

Wisconsin Security and Privacy Project

Legal Analysis Summaries

Scenarios 1-18

Table of Contents

Scenario 1 – Patient Care Scenario A 2
Scenario 2 – Patient Care Scenario B 4
Scenario 3 – Patient Care Scenario C 6
Scenario 4 – Patient Care Scenario D 8
Scenario 5 - Payment 9
Scenario 6 - RHIO 10
Scenario 7 – Research 10
Scenario 8 – Law Enforcement 11
Scenario 9 – Pharmacy Benefit Scenario A 13
Scenario 10 – Pharmacy Benefit Scenario B 14
Scenario 11 - Health care Operations and Marketing - Scenario A 15
Scenario 12 - Health care Operations and Marketing - Scenario B 17
Scenario 13 - Bioterrorism event 19
Scenario 14 – Employee Health 21
Scenario 15 - Public Health - Scenario A - Active carrier, communicable disease notification 22
Scenario 16 – Public Health - Scenario B -Newborn screening 24
Scenario 17 – Public Health Scenario C- Homeless shelters 26
Scenario 18 - Health Oversight: Legal compliance/government accountability 28

Scenario 1 – Patient Care Scenario A

Patient X presents to emergency room of General Hospital in State A. She has been in a serious car accident. The patient is an 89-year-old widow who appears very confused. Law enforcement personnel in the emergency room investigating the accident indicate that the patient was driving. There are questions concerning her possible impairment due to medications. Her adult daughter informed the ER staff that her mother has recently undergone treatment at a hospital in a neighboring state and has a prescription for an antipsychotic drug. The emergency room physician determines there is a need to obtain information about Patient X's prior diagnosis and treatment during the previous inpatient stay.

Legal Analysis

The legal analysis in this scenario requires a determination of which state and federal privacy laws apply to the inpatient information requested. If the information requested is general health care information Wisconsin Statute 146.81-146.84 and the HIPAA Privacy Rule will apply. If the information requested fits the legal protection afforded mental health, alcohol and drug abuse and developmentally disabled patient information then Wisconsin Statute 51.30, the HIPAA Privacy Rule and 42 CFR Part 2 may apply.

A written authorization is not required under state or federal law¹ to exchange patient information between providers for treatment purposes unless the inpatient information includes specifically protected information such as for mental illness.² The Federal Privacy Rule, 45 CFR §164.502(a) (1) (ii) and §164.506(c) (2), authorizes the use and disclosure of protected health information for treatment without the written or oral consent of the patient. There are two Wisconsin laws that are relevant to this scenario. Wis. Stats. 146.81-146.84³ and 51.30.⁴ Wisconsin Statutes 146.81-146.82 govern general health care information and contain an exception that allows for release of patient care information from provider to provider for patient treatment without patient consent. This state law is consistent with the Federal Privacy Rule, which also does not require patient consent for disclosure from provider to provider for treatment, and consent would not be required.⁵ If the inpatient information requested is general health care information under s 146.81 then patient consent would not be required.

If the information requested relating to the anti-psychotic drug is from a Wisconsin hospital, is “sensitive” under Wisconsin law (e.g., relating to mental illness, developmental disabilities, alcohol and drug abuse) and is protected under s.51.30, a specific, written patient consent is required to authorize the health information exchange.⁶ If the request originates in Wisconsin and is directed to an out-of-state facility, then the law of the state in which the information is contained would apply. State

¹ Wisconsin Statute 146.82(2)(a)2; 45 CFR §§164.502(a)(1)(ii) and 164.506(c)(2),

² Wisconsin Statute 51.30(4)(b)8 and 8g

³ Wisconsin Statutes 146.81 – 146.84

⁴ Wisconsin Statute 51.30

⁵ 45 CFR 164.506(c)(2)

⁶ Wis. Stat. 51.30

laws regulating the disclosure of “sensitive” patient information may differ and it may be difficult to determine whether patient consent is required.

If Wisconsin Statute 51.30 applies in this scenario and the HIPAA Privacy Rule also applies, Wisconsin law is more stringent and more protective by requiring patient consent for disclosure and Wisconsin law would preempt the federal Privacy Rule. While HIPAA would normally preempt a contrary state law, 45 CFR §160.203(b), provides an exception for state laws that are more stringent than HIPAA. Consequently, Wisconsin law regulating mental health records would be controlling in this scenario if the information requested contains mental health, alcohol and drug abuse or developmental disability information, and consent would be required. If consent is required there are very specific requirements that must be included in the consent form for it to be deemed legal.⁷

The federal Privacy Rule applies a minimum necessary standard to the amount of information disclosed. However this law does not require that the standard be applied when the exchange is for treatment. However s.51.30 and HFS 92.03(1)(n) also contain a minimum necessary standard that does apply to an exchange for treatment. So, if s.51.30 applies, the more stringent state law would again preempt HIPAA and the minimum necessary law would apply.

Legal Barriers

Federal law requires that the identity of the requestor be verified.⁸ State law does not have a specific provision requiring verification of the requestor. In this scenario, most of the stakeholders would have verified the identity of the requestor. This requirement for a verification process presents a barrier to health information exchange.

Although HIPAA would not require documentation of disclosures for treatment⁹ as depicted in this scenario, Wisconsin Statute 146.82(2)(d) requires documentation of disclosures made by a health care provider when made without the consent of the patient. Wisconsin Statute 51.30, if applicable, also requires documentation of disclosures for treatment. This documentation requirement presents barriers to health information exchange by requiring specific documentation of a disclosure every time a designated disclosure occurs. Although this requirement may be met by audit and monitoring techniques in an electronic exchange, the electronic system will be required to document the statutorily required elements.

Additional barriers to health information exchange identified in this scenario relate to security of information transfer and transmission. If the HIPAA Security Rule applies to any of the disclosers of information in this scenario the following requirements would need to be met and will present barriers to the exchange of information.

- Method of exchange and security measures for protection of exchange¹⁰
- Requirements for receipt of the information¹¹

⁷ Wisconsin Statute 51.30 (2)

⁸ 45 CFR 164.312(d); 45 Cfr 164.514(h)

⁹ 45 CFR 164.528(a)(1)(i)

¹⁰ Security and Privacy Rules

¹¹ Wis. Stat.146.82; 45 CFR 164.501 Definition of designated record set

In addition, HIPAA allows a patient to request that restrictions be imposed on the information exchanged and the provider must review and respond to that request.¹² This right of restriction may cause additional barriers to information exchange. This scenario contemplated an exchange of information between providers in two different states. Accordingly, the legal analysis above could be different depending on the law of the unnamed state; and variability in state laws may present a barrier to health information exchange.

Scenario 2 – Patient Care Scenario B

An inpatient specialty substance abuse treatment facility intends to refer client X to a primary care facility for a suspected medical problem. The two organizations do not have a previous relationship. The client has a long history of using various drugs and alcohol that is relevant for medical diagnosis. The primary care provider has requested that the substance abuse information be sent by the treatment facility. The primary care provider intends to refer the patient to a specialist and plans to send all of the patient's medical information, including the substance abuse information that was received from the substance abuse treatment facility, to the specialist.

Legal Analysis

The federal Privacy Rule allows disclosure of patient information from provider to provider for treatment purposes without patient consent; however, Wisconsin privacy law and the federal law regulating alcohol and drug treatment records impose more stringent standards for sensitive patient information such as mental health, alcohol and drug abuse and developmental disability and requires consent from the patient.¹³

The federal Privacy Rule requirement that requires scrutiny of the amount of patient information disclosed does not require application of the minimum necessary standard for records released for treatment, but Wisconsin law¹⁴ does apply this standard for more sensitive patient information (alcohol and drug abuse).

The federal Privacy Rule does not require that disclosures for treatment be documented, but again a more stringent standard is required under Wisconsin law and documentation is required.¹⁵

Legal Barriers

In Wisconsin statutes dating from 1977 regulate and stringently protect patient information relating to mental health, alcohol and drug abuse and developmental disability. Wisconsin law and the federal law regulating alcohol and drug abuse patient information require patient consent authorizing information exchange between providers for treatment purposes.¹⁶ The federal Privacy Rule allows disclosure without patient consent and this divergence in state and federal laws requires interface between state

¹² 45 CFR 164.532(a)

¹³ 42 CFR Part 2; s.51.30

¹⁴ HFS 92.03(1)(n)

¹⁵ s.51.30(4)(e)

¹⁶ Wis. Stat. 51.30(2); 42 CFR 2.1

and federal law that is specifically addressed under HIPAA.¹⁷ The resolution, by federal law, is to apply the law (state or federal) that provides the most protection to the patient information. In this scenario, HIPAA would require application of the more stringent requirements under state and federal law and consent from the patient would be required for disclosure of the substance abuse facility information to the primary care provider.

In addition, state¹⁸ and federal¹⁹ law allow for re-disclosure with patient consent. The same analysis applied above would control the re-disclosure of the substance abuse facility information to the specialist, and re-disclosure would require patient consent.

Any time consent is required to exchange information, it creates a barrier to exchange. The process to share information requires a determination of whether consent is required and the analysis presents a barrier to health information exchange. The process to obtain consent poses an additional barrier to exchange because it requires contact with the patient or other legally authorized person to obtain the consent. Additional barriers include determining who is legally authorized to sign the consent and validating the statutorily required elements of the consent.

The federal Privacy and Security Rules require that the identity of a requester for protected health information be verified to determine that the individual is who they claim to be. In this scenario, verification of the primary care provider requesting the patient information would be required. This requirement presents a barrier to health information exchange.

Although HIPAA would not require documentation of disclosures for treatment²⁰ Wisconsin Statutes 146.82(2)(d) and 51.30 require documentation of disclosures made by a health care provider. This documentation requirement presents barriers to health information exchange by requiring specific documentation of a disclosure every time a designated disclosure occurs. Although this requirement may be met by audit and monitoring techniques in an electronic exchange, the electronic system will be required to document the statutorily required elements.

The federal Privacy Rule requirement that requires scrutiny of the amount of patient information disclosed does not require application of the minimum necessary standard for information released for treatment, but Wisconsin law does apply this standard in this scenario for more sensitive patient information.²¹

Additional barriers to health information exchange identified in this scenario relate to security of information transfer and transmission. If the HIPAA Security Rule applies to any of the disclosers of information in this scenario the following requirements would need to be met and will present barriers to the exchange of information.

- Method of exchange and security measures for protection of exchange²²
- Requirements for receipt of the information²³

¹⁷ 45 CFR §160.203(b)

¹⁸ HFS 92.03(1)(h)

¹⁹ 42 CFR 2.31

²⁰ 45 CFR 164.528(a)(1)(i)

²¹ HFS 92.03(1)(n)

²² Security and Privacy Rules

Scenario 3 – Patient Care Scenario C

At 5:30 pm Dr. X, a psychiatrist, arrives at the skilled nursing facility to evaluate his patient, recently discharged from the hospital psychiatric unit to the skilled nursing facility. The hospital and skilled nursing facility are separate entities and do not share electronic record systems. At the time of the patient's transfer, the discharge summary and other pertinent records and forms were electronically transmitted to the skilled nursing home.

When Dr. X enters the facility, he seeks assistance locating his patient, gaining entrance to the locked psychiatric unit, and accessing the patient's electronic health record to review the discharge summary, I&O, MAR and progress notes. Dr. X was able to enter the unit by showing a picture identification badge, but was not able to access the EHR. As it is Dr. X's first visit, he has no login or password to use their system.

Dr. X completes his visit and prepares to complete his documentation for the nursing home. Unable to access the skilled nursing facility EHR, Dr. X dictates his initial assessment via telephone to his outsourced, offshore transcription service. The assessment is transcribed and posted to a secure web portal.

The next morning, from his home computer, Dr. X checks his e-mail and receives notification that the assessment is available. Dr. X logs into his office web portal, reviews the assessment, and applies his electronic signature.

Later that day, Dr X's Office Manager downloads this assessment from the web portal, saves the document in the patient's record in his office and forwards the now encrypted document to the long-term care facility via e-mail.

The skilled nursing facility notifies Dr. X's office that they are unable to open the encrypted document because they do not have the encryption key.

Legal Analysis

In this scenario there are several exchanges of information between providers and individuals contracting to provide services to providers. The Legal Workgroup stakeholders clearly identified that if the information exchange was between providers for treatment and related to general health information, no consent would be required for disclosure under state and federal law.²⁴ If, however, the exchange contained information relating to mental illness, substance abuse or developmental disability as in the exchange between the psychiatric inpatient hospital and the skilled nursing facility, a patient consent for exchange would be required by Wisconsin law and possibly the federal law regulating alcohol and drug abuse records.²⁵ In addition, Wisconsin law requires that patient information be sent with the patient when transferring from an inpatient facility to a nursing home facility.²⁶ So the patient records would be required to be sent to the nursing home facility with patient consent.

²³ Wis. Stat. 51.30; 45 CFR 164.501 Definition of designated record set

²⁴ Wis. Stat. 146.82(2) (a) 2. a and b; 45 CFR 164.506(c)(2);

²⁵ Wis. Stat. 51.30(2); 42 CFR 2.1

²⁶ HFS 132, Nursing Home Records

All stakeholders agreed patient information could be shared between the physician and his transcription company without patient consent but that some type of contractual relationship such as employment or a business associate agreement would be required to allow this exchange.

The stakeholders generally agreed that they would not require patient consent for disclosure of the physician's transcription to the nursing home as this appears to be a provider-to-provider information exchange of non-sensitive information for treatment and there appears to be a relationship between the physician and the nursing home. If the physician's dictation is regulated by 51.30, contains sensitive health care information, consent would be required to share between non-related entity providers.²⁷

Legal Barriers

Consent

In this scenario if the information exchanged was mental health, alcohol or drug abuse or developmentally disabled information, the exchange between providers for treatment purposes would require a patient consent.²⁸ This would include the exchange between the hospital inpatient psychiatric unit and the nursing home and the nursing home and the psychiatrist.²⁹

For information to be exchanged between a physician and a transcription employee or company, the federal Privacy Rule would require some type of contractual relationship such as employment or a business associate agreement. The Federal Privacy Rule requires that the agreement between the physician and the transcription company be in writing and meet specific requirements before exchange can occur.³⁰ Wisconsin law does not control this exchange as it is considered a use, not a disclosure. In this case, federal law is more stringent than state law and presents a barrier to health information exchange.

Minimum Necessary

The federal Privacy Rule requirement that requires scrutiny of the amount of patient information disclosed does not require application of the minimum necessary standard for information released for treatment, but Wisconsin law does apply this standard in this scenario for more sensitive patient information.

If information is transferred electronically, there is no controlling Wisconsin law relating to transmission security but the Federal Security Rule when applicable would require that the transmission be secure.³¹ Wisconsin law also requires that disclosure of the patient health record from the inpatient psychiatric unit be documented.³² Both the requirement of a secured transmission and documentation of the disclosure present barriers to information exchange.

²⁷ Wis. Stat. 51.30 (2)

²⁸ Wis. Stat. 51.30(2); 42 CFR 2.1

²⁹ Wis. Stat. 51.30 (2)

³⁰ 45 CFR 164.502(e)(1)

³¹ 45 CFR 164 Subpart C

³² Wis. Stat. 51.30(4)(e)

Scenario 4 – Patient Care Scenario D

Patient X is HIV positive and is having a complete physical and an outpatient mammogram done in the Women's Imaging Center of General Hospital in State A. She had her last physical and mammogram in an outpatient clinic in a neighboring state. Her physician in State A is requesting a copy of her complete records and the radiologist at General Hospital would like to review the digital images of the mammogram performed at the outpatient clinic in State B for comparison purposes. She also is having a test for the BrCa gene and is requesting the genetic test results of her deceased aunt who had a history of breast cancer.

Legal Analysis

Patient consent is not required to disclose a patient's record, containing an HIV test result, from provider to provider for treatment under either state or federal law.³³ Therefore, the information exchange between the patient's providers would not require patient consent. The federal Privacy Rule would also not require that this disclosure for treatment purposes or the disclosure authorized by consent to the niece be documented or that the minimum necessary standard apply.

Legal Barriers

The Legal Workgroup agreed, consistent with state and federal law, that the disclosure of the aunt's genetic information from a provider to the niece would require a valid patient consent. There is no applicable state or federal exception that would allow this disclosure without patient consent; therefore consent would be required. The process of obtaining a valid patient consent with the appropriate legally authorized signature for a deceased patient's information was identified as a barrier to health information exchange.³⁴

Wisconsin law would require that the disclosure between providers and the disclosure to the niece be documented under Wis. Stat. 146.82(2)(d) and maintained as a part of the patient's health care record. The stringency of the documentation requirement presents a barrier to health information exchange.

Additional barriers to health information exchange identified in this scenario relate to security of information transfer and transmission. If the HIPAA Security Rule applies to any of the disclosers of information in this scenario the following requirements would need to be met and will present barriers to the exchange of information.

- Method of exchange and security measures for protection of exchange³⁵
- Requirements for receipt of the information³⁶

³³ Wis. Stat. 252.15(5)(2); Wis. Stat. 146.82(2)(a)2.; 45 CFR §§164.502(a)(1)(ii) and 164.506(c)(2),

³⁴ Wis. Stat. 146.81(2) and (5); 45 CFR 165.508

³⁵ Security and Privacy Rules

³⁶ Wis. Stat.146.82 and 252.15 ; 45 CFR 164.501 Definition of designated record set

Scenario 5 - Payment

X Health Payer (third party, disability insurance, employee assistance programs) provides health insurance coverage to many subscribers in the region the health care provider serves. As part of the insurance coverage, it is necessary for the health plan case managers to approve/authorize all inpatient encounters. This requires access to the patient health information (e.g., emergency department records, clinic notes, etc.).

The health care provider has recently implemented an electronic health record (EHR) system. All patient information is now maintained in the EHR and is accessible to users who have been granted access through an approval process. Access to the EHR has been restricted to the health care provider's workforce members and medical staff members and their office staff.

X Health Payer is requesting access to the EHR for their accredited case management staff to approve/authorize inpatient encounters.

Legal Analysis

According to state and federal law, consent would not be necessary to release limited information related to the inpatient service that needed to be pre-authorized for payment purposes.³⁷ None of the stakeholders were comfortable with the concept of allowing the payer unlimited access to patient information. If the payer requested full access to the EHR, including patient information not necessary to determine payment, patient consent is required. If the payer requested information related to an HIV test result, mental health, alcohol and drug abuse, or developmental disability, consent would be required.³⁸

Legal Barriers

Verification of the payer making the request for the pre-authorization information would be required by federal law.³⁹ This requirement presents a barrier to health information exchange.

Documentation of the disclosure for payment purposes, although not required by federal law, would be required by state law.⁴⁰ This documentation requirement presents barriers to health information exchange by requiring specific documentation of a disclosure every time a designated disclosure occurs. Although this requirement may be met by audit and monitoring techniques in an electronic exchange, the electronic system will be required to document the statutorily required elements.

Although there is no applicable state limitation, federal law requires that the information disclosed for payment purposes be limited to that which is minimally necessary to be able to make payment for the service provided.⁴¹ The application of this standard presents a significant barrier to health information exchange.

³⁷ Wis. Stat. 146.82(2)(a)3; 45 CFR §§164.502(a)(1)(ii) and 164.506(c)(3)

³⁸ Wis. Stat. 252.15; Wis. Stat. 51.30; 45CFR 164.512

³⁹ 45 CFR 164.514(h)

⁴⁰ Wis. Stats. 146.82(2)(d); 51.30(4)(e)

⁴¹ 45 CFR 164.502(b)(1)

An additional barrier to health information exchange identified in this scenario relates to security of information transfer and transmission. The HIPAA Security Rule applies to the electronic exchange of health care information and would require that the exchange in this scenario meet the Security Rule requirements for a secured transmission, which will present a barrier to the exchange of information.

Scenario 6 - RHIO

Critical Observations

Wisconsin has a number of health information exchanges in the early stages of formation. Currently only the Wisconsin Health Information Exchange (WHIE) meets the definition of a Regional Health Information Organization (RHIO).⁴² WHIE has established a formal governance and membership structure, but has not yet entered into the implementation stage or begun to exchange data.

Many of the issues that are addressed in this scenario have been considered in developing the governance structures for WHIE. For example, business associate agreements will allow for the greatest exchange of information, while still meeting the needs of the member organizations.

Additionally, in the process of developing information exchange, there has been intensive discussion about who “owns” the data and ensuring its validity. A statewide Action Plan, to be submitted to the Governor by the end of 2006, will serve as a catalyst for the development and implementation of RHIOs in Wisconsin. The issues related to data ownership and use will continue to be addressed, and solutions will likely be found to allow for the sharing of health information for both treatment purposes and public health.

Scenario 7 – Research

A research project on children younger than age 13 is being conducted in a double-blind study for a new drug for ADD/ADHD. The research is being sponsored by a major drug manufacturer conducting a double-blind study approved by the medical center’s IRB where the research investigators are located. The data being collected is all electronic and all responses from the subjects are completed electronically on the same centralized and shared data base file.

The principle investigator was asked by one of the investigators if they could use the raw data to extend the tracking of the patients over an additional six months and/or use the raw data collected for a white paper that is not part of the research protocol’s final document for his post-doctoral fellow program.

⁴² RHIO: an independent corporation that is intended to operate an exchange of clinical health information among competing stakeholder organizations supporting multiple use cases (Gartner Health Care; U.S. Clinical IT Initiatives: A Hype Cycle; 13-16 November 2005; The Hyatt Regency Grand Cypress; Orlando, Florida).

Legal Analysis

State and federal law require that certain legal requirements be met for patient information to be accessible for research purposes without patient consent. In this scenario, the Legal Workgroup made the assumption that the research project had been approved by the Institutional Review Board (IRB), the waiver was obtained through this process and consent from the patient for the disclosure of information for research purposes would not be required. In this case, state requirements for release without consent⁴³ for research purposes are less stringent than HIPAA⁴⁴ and federal law would control. Therefore, consent would not be required for disclosures related to the IRB-approved research project.

Legal Barriers

In this scenario, both requests for disclosure of patient information appear to be outside IRB approval and patient consent would be required under both state and federal law to disclose for an additional six months of research or for a post-graduate paper. Any time consent is required to exchange information, it creates a barrier to exchange. The process to share information requires a determination of whether consent is required and the analysis presents a barrier to health information exchange. The process to obtain consent poses an additional barrier to exchange because it requires contact with the patient or other legally authorized person to obtain the consent. Additional barriers include determining who is legally authorized to sign the consent and validating the statutorily required elements of the consent.

If HIPAA applies to the research project then the following statutory requirements would present barriers to health information exchange:

- Verification of the requester
- Application of the minimum necessary standard
- Security in the electronic transfer of information
- Documentation of disclosures.

Scenario 8 – Law Enforcement

An injured nineteen-year-old college student is brought to the ER following an automobile accident. It is standard to run blood alcohol and drug screens. The police officer investigating the accident arrives in the ER claiming that the patient may have caused the accident. The patient's parents arrive shortly afterward. The police officer requests a copy of the blood alcohol test results and the parents want to review the ER record and lab results to see if their child tested positive for drugs. These requests to print directly from the electronic health record are made to the ER staff.

The patient is covered under their parent's health and auto insurance policy.

⁴³ Wis. Stats. 146.81(2)(a)6, 51.30(4)(b)3, 252.15(5)(a)10

⁴⁴ 45 CFR 164.512(i)

Legal Analysis

Under the scenario it was not clear if the blood draw was performed for treatment purposes or at the request of law enforcement for the determination of intoxication related to the automobile accident. If the blood draw had been performed at the request of law enforcement and not for treatment, the test result would not have been protected from access by law enforcement under Wisconsin law and the result would have been accessible to law enforcement.⁴⁵ No barrier would have been presented to this exchange of information.

Legal Barriers

If the blood draw in this scenario is performed for treatment purposes, consent is required for disclosure to law enforcement or to the parents as there is no statutory exception under Wisconsin law that allows for disclosure to either without patient consent.⁴⁶ Because the patient is of the age of majority in Wisconsin, consent would be required to release patient information to the parents.⁴⁷ Any time consent is required to exchange information, it creates a barrier to exchange. The process to share information requires a determination of whether consent is required and the analysis presents a barrier to health information exchange. The process to obtain consent poses an additional barrier to exchange because it requires contact with the patient or other legally authorized person to obtain the consent. Additional barriers include determining who is legally authorized to sign the consent and validating the statutorily required elements of the consent.

HIPAA would require that the identity of the individuals requesting the patient information, in this case law enforcement and the parents, be verified.⁴⁸ This requirement presents a barrier to health information exchange.

Although federal law would not require documentation of a disclosure with patient consent, documentation is required under Wis. Stat. 146.82(2)(d). This documentation requirement presents barriers to health information exchange by requiring specific documentation of a disclosure every time a designated disclosure occurs. Although this requirement may be met by audit and monitoring techniques in an electronic exchange, the electronic system will be required to document the statutorily required elements.

Additional barriers to health information exchange identified in this scenario relate to security of information transfer and transmission. If the HIPAA Security Rule applies to any of the disclosers of information in this scenario the following requirements would need to be met and will present barriers to the exchange of information.

- Determination of information to be disclosed and application of minimum necessary standard⁴⁹
- Method of exchange and security measures for protection of exchange.⁵⁰

⁴⁵ Wis. Stat. 146.81(4)

⁴⁶ Wis. Stat. 146.82(1)

⁴⁷ Wis. Stats. 146.82(1), 146.81(5)

⁴⁸ 45 CFR 514(h)(1)

⁴⁹ 45CFR 164.502(b) minimum necessary

⁵⁰ Security and Privacy Rules

Scenario 9 – Pharmacy Benefit Scenario A

The Pharmacy Benefit Manager (PBM) has a mail order pharmacy for a hospital which is self-insured and also has a closed formulary. The PBM receives a prescription from Patient X, an employee of the hospital, for the antipsychotic medication Geodon. The PBM's preferred alternatives for antipsychotics are Risperidone (Risperdal), Quetiapine (Seroquel), and Aripiprazole (Abilify). Since Geodon is not on the preferred alternatives list, the PBM sends a request to the prescribing physician to complete a prior authorization in order to fill and pay for the Geodon prescription. The PBM is in a different state than the provider's Outpatient Clinic.

Legal Analysis

The Legal Workgroup agreed that a disclosure from the patient is not protected under state or federal law. Once the prescription is received from the patient, the PBM would be required to maintain the patient information in a confidential manner.

If the self-insured hospital is considered to be a covered entity as either a hospital or health plan⁵¹ under HIPAA, a business associate agreement would be required to enable the self-insured hospital to share information with the PBM, a business associate providing services to the hospital.⁵²

If the Geodon prescription is considered general health information, patient consent would not be required under state or federal law for an exchange between health care providers for treatment or payment purposes.⁵³ If the Geodon prescription is considered to be sensitive patient information and is regulated by Wis. Stat. 51.30, consent would be required for disclosure for payment purposes from the physician to the PBM.

Legal Barriers

If the self insured hospital is considered to be a covered entity⁵⁴ under HIPAA, a business associate agreement would be required to enable the self-insured hospital to share information with the PBM.⁵⁵ The legal requirements and the process required to obtain a business associate agreement present a barrier to health information exchange.

If the Geodon prescription is considered to be mental health information, the controlling law would be Wis. Stat 51.30 and more stringent protections would apply. Patient consent for information exchange between the PBM and the prescribing physician would be required as there are no statutory exceptions for treatment or payment purposes under this Wisconsin law.⁵⁶ Any time consent is required to exchange information, it creates a barrier to exchange. The process to share information requires a determination of whether consent is required and the analysis presents a barrier to health information exchange. The process to obtain consent poses an additional barrier to exchange because it requires contact with the patient or other legally authorized

⁵¹ 45CFR 164.103

⁵² 45 CFR 164.502(2)(e); 45 CFR 164.504(e); 45 CFR 164.506(c)(3)

⁵³ Wis. Stat. 146.82(2)(a)2; 45 CFR 164.506(c)2

⁵⁴ 45CFR 164.103

⁵⁵ 45 CFR 164.502(2)(e); 45 CFR 164.504(e); 45 CFR 164.506(c)(3)

⁵⁶ Wis. Stat. 51.30(4)

person to obtain the consent. Additional barriers include determining who is legally authorized to sign the consent and validating the statutorily required elements of the consent.

The federal Privacy and Security Rules require that the identity of a requester for protected health information be verified to determine that the individual is who they claim to be. In this scenario, verification of the PBM requesting the patient information would be required.⁵⁷ There is no similar requirement in Wisconsin law unless the Geodon is mental health information and then verification of the requestor is also required under Wisconsin law.⁵⁸ This requirement presents a barrier to health information exchange.

State law is also more stringent than HIPAA in requiring the application of the minimum necessary standard to treatment information released for mental health information disclosures.⁵⁹ If the disclosure is for payment purposes HIPAA and state law would require application of the minimum necessary standard.

Documentation of the disclosure of general health information or sensitive health information, although not required by federal law, would be required by state law and under the preemption analysis, state law would control.⁶⁰ This documentation requirement presents barriers to health information exchange by requiring specific documentation of a disclosure every time a designated disclosure occurs. Although this requirement may be met by audit and monitoring techniques in an electronic exchange, the electronic system will be required to document the statutorily required elements.

If the exchange is electronic, HIPAA would require that the prescribing physician secure the transmission to the PBM.⁶¹

Scenario 10 – Pharmacy Benefit Scenario B

A Pharmacy Benefit Manager 1 (PBM1) has an agreement with Company A to review the companies' employees' prescription drug use and the associated costs of the drugs prescribed. The objective would be to see if the PBM1 could save the company money on their prescription drug benefit. Company A is self insured and as part of their current benefits package, they have the prescription drug claims submitted through their current PBM (PBM2). PBM1 has requested that Company A send their electronic claims to them to complete the review.

Legal Analysis

Company A, as a self-insured business, would be considered a health plan under HIPAA and would be required to have a business associate agreement with both PBM1 and PBM2 to share protected health information. The business associates, through their

⁵⁷ 45 CFR 164.514(h)

⁵⁸ HFS 92.03(1)(m)

⁵⁹ HFS 92.03(n)

⁶⁰ Wis. Stat. 51.30(4)(e)

⁶¹ 45 CFR 164 Subpart C

relationship with the health plan, would be required to adhere to the restrictions of the HIPAA Privacy and Security Rules.⁶²

Unless Company A could be considered a health care provider under Wisconsin law, there would be no state privacy protection relating to this scenario. Exchange between these entities would be considered a “use,” not a protected disclosure.

Legal Barriers

Whenever a business associate agreement (BAA) is required there are barriers to information exchange. The BAA must contain required statutory elements and must often be reviewed and approved by legal counsel. This agreement, which may be necessary to assure patient confidentiality, would present a barrier to health information exchange.

Under federal law, PBM2, as the business associate of company A, would be required to verify the identity of the requestor PBM1.⁶³ This requirement presents a barrier to health information exchange.

Disclosures within this scenario would be controlled by the HIPAA minimum necessary standard⁶⁴ and the application of this standard presents a barrier to health information exchange.

If the sharing of information is electronic, under the HIPAA Security Rule the exchange would be required to be secured.⁶⁵

Scenario 11 - Health Care Operations and Marketing - Scenario A

ABC Health Care is an integrated health delivery system comprised of ten critical access hospitals and one large tertiary hospital, DEF Medical Center, which has served as the system’s primary referral center. Recently, DEF Medical Center has expanded its rehab services and created a state-of-the-art, stand-alone rehab center. Six months into operation, ABC Health Care does not feel that the rehab center is being fully utilized and is questioning the lack of rehab referrals from the critical access hospitals.

ABC Health Care has requested that its critical access hospitals submit monthly reports containing patient identifiable data to the system six-sigma team to analyze patient encounters and trends for the following rehab diagnoses/ procedures:

- Cerebrovascular Accident (CVA)
- Hip Fracture
- Total Joint Replacement

Additionally, ABC Health Care is requesting that this same information, along with

⁶² 45 CFR 164.504(e)(1)

⁶³ 45 CFR 164.514(h)

⁶⁴ 45 CFR 164.514(d)

⁶⁵ 45 CFR 164 Subpart C

individual patient demographic information, be provided to the system Marketing Department. The Marketing Department plans to distribute to these individuals a brochure highlighting the new rehab center and the enhanced services available.

Legal Analysis

In this scenario the request for patient information is an internal request from one department to another, either within a health care facility or within an organized health care arrangement or an affiliated network.

In Scenario 11, if ABC Health care is considered an organized health care arrangement or an affiliated health care arrangement, both state and federal law would allow the internal sharing of identifiable patient information for quality assurance activities which fit under the definition of allowable health care operations. Both laws allow the sharing of information for health care operations without patient consent, and the described activity with sigma six appears to meet the definition of health care activities.⁶⁶

Generally state law does not control an internal disclosure of patient information within a health care facility or network as it is considered an acceptable internal “use” where internal confidentiality policies, not state law, control the protection of the information. Generally, marketing activities are considered an internal “use” and would not be controlled by state law.

Federal law (HIPAA) has very specific guidance relating to the use of patient information for marketing activities. Since state law is silent unless a disclosure occurs, federal law, when applicable, controls internal use of patient information for marketing activities. HIPAA requires patient consent for marketing activities.⁶⁷ The requirement of patient consent for marketing activities does not apply if the activity does not meet the HIPAA definition of marketing.⁶⁸ Based on the HIPAA exclusions from the marketing definition, the activity of the marketing department to send information to patients relating to the new rehab center and enhanced services available would not be deemed marketing as it is providing information to patients on hospital services, and patient consent would not be required.

Neither state nor federal law requires documentation of an internal use/disclosure for marketing.

Legal Barriers

State law does not require verification of a requestor of identifiable patient information, however federal law does. That means that all covered entities must have written policies and procedures for verifying and authenticating the identity of a requestor of patient identifiable information.⁶⁹ Most responses from stakeholders indicated that knowing the requestor for an internal exchange would be sufficient verification of identity. This requirement may present a barrier to information exchange.

⁶⁶ Wis. Stat. 146.82 (1); 45 CFR 164.501 Definitions; 45 CFR 164.506

⁶⁷ 45 CFR 164.508(a)(3)

⁶⁸ 45 CFR 164.501 Definitions Marketing

⁶⁹ 45 CFR 164.514(h)(1)

Federal law requires that the minimum necessary standard be applied to disclosures of identifiable information to an internal marketing department. Most of the stakeholders applied this standard when disclosing information to the marketing department. The application of this standard presents a barrier to health information exchange.

State law does not control the internal transmission of patient identifiable data but federal law does. Federal law requires that security and privacy precautions be implemented regarding the internal transfer of patient identifiable data.⁷⁰ This requirement, if deemed necessary, would be an impediment to the exchange of health care information.

Scenario 12 - Health care Operations and Marketing - Scenario B

ABC hospital has approximately 3,600 births/year. The hospital Marketing Department is requesting identifiable data on all deliveries including mother's demographic information and birth outcome (to ensure that contact is made only with those deliveries resulting in healthy live births).

The Marketing Department has explained that they will use the patient information for the following purposes:

1. To provide information on the hospitals' new pediatric wing/services.
2. To solicit registration for the hospital's parenting classes.
3. To request donations for construction of the proposed neonatal intensive care unit.
4. They will sell the data to a local diaper company to use in marketing diaper services directly to parents.

Legal Analysis

In this scenario the request for patient information is an internal request from the marketing department to another internal department within a hospital facility.

Generally state law does not control a disclosure of patient information within a health care facility as it is considered an acceptable internal "use" where internal confidentiality policies, not state law, control the protection of the information. Generally, marketing activities would be considered an internal "use" and would not be controlled by state law. Therefore patient consent would not be required for an internal use. In the event that the internal use results in an external disclosure, such as to a diaper company, then state law would treat that occurrence as a disclosure and state law privacy protections would apply.

Federal law (HIPAA) has very specific guidance relating to the use of patient information for marketing activities. Since state law is silent until a disclosure occurs, federal law, when applicable, will control internal use of patient information for marketing activities. HIPAA requires patient consent for marketing activities.⁷¹ The way in which HIPAA control over marketing activities may not apply is to determine that the specific activity

⁷⁰ Federal Security and Privacy Rules (HIPAA)

⁷¹ 45 CFR 164.508(a)(3)

does not meet the HIPAA definition of marketing and therefore is not controlled by HIPAA.⁷²

Based on the HIPAA exclusions from the marketing definition, the following communications under Scenario 12 would be excluded from HIPAA marketing control and patient consent would not be required:

- To provide information on the new pediatric wing
- To provide information about parenting classes

Neither state nor federal laws require documentation of an internal disclosure for marketing. However, if the use is deemed a disclosure, as in the relationship with the diaper company, documentation would be required under state and federal law.⁷³

Legal Barriers

State law does not require verification of a requestor of identifiable patient information, however federal law does. That means that all covered entities must have written policies and procedures for verifying and authenticating the identity of a requestor of patient identifiable information.⁷⁴ Most responses from stakeholders indicated that knowing the requestor would be sufficient verification of identity. This process may present a minimal barrier to information exchange.

Generally, marketing activities would be considered an internal “use” and would not be controlled by state law. Therefore patient consent would not be required for an internal use. In the event that the internal use results in an external disclosure, such as to a diaper company, then state law would treat that occurrence as a disclosure and state law privacy protections would apply.

The two marketing activities which meet the HIPAA definition of marketing and therefore require patient consent under HIPAA for this use/disclosure are the disclosure for fundraising and for marketing with the diaper company. Since the exchange with the diaper company would be deemed a disclosure under Wisconsin law and there is no statutory exception for this type of disclosure, the exchange with the diaper company would also require patient consent under Wisconsin law. Any time consent is required to exchange information, it creates a barrier to exchange. The process to share information requires a determination of whether consent is required and the analysis presents a barrier to health information exchange. The process to obtain consent poses an additional barrier to exchange because it requires contact with the patient or other legally authorized person to obtain the consent. Additional barriers include determining who is legally authorized to sign the consent and validating the statutorily required elements of the consent. In addition, under HIPAA, when an activity is deemed marketing, the patient must be offered the opportunity to opt out. The activation of the patient “opt out” would impede information exchange.

⁷² 45 CFR 164.501 Definitions Marketing

⁷³ Wis. Stat. 146.82(d); 45 CFR 164.528

⁷⁴ 45 CFR 164.514(h)(1)

Federal law requires that the minimum necessary standard be applied to disclosures of identifiable information to an internal marketing department. Most of the stakeholders apply this standard when disclosing information to the marketing department and agree that the application of this standard presents a barrier to health information exchange.

Neither state nor federal laws require documentation of an internal disclosure for marketing. However, if the use is deemed a disclosure, as in the relationship with the diaper company, documentation would be required under state and federal law.⁷⁵ This documentation requirement presents barriers to health information exchange by requiring specific documentation of a disclosure every time a designated disclosure occurs. Although this requirement may be met by audit and monitoring techniques in an electronic exchange, the electronic system will be required to document the statutorily required elements.

State law does not control the internal transmission of patient identifiable data but federal law does. Federal law requires that security and privacy precautions be implemented regarding the internal transfer of patient identifiable data.⁷⁶ This requirement, if deemed necessary, would be an impediment to the exchange of health care information.

Scenario 13 - Bioterrorism event

A provider sees a person who has anthrax, as determined through lab tests. The lab submits a report on this case to the local public health department and notifies their organizational patient safety officer. The public health department in the adjacent county has been contacted and has confirmed that it is also seeing anthrax cases, and therefore this could be a possible bioterrorism event. Further investigation confirms that this is a bioterrorism event, and the State declares an emergency. This then shifts responsibility to a designated state authority to oversee and coordinate a response, and involves alerting law enforcement, hospitals, hazmat teams, and other partners, as well informing the regional media to alert the public to symptoms and seek treatment if feel affected. The State also notifies the Federal Government of the event, and some federal agencies may have direct involvement in the event. All parties may need to be notified of specific identifiable demographic and medical details of each case as they arise to identify the source of the anthrax, locate and prosecute the parties responsible for distributing the anthrax, and protect the public from further infection.

Legal Analysis

State and federal law either mandate or allow disclosure of a positive lab test for anthrax without patient consent to the patient's treating provider, local public health, state agencies with a statutory need to know and federal agencies that provide emergency public health services.⁷⁷ Anthrax is a category 1 communicable disease, which means notification must occur within 24 hours to the local health officer.⁷⁸ According to Wis. Stat. 252.03(2), local health officers may do what is reasonable and necessary for the

⁷⁵ Wis. Stat. 146.82(d); 45 CFR 164.528

⁷⁶ Federal Security and Privacy Rules (HIPAA)

⁷⁷ HFS 145.04(2) (d)

⁷⁸ HFS 145 Appendix A; Wis. Stat. 252.05(5)

prevention and suppression of disease. Under the authority of Wis. Stat. 252.02(1) the Department may also establish systems of disease surveillance and inspection to ascertain the presence of any communicable disease.

The Wisconsin Department of Health and Family Services (“DHFS”) is provided with broad authority and emergency management powers under Wisconsin Statute 252, where the Department may authorize and implement all emergency measures to control communicable diseases, including anthrax. According to Wis. Stat. 252.02(6), the Department may authorize and implement all emergency measures necessary to control communicable diseases. This statute also requires physicians, health care facilities, and laboratories that know or have reason to believe that a person treated or visited by him/her has a communicable disease, has died, and shall immediately report to their local health officer. The local health officer shall report this information to DHFS.⁷⁹ The powers defined in this statute allow the removal of barriers to allow rapid and effective responses to an anthrax threat. Local health officers are provided with powers similar to those of the Department; however, they need to keep the Department updated on measures taken. In addition, Wisconsin is part of an informal group of states (Greater Board of Health Initiative) which will share data interstate, in the event of communicable disease outbreaks.

State law allows the Governor to declare an emergency, and that order empowers the exchange of information relating to, in this case, a communicable disease.⁸⁰

Wisconsin also has a health network that provides primary information and timely communications about public health threats. This information is distributed in a number of forms, including “fax blast,” e-mail, U.S. mail, etc., to all health care providers and public health agencies to help them understand the threat and be alerted to possible cases. This communication most likely will not identify patients by name; however it may contain other elements of protected health information such as demographic characteristics, age, gender, etc. However, if identifying the patient is necessary to help find cases of anthrax, then the patient’s identity would probably be disclosed. Wisconsin law will allow this and the decision would be based on balancing a patient’s privacy versus protecting the public. In Wisconsin there are no privacy barriers to prevent exchanging this information.⁸¹

The Federal Privacy Law (HIPAA) also provides for the disclosure of patient information without patient consent under this scenario through the exceptions allowing for disclosure when required by law, for public health purposes and for public oversight.⁸²

Neither state nor federal law present privacy barriers, such as requiring patient consent, for the disclosures within this scenario.

This scenario did not present an information exchange in which there is a request for information so the requirement for verification of the requester did not need to be met in this scenario and did not present a barrier to information exchange.

⁷⁹ HFS 145.04(2)(d)

⁸⁰ Wis. Stat. 166.03 Emergency powers of Governor

⁸¹ Wis. Stat. 252.02(6)

⁸² 45 CFR 164. 512 (a) and (b)

Legal Barriers

State and federal law require the documentation of disclosures within this scenario, although the stakeholder practices were variable.⁸³ This requirement presents barriers in health information exchange by requiring specific documentation of a disclosure every time a designated disclosure occurs. Although this requirement may be met by audit and monitoring techniques in an electronic exchange, the electronic system will be required to document the statutorily required elements.

Additional barriers to health information exchange identified in this scenario relate to security of information transfer and transmission. If the HIPAA Security Rule applies to any of the disclosers of information in this scenario the following requirements would need to be met and will present barriers to the exchange of information.

- Determination of information to be disclosed⁸⁴
- Method of exchange and security measures for protection of exchange⁸⁵
- Requirements for receipt of the information⁸⁶

Scenario 14 – Employee Health

An employee (of any company) presents in the local emergency department for treatment of a chronic condition that has exacerbated which is not work-related. The employee's condition necessitates a four-day leave from work for illness. The employer requires a "return to work" document for any illness requiring more than 2 days leave. The hospital Emergency Department has an EHR and their practice is to cut and paste patient information directly from the EHR and transmit the information via email to the Human Resources department of the patient's employer.

Legal Analysis

State and federal law require patient consent to disclose the patient's medical information related to the back-to-work form from the provider to the employer.⁸⁷

Wisconsin law and the federal privacy law do not require patient consent for release of information to the patient. Therefore, if the form validating the employee's return to work is provided to the patient, no consent is required.⁸⁸ A provider, under the Federal Privacy Rule, may require that the request for information from the patient be provided in writing.

Legal Barriers

State and federal law require patient consent to disclose the patient's medical information related to the back-to-work form from the provider to the employer.⁸⁹

⁸³ Wis. Stat. 146.82(2)(d); 45 CFR 164.528(a) and (b)

⁸⁴ Wis. Stat. 252.05(2); HFS 145.04(1) and (2); and 45CFR 164.502(b) minimum necessary did not apply

⁸⁵ Security and Privacy Rules

⁸⁶ Wis. Stat. 252.05(6); HFS 145.04(2)(d) 45 CFR 164.501 Definition of designated record set

⁸⁷ Wis. Stats. 146.82(1), 51.30(4)(a), 252.15(5); 45 CFR 164.508

⁸⁸ Wis. Stats. 146.83, , 252.15(5)(a); 1HFS 92.05; 45 CFR 164.524

⁸⁹ Wis. Stats. 146.82(1), 51.30(4)(a), 252.15(5); 45 CFR 164.508

Any time consent is required to exchange information, it creates a barrier to exchange. The process to share information requires a determination of whether consent is required and the analysis presents a barrier to health information exchange. The process to obtain consent poses an additional barrier to exchange because it requires contact with the patient or other legally authorized person to obtain the consent. Additional barriers include determining who is legally authorized to sign the consent and validating the statutorily required elements of the consent.

State law does not require verification of a requestor of identifiable patient information, however federal law does. Therefore all covered entities must have written policies and procedures for verifying and authenticating the identity of a requestor of patient identifiable information.⁹⁰

The stakeholders agreed that a “cut and paste” process from the provider’s EHR would not be an acceptable process for assembling patient information that will be sent to the patient’s employer. The Federal Privacy Rule requires that the provider releasing the patient back-to-work information apply the HIPAA minimally necessary standard in relation to the information released.⁹¹ The application of this process is agreed to present a barrier to health information exchange.

Both state and federal law require documentation of a disclosure to the patient’s employer.⁹² Only state law requires documentation of disclosure to the patient.⁹³

This documentation requirement presents barriers to health information exchange by requiring specific documentation of a disclosure every time a designated disclosure occurs. Although this requirement may be met by audit and monitoring techniques in an electronic exchange, the electronic system will be required to document the statutorily required elements.

An additional barrier to health information exchange identified in this scenario relates to security of information transfer and transmission. If the HIPAA Security Rule applies to the discloser of information from the health care provider to the employer, the method and means of exchange would be required to be secured.⁹⁴

Scenario 15 - Public Health Scenario A - Active carrier, communicable disease notification

A patient with active TB, still under treatment, has decided to move to a desert community that focuses on spiritual healing, without informing his physician. The TB is classified MDR (multi-drug resistant). The patient purchases a bus ticket - the bus ride will take a total of nine hours with two rest stops across several states. State A is made aware of the patient's intent two hours after the bus with the patient leaves. State A now needs to contact the bus company and other states with the relevant information.

⁹⁰ 45 CFR 164.514(h)(1)

⁹¹ 45 CFR 164.514(d)

⁹² Wis. Stats. 146.82(d); 45 CFR 164.528

⁹³ Wis. Stats. 146.83

⁹⁴ Security and Privacy Rules

Legal Analysis

State and federal law either mandate or allow disclosure of a communicable disease such as tuberculosis (TB) without patient consent to the patient's treating provider, local public health, state agencies with a statutory need to know and federal agencies that provide emergency public health services.⁹⁵ According to Wis. Stat. 252.03(2), local health officers may do what is reasonable and necessary for the prevention and suppression of disease; according to Wis. Stat. 252.02(1), the Department may also establish systems of disease surveillance and inspection to ascertain the presence of any communicable disease.

The Wisconsin Department of Health and Family Services ("DHFS") is provided with broad authority and emergency management powers under Wisconsin Statute 252, where the Department may authorize and implement all emergency measures to control communicable diseases, including TB. According to Wis. Stat. 252.02(6), the Department may authorize and implement all emergency measures necessary to control communicable diseases. This statute also requires physicians, health care facilities, and laboratories that know or have reason to believe that a person treated or visited by him/her has a communicable disease, has died, and shall immediately report to their local health officer. The local health officer shall report this information to DHFS.⁹⁶ The powers defined in this statute allow the removal of barriers to allow rapid and effective responses to a TB threat. Local health officers are provided with powers similar to those of the Department; however, the need to keep the Department updated of measures taken. In addition, Wisconsin is part of an informal group of states (Greater Board of Health Initiative) which will share data interstate, in the event of communicable disease outbreaks.

Wisconsin also has a health network that provides primary information and timely communications about public health threats. This information is distributed in a number of forms, including "fax blast," e-mail, U.S. mail, etc., to all health care providers and public health agencies to help them understand the threat and be alerted to possible cases. This communication most likely will not identify patients by name; however may have other elements of protected health information such as demographic characteristics, age, gender, etc. However, if identifying the patient is necessary to help find TB cases, then the patient's identity would probably be disclosed. Wisconsin law will allow this and the decision is based on balancing of privacy versus protecting the public. In Wisconsin there are no privacy barriers to prevent exchanging this information.⁹⁷

The Federal Privacy Law (HIPAA) also provides for the disclosure of patient information without patient consent under this scenario through the exceptions allowing for disclosure when required by law, for public health purposes and for public oversight.⁹⁸

Neither state nor federal law present privacy barriers such as requiring patient consent to the disclosures within this scenario.

⁹⁵ HFS 145.04(2) (d)

⁹⁶ HFS 145.04(2)(d)

⁹⁷ Wis. Stat. 252.02(6)

⁹⁸ 45 CFR 164. 512 (a) and (b)

This scenario did not present an information exchange in which there is a request for information so the requirement for verification of the requester did not need to be met in this scenario and did not present a barrier to information exchange.

The scenario also did not present a barrier in relation to the determination of information to be disclosed. The state is granted broad powers of authority to maintain and control communicable disease and would be enabled to disclose information as deemed necessary. The federal law, although questionable in its applicability in this scenario, does not apply the minimum necessary standard to disclosures required by law⁹⁹.

Legal Barriers

State and federal law require the documentation of disclosures within this scenario, although the stakeholder practices were variable.¹⁰⁰ Wisconsin law requires the Department to maintain reports of communicable diseases as health care records under Wis. Stats. 146.81-.835¹⁰¹ and therefore disclosure of information from reports would require documentation of the disclosure under Wis. Stat.146.82(2)(d). If the state authority in this scenario is a HIPAA covered entity then the Privacy Rule would also require documentation of the disclosures to meet the patient's right of accountability.¹⁰² This requirement presents barriers in health information exchange by requiring specific documentation of a disclosure every time a designated disclosure occurs. Although this requirement may be met by audit and monitoring techniques in an electronic exchange, the electronic system will be required to document the statutorily required elements.

An additional barrier to health information exchange identified in this scenario relates to security of information transfer and transmission. If the HIPAA Security Rule applies to any of the disclosers of information in this scenario the federal requirements relating to a secured method of information exchange and security measures for protection of the exchange¹⁰³ would need to be met and would present a barrier to the exchange of information.

Scenario 16 – Public Health - Scenario B -Newborn screening

A newborn's screening test comes up positive for a state-mandated screening test and the state lab test results are made available to the child's physicians and specialty care centers specializing in the disorder via an Interactive Voice Response (IVR) system. The state lab also enters the information in its registry, and tracks the child over time through the child's physicians. The state public health department provides services for this disorder and notifies the physician that the child is eligible for those programs.

Legal Analysis

Wisconsin law allows disclosure of a state-mandated newborn screening test results to the state lab, the child's physician and family, to specialty care centers providing

⁹⁹ 45 CFR 164.512(a); 45 CFR 164.502(b)(2)(v)

¹⁰⁰ Wis. Stat. 146.82(2)(d); 45 CFR 164.528(a) and (b)

¹⁰¹ Wis. Stat. 252.05(6)

¹⁰² 45 CFR 164.528

¹⁰³ Security and Privacy Rules

specialized treatment for the screened anomaly and to the state health department without patient consent. Wisconsin law also mandates the Department to establish and maintain a registry for identified birth defects as depicted in this scenario.

Wisconsin law requires screening for congenital disorders of all newborns; screening samples are to be submitted and processed through the state laboratory of hygiene (“state lab”) (Wisconsin Statutes 253.13). This scenario presents a similar process to that authorized by Wisconsin law.

Wisconsin law mandates disclosure of the screening result from the state lab to the physician [Wisconsin Statutes 253.13(4)], and the HIPAA Privacy Rule allows disclosures without patient authorization when a use/disclosure is required by law, for public health activities or for treatment purposes. [45 CFR 164.512(a) and (b); 45 CFR 164.506].

State and federal law allow disclosure of information relating to a positive screening test from physician to parents [Wisconsin Statutes 146.83 and 253.13 (4)]. Additionally, the patient (parent of minor) has legal right of access to his or her own patient information under state and federal law [Wisconsin Statutes 146.83 and 253.14(5)1 and 45 CFR 164.524].

The state lab is contracted to perform the necessary diagnostic services and tests on behalf of the Department so exchange between these entities would be allowed by law without patient consent.¹⁰⁴

The Department has an obligation under Wis. Stat. 252.12 and s.252.13 to refer individuals with positive screening tests for early intervention and other appropriate services. If the disclosure is specifically for purposes of treatment and/or intervention, it would be allowable under Wis. Stat. 253.12 (3)(a)1.d. and Wis. Stat. 253.13(4) and (5). The State agency may notify the physician and the patient’s family of eligibility for state programs; however, the patient/family may opt out of this notification [Wisconsin Statutes 252.13(3), (4) & (5)]. In Wisconsin, the disclosures relating to referral for treatment are made to the provider and patient’s family and generally not disseminated to specialty care centers except when the Department is involved in a specific referral for treatment. A general disclosure to multiple specialty care centers without a more specific referral may require patient consent.

Wisconsin law also requires the maintenance of a state registry of individuals with positive screening results [Wisconsin Statutes 253.12], in the form of a registry of children with birth defects [Wisconsin Statutes 253.12 (3)1.].

There is no requirement or continuing allowance for follow-up by the state registry to a physician [Wisconsin Statutes 253.13(3)(a)1]. State law does however allow for disclosure by a physician to a state agency that is determining a duly authorized function without patient consent upon the receipt of a written request [Wisconsin Statutes 146.82(2)(a)5]. HIPAA 45 CFR 164.512(b) would also allow disclosure by the physician to the state registry for public health purposes without patient authorization.

¹⁰⁴ Wis. Stat. 253.13(2)

There are no privacy barriers, such as requiring patient consent, related to the disclosures within this scenario.

This scenario did not present an information exchange in which there is a request for information so the requirement for verification of the requester did not need to be met in this scenario and did not present a barrier to information exchange.

Legal Barriers

State and federal law require the documentation of disclosures within this scenario¹⁰⁵ although the stakeholder practices were variable. Wisconsin law would require the physician to document disclosures to the patient/patient representative and to the state registry.¹⁰⁶ State law would also require the state laboratory if deemed a health care provider to document disclosures made without consent to the physician and the specialty centers.¹⁰⁷ HIPAA also requires covered entities to document disclosures made so that an accounting of disclosures is available to the patient.¹⁰⁸ These documentation requirements present barriers to health information exchange by requiring specific documentation of a disclosure every time a designated disclosure occurs. Although this requirement may be met by audit and monitoring techniques in an electronic exchange, the electronic system will be required to document the statutorily required elements.

The federal Privacy and Security Rules require that the identity of a requester for protected health information be verified to determine that the individual is who they claim to be. In this scenario, the physician as a covered entity under HIPAA would be required to verify the requester from the state registry tracking the patient through the registry process. This requirement presents a barrier to health information exchange.

Additional barriers to health information exchange identified in this scenario relate to security of information transfer and transmission. If the HIPAA Security Rule applies to any of the disclosers of information in this scenario, the following requirements would need to be met and will present barriers to the exchange of information.

- Determination of information to be disclosed¹⁰⁹
- Method of exchange and security measures for protection of exchange¹¹⁰
- Requirements for receipt of the information¹¹¹

Scenario 17 – Public Health Scenario C- Homeless shelters

A homeless man arrives at a county shelter and is found to be a drug addict and in need of medical care. The person does have a primary care provider, and he is sent there for medical care. Primary care provider refers patient to a hospital-affiliated drug treatment clinic for his addiction under a county program. The addiction center must report treatment information back to the county for program reimbursement, and back to the

¹⁰⁵ Wis. Stat. 146.82(2)(d); 45 CFR 164.528(a) and (b)

¹⁰⁷ Wis. Stat. 146.82(2)(d)

¹⁰⁸ 45 CFR 164.528

¹⁰⁹ 45CFR 164.502(b) minimum necessary

¹¹⁰ Security and Privacy Rules

¹¹¹ Wis. Stat. 253.13(4); 45 CFR 164.501 Definition of designated record set

shelter to verify that the person is in treatment. Someone claiming to be a relation of the homeless man requests information from the homeless shelter on all the health services the man has received. The staff at the homeless shelter is working to connect the homeless man with his relative.

Legal Analysis

State and federal law require an exchange-by-exchange analysis in this scenario to determine whether or not the requested information may be disclosed with or without patient consent. This scenario clearly depicts the complexities of the health information exchange process in Wisconsin. It requires determining who is requesting the information, whether they are who they say they are, whether they have the authority to access the information, what law applies, whether the information exchanged is sensitive, what should be disclosed if the information is releasable, and what additional restrictions apply to the mode and security of the exchange.

The process for information exchange in this scenario required the application of at least four laws and an administrative code, including the HIPAA Privacy and Security Rules, the federal rules regulating alcohol and drug abuse, Wis. Stat. 146.82, Wis. Stat. 51.30 and Wisconsin administrative code HFS 92. The application of that analysis to these exchanges, understanding there are very specific constraints under Wisconsin law, allows disclosure from provider to provider of non-sensitive patient information without consent. The disclosure of sensitive information from the drug treatment clinic to the county for reimbursement purposes and to the county homeless shelter for verification of treatment was allowable without consent under the state and federal privacy rules¹¹² but consent was required by the rules regulating alcohol and drug abuse treatment records.¹¹³

Legal Barriers

The federal regulations controlling records related to alcohol and drug abuse provide very restrictive privacy protection to sensitive patient information. These regulations preempt both state and federal privacy rules in requiring patient consent for disclosures to the county for reimbursement purposes and to the county homeless shelter for verification of treatment. The complexity of this analysis, the variability in the application of the laws, and variability in current practices present significant barriers to health information exchange of sensitive patient information.

This scenario also presented an opportunity to review access to patient information by the family. In this case, analysis of state and federal law clarified that a patient consent is required to release patient information to the patient's family.¹¹⁴ HIPAA would have allowed disclosure to the family members if they were involved with the patient's care and the patient agreed, but these facts were not present in this scenario and HIPAA was preempted by state and other more protective federal law.

Any time consent is required to exchange information, it creates a barrier to exchange. The process to share information requires a determination of whether consent is

¹¹² Wis. Stat. 51.30(4)(b)2; Wis. Stat. 46.215, 46.22, 51.42 or 51.437; 45 CFR 164.506

¹¹³ 42 CFR Part 2

¹¹⁴ Wis. Stat. 51.30(4)(b); 45 CFR 164.512 and 164.508; 42 CFR Part 2

required, and the analysis presents a barrier to health information exchange. The process to obtain consent poses an additional barrier to exchange because it requires contact with the patient or other legally authorized person to obtain the consent. Additional barriers include determining who is legally authorized to sign the consent and validating the statutorily required elements of the consent.

The federal Privacy and Security Rules require that the identity of a requester for protected health information be verified to determine that the individual is who they claim to be. In this scenario, if the county homeless shelter either by contract or by definition is governed by HIPAA Privacy and Security laws, verification of the family member requesting the patient information would be required. This requirement presents a barrier to health information exchange.

Although HIPAA would not require documentation of disclosure for treatment and payment purposes¹¹⁵ as depicted in this scenario, Wisconsin Statute 51.30 requires documentation of disclosures made by a health care provider so when applicable in this scenario, such as from the substance abuse facility, documentation would be required. This documentation requirement presents barriers to health information exchange by requiring specific documentation of a disclosure every time a designated disclosure occurs. Although this requirement may be met by audit and monitoring techniques in an electronic exchange, the electronic system will be required to document the statutorily required elements.

Additional barriers to health information exchange identified in this scenario relate to security of information transfer and transmission. If the HIPAA Security Rule applies to any of the disclosers of information in this scenario, the following requirements would need to be met and will present barriers to the exchange of information.

- Determination of information to be disclosed and application of minimum necessary standard¹¹⁶
- Method of exchange and security measures for protection of exchange¹¹⁷
- Requirements for receipt of the information¹¹⁸

Scenario 18 - Health Oversight: Legal compliance/government accountability

The Governor's office has expressed concern about compliance with immunization and lead screening requirements among low income children who do not receive consistent health care. The state agencies responsible for public health, child welfare and protective services, Medicaid services, and education are asked to share identifiable patient-level health care data on an ongoing basis to determine if the children are getting the health care they need. This is not part of a legislative mandate. The Governor in this state and those in the surrounding states have discussed sharing this information to determine if patients migrate between states for these services. Because of the complexity of the task, the Governor has asked each agency to provide these data to faculty at the state university medical campus who will design a system for integrating and analyzing the data. There is no existing contract with the state university for

¹¹⁵ 45 CFR 164.528(a)(1)(i)

¹¹⁶ 45CFR 164.502(b) minimum necessary

¹¹⁷ Security and Privacy Rules

¹¹⁸ Wis. Stat.51.30; 45 CFR 164.501 Definition of designated record set

services of this nature.

Legal Analysis

For disclosures among state agencies with statutory authority to collect patient information and statutory authority to use that patient information for a legally authorized function, patient consent would not be required. However, without appropriate statutory authority to share identifiable patient information among state agencies or patient consent, a contractual agreement would be required.

Legal Barriers

In this scenario, the Governor requested state agencies to share identifiable patient information, including Medicaid services data, to determine if the children were receiving appropriate health care services. Both federal and state law (Wis. Stat. 49.45(4)) do not allow DHFS to disclose identifiable information about recipients enrolled in the Medicaid Program unless the disclosure is for the administration of the Medicaid Program. In this scenario, the intent of the disclosure is not really clear based on the information provided. An analysis would need to be completed prior to the release of this information and a patient consent or contractual agreement may be required. The need for further legal analysis, the complexity of application of the laws and the variability in practice of rules and regulations applied by multiple state agencies create a barrier to the inter-agency exchange of patient information.

Disclosures of patient identifiable information between state agencies and a state university for the purpose of building a data bank for the state would require patient consent or some type of legally authorized contractual agreement such as a business associate agreement. More specifically in this scenario, Wisconsin Medicaid data cannot be disclosed unless there is a business associate agreement in place between the University and the Department; otherwise the disclosures would be in violation of the federal privacy regulation. This disclosure would be regulated by the HIPAA Security and Privacy Rules and, in relation to some state agency records, the Wisconsin privacy rules and would require a business associate agreement between the entities to share/exchange identifying patient information. The requirement of a legal agreement to exchange would impose a barrier to information exchange.

Additional barriers to health information exchange identified in this scenario relate to security of information transfer and transmission. If the HIPAA Security Rule applies to any of the disclosers of information in this scenario the following requirements would need to be met and will present barriers to the exchange of information.

- Determination of information to be disclosed and application of minimum necessary standard¹¹⁹
- Method of exchange and security measures for protection of exchange¹²⁰

¹¹⁹ 45CFR 164.502(b) minimum necessary

¹²⁰ Security and Privacy Rules