    - Medical malpractice, breach of confidential relationship, or breach of (implied) contract;
    - Defamation;
        - Slander—spoken defamation
        - Libel—printed defamation
    - Negligence; or
    - Intentional Infliction of Emotional Distress.
- Florida—there is also no law in Florida that provides the ability to sue for a violation of HIPAA or related state laws. In addition to filing one of the above described lawsuits, under §456.057, Florida does allow for violators to be disciplined.
    - under § 456.057 paragraph 7(a), records may not be furnished to any person other than the patient, their legal representative, or other health care practitioners/providers involved in the patient's care or treatment, unless the patient provides written authorization.
    - § 456.057 paragraph 15, a violation of this will result in discipline by the "appropriate licensing authority".
    - § 456.057 paragraph 16, The Attorney General is authorized to enforce this provision, through injunctive relief and fines, which cannot exceed $5,000 per violation.
- New Hampshire—Under RSA 332-1:6, New Hampshire allows for civil action under RSA 332-1:4 (marketing and fundraising disclosures) or 332-1:5 (unauthorized disclosures).
    - This statute stipulates that damages (special or general) will be awarded to successful complainants, and that damage awards shall be no less than $1,000 for each violation + cost + reasonable legal fees.[24] However, it appears that this

[23] https://pdfs.semanticscholar.org/8fd4/d7ff560a3d9ef03ca4a622d470837b5d4374.pdf
[24] https://law.justia.com/codes/new-hampshire/2017/title-xxx/chapter-332-i/section-332-i-6/

action is limited to only violations of disclosures for the purpose of marketing and fundraising.

- Rhode Island—Confidentiality of Health Care Communications and Information Act,
    - RI Gen L § 5-37.3-4 states that any person who violates the *section* may be liable for actual and punitive damages, and that the court may award a reasonable attorney's fee to the prevailing party.
        - Knowing and intentional violations can result in fines up to $5,000 and/or imprisonment of up to 6 months, for each violation.
    - RI Gen L § 5-37.3-9 outlines civil penalties for violating the Act, which includes actual and exemplary damages.
        - Applicable to anyone who obtains confidential health care information through the commission of a crime.
    - Under § 5-37.3-9, Rhode Island law states that criminal penalties for an intentional and knowing violation of this *chapter* include a fine of no more than $1,000 and/or imprisoned up to 6 months.
    - Both civil and criminal penalties are application to anyone who obtains confidential health care information through the commission of a crime.
    - Attorney's Fees may be awarded, at the discretion of the court, to any successful party in any action under this Act.
- Tennessee—§ 68-11-1504 of Tennessee Code states that penalties and injunctions are available under the Patient Privacy Protection Act, but does not state what the penalties include. This section also states that civil actions for damages for invasion of privacy is also available to persons for violations of the Act.
- Washington—although Washington code mimics HIPPA, § 70.02.170 allows for civil remedies should a person violate that chapter of Washington code.
    - The civil remedies include:
        - Court may order the health care provider or person to comply with the chapter.
        - Relief may include actual damages, but cannot include consequential or incidental damages.
        - Court shall award reasonable attorneys' fees and all other expenses reasonably incurred to the prevailing party.
    - Actions must be commenced within 2 years after the cause of action is discovered.

As demonstrated, although several states have laws that provide a means for legal remedy when a patient's privacy rights have been violated, many do not. As a result, patients who have had their privacy compromised or violated have limited options when seeking redress. In order to be compensated a patient must often file a lawsuit alleging negligence, defamation, intentional infliction of emotional distress, etc. Although permitting a private lawsuit may provide better results than a HIPAA complaint, it places a great burden on the victims who have had their private health information wrongfully disclosed or shared.

First, in order to pursue a lawsuit, victims must know whether their privacy has been violated. This will require either a whistleblower reporting improper disclosures to HHS, requesting a

patient's entire medical history, and, or requesting an accounting of disclosures.[25] Unless a whistleblower reports improper disclosures, determining whether an improper disclosure has occurred depends entirely on the patient performing requests, including record requests and, or requests for an accounting of disclosures. Requesting medical records is often more complex and expensive than patients imagine, as records can be hundreds or thousands of pages with medical information that patients do not understand. An accounting of disclosures will be more helpful in determining how, when, and to whom have records been disclosed. This process may be less burdensome, as the first copy requested in a 12-month period is free. However, the accounting record may not be received for two to three months, because providers are granted 60 to 90 days to fulfill any accounting requests.

Second, patients are burdened by the requirement that they establish the necessary elements of their claim, and that they do so within the statute of limitations. These elements will vary based on the claims made by patients. For example, in a state that permits action under a public disclosure of private fact claim, a patient must establish four things:

- the disclosed fact was private;
- there was a public disclosure of the private fact;
- the public disclosure of private facts is offensive to a reasonable person; and
- that the fact is not a matter of legitimate public concern.

Although these four elements seem relatively easy to demonstrate, there are two important considerations. First, under this claim a simple wrongful disclosure is not sufficient. It requires that someone publish or make public the patient's private health information. Second, the statute of limitations for a public disclosure of private fact claim is often only one to three years. Given the length of time it takes to learn and determine that there has been a wrongful disclosure, this statute of limitations may be incredibly rigid and difficult to satisfy.

Lastly, patients must establish and prove damages. This requires a patient to establish the harm or effect the wrongful disclosure had upon them. For example, if a public disclosure of private fact resulted in a loss of business, the patient may allege damages equivalent to the amount of business lost. There are several other means of establishing damages, but whether a patient's alleged damages are compensable will vary from state to state.

Even in the circumstances in which a patient overcomes the above-mentioned hurdles, and does obtain a favorable outcome, these lawsuits do very little to remedy the wrongful disclosure. For example, unlike the OCR complaint process, a lawsuit does not track those with repeat violations. Additionally, a lawsuit cannot repair the harm done to a patient's privacy. Instead, lawsuits provide patients, those with the necessary resources and time, financial compensation. That said, a private action under state law will also do very little to remedy a wrongful disclosure, and will also place some burdens on the harmed patient. For example, patients pursuing an action under § 144.298 must still make the effort to determine whether there has been a wrongful disclosure, and must also establish damages. Whereas through the OCR complaint process, the OCR determines penalties based on the number and severity of violations.

[25] https://www.worldprivacyforum.org/2013/09/hipaaguidepart2/

Question 6:

Does HIPAA require an accounting of disclosures for every disclosure of their information, including for research, payment, treatment, health care operations, and the 12 national priority purposes?

HIPAA, in some circumstances, does require an accounting of disclosures of protected health information (PHI) made by a covered entity. In those circumstances, when an individual requests an accounting of disclosures, the covered entity must provide an accounting of the last six years prior to the date of the request. However, a covered entity does not need to account for the following disclosures:

- Disclosures for the purpose of treatment, payment, and health care operations;
- Disclosures made to the individual subject of the PHI;
- Disclosures incident to a use or disclosure that is otherwise permitted or required by this subpart (subpart E);
    - This includes incidents where a covered entity discloses a limited data set to a public health authority, according to their data use agreement.[26]
- Disclosures pursuant to authorization as provided in §164.508 (psychotherapy notes, marketing, sales);
- Disclosures for the facility's director or to persons involved in the individual's care or for other notification purposes;
- Disclosures for national security or intelligence purposes;
- Disclosures to correctional institutions or law enforcement officials;
- Disclosures that occurred prior to the compliance date for the covered entity;[27]
- Disclosures in the form of a limited data set.[28]

The above listed exceptions to the accounting requirement leave few instances in which an accounting of disclosures is required. The accounting of disclosures requirement does require the following three disclosures to be included in accounting:

- General disclosures of PHI as required by or authorized by law, or made in response to court orders, subpoenas, etc.;
- General disclosures of PHI as required for a proceeding before a health oversight agency pursuant to § 164.512(d); and
- Disclosures of PHI for the purpose of research, if the research was or will be obtained or disclosed without an individual's authorization.[29]

Under HIPAA § 164.528 (a)(4), a disclosure of PHI within the last six years, for the purpose of research for 50 or more individuals, must be included in an accounting of disclosures. Accounting of disclosures for the purpose of research must include the following:

---

[26] https://www.hhs.gov/hipaa/for-professionals/faq/467/must-a-covered-entity-provide-an-accounting-for-disclosures/index.html
https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-528.xml

[27] https://www.law.cornell.edu/cfr/text/45/164.528

[28] https://www.hopkinsmedicine.org/institutional_review_board/hipaa_research/tracking.html

[29] https://www.hopkinsmedicine.org/institutional_review_board/hipaa_research/tracking.html

- The name of the protocol or research activity;
- A plain language description of the research activity, the purpose of the research, and the criteria for selecting records;
- A brief description of the type of PHI that was disclosed;
- The data or period of time during which disclosures occurred, or may have occurred;
- The name, address, and telephone number of the entity that sponsored the research, and the name, address, and telephone number of the researcher to whom the information was disclosed; and
- A statement that the PHI of the individual may or may not have been disclosed for a particular protocol or other research activity.[30]

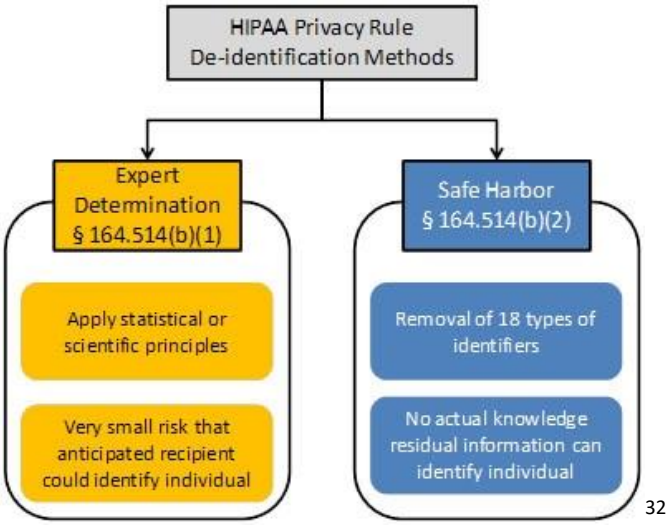
It should be noted that MHRA does require an accounting of disclosures for all disclosures made without a patient's consent. Under § 144.293, subdivision 9, in circumstances in which a provider "releases health records without patient consent as authorized by law, the release must be documented in the patient's health record."[31] Therefore, hypothetically, under MHRA, if a disclosure is made absent patient consent, for the purpose of treatment, payment, or health care operations, there must be an accounting of that disclosure.

Question 7:

If the data is de-identified under HIPAA is it still considered protected health information (PHI) and subject to the federal HIPAA rule?
Are patients informed when their PHI is de-identified?

According to the U.S. Department of Health and Human Services, de-identified data is no longer considered protected health information (PHI). There does not appear to be any requirement to inform a patient when their PHI is de-identified, as it is no longer considered PHI. Data can be de-identified in two ways, either by a formal determination by a qualified expert, or the removal of specified individual identifiers.

[30] https://www.law.cornell.edu/cfr/text/45/164.528
[31] https://www.revisor.mn.gov/statutes/cite/144.293



The expert method for de-identification requires that experts use a series of principles to determine if the information is identifiable. These principles include replicability, data source availability, distinguishability, and assess risk.[33] Under the safe harbor standard, the covered entity must remove 18 identifiers, and must not have knowledge that the information could be used alone or in combination with other information to identify the individual. Therefore, although de-identified information retains a small risk of identification, especially when combined with other information, it is considered de-identified so long as the covered entity does not know how the information may be used to identify the individual.[34]

Question 8:

If Minnesota reverts to the "HIPAA data-sharing standard" how will patients be informed that they no longer have the privacy rights and consent requirements?

Currently, § 144.292, subdivision 4, of the MHRA requires providers to give patients notice concerning practices and rights with respect to access to health records. This notice may be displayed in the provider's office or a copy may be given to a new patient. The notice must include an explanation of disclosures that the provider may make without the written consent of the patient. In addition, the statute requires the commissioner of health to develop the notice. The current notice can be found here, http://www.health.state.mn.us/divs/hpsc/dap/notice.pdf.

Current law does not require existing patients to be notified whenever the legislature amends the Minnesota Health Records Act. Unless the new law requires an additional patient notification, the current provisions of § 144.292, subdivision 4, will apply. A provider may, however, choose

[32] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html
[33] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#rationale
[34] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#rationale

to notify existing patients regarding the change, but this would be determined by the individual provider.

Question 9:

What do hospitals, clinics, physicians, and providers currently do when a patient does not give consent for sharing of personal health information for treatment, payment, and operations?

Without consent, or an applicable exception to the consent requirement, the provider is prohibited from sharing records. A health care provider or covered entity, subject to state law and HIPAA, must follow the law that is most restrictive when handling PHI. However, if there is no state law, or the state law is the same or less restrictive than HIPAA, the covered entity must default to HIPAA's standard for disclosure. If the covered entity does default to HIPAA, the covered entity may disclose PHI for the purpose of treatment, payment, and health care operations.

If a state law, like MHRA, is more restrictive than HIPAA, and does not have exceptions for treatment, payment, and health care operations, then the covered entity may not disclose PHI for these purposes.

Question 10:

How many hospital and clinic consent forms include consent for data-sharing on the same form as the consent for treatment? Is there one signature or separate signatures?

There is no information, readily available, that determines how many health care providers have forms that include consent for data sharing, or how many signatures are obtained in the process of gaining consent. This would require a study of the policies and procedures of every hospital, clinic, etc. However, a 2017 Report to the Minnesota Legislature, by the Minnesota Department of Health (MDH), shed some light on the process for obtaining patient consent, but does not directly address consent for data sharing. The Report is based on a set of questions concerning MHRA, which were distributed to advisory committees, health associations, and key advocacy groups. MDH received 86 responses to their set of questions, and analyzed 81 of those responses. Of the 81 responses analyzed, 57 responses were from the provider perspective. The other responses were either from the patient perspective, or a combination of the patient and provider prospective.

The Report found it was common for the process of obtaining consent to vary widely across health care providers. This was determined or based on responses from health care providers across Minnesota, and suggested that the variation of consent processes could be due to providers varying in size, location, organization type, and operational practices of health care entities.[35] The following are the Report's findings that are most pertinent to this question:

- 67% of respondents described that consent must be obtained via a signed writing.

[35] http://www.health.state.mn.us/e-health/legrpt/docs/rfi-health-record-act2017.pdf

- Providers typically obtain consent during registration or upon a patient's first visit.
- Some providers, presumably not a majority, reported that they have to scan consent into an electronic health record (EHR) system.
- 26% of respondents reported using a process that requires printing, mailing, or faxing paper forms.
- 12% of respondents used an e-consent process, where a consent form is signed and sent via e-mail or contains an electronic signature.

Question 11:

Who were the "national organizations" contacted for the Care Coordination Measures Atlas (and the updated Atlas) and what information did they provide?
Did any Minnesota providers or companies participate/provide info toward development of the Atlas?

The Care Coordination Measures Atlas was prepared by the Agency for Healthcare Research and Quality (AHRQ). The Atlas can be found here:

- https://www.ahrq.gov/professionals/prevention-chronic-care/improve/coordination/atlas2014/jumpstart-guide.html

It is described as an "investigation into care coordination definitions, practices, and interventions" that is sponsored by several national organizations. AHRQ only identifies three organizations as sponsors of the atlas, but states that there are additional sponsors. The three organizations expressly identified as sponsors are:

- AHRQ;
- the Institute of Medicine; and
- the American College of Physicians.

There are several other organizations included in the footnote citations. These organizations did not necessarily sponsor the Atlas. The cited organizations include, but are not limited to:

- The National Quality Forum;
- The Commonwealth Fund;
- Oxford's Journal of the National Cancer Institute;
- Mathematica Policy Research Inc.;
- Office of the National Coordinator for Health Information Technology;
- American Medical Association; and
- Centers for Medicare and Medicaid Services.