



## Managing Information Privacy & Security in Healthcare

### RHIOs and HIPAA

Steven J. Fox  
Pepper Hamilton LLP

David S. Szabo  
Nutter, McClennen & Fish, LLP

Howard A. Burde  
Blank Rome LLP

Extracted from the book, *Guide to Establishing a Regional Health Information Organization*, edited by Christina Beach Thielst, FACHE, and LeRoy E. Jones, and written by the HIMSS RHIO Guidebook Task Force. Chicago: HIMSS; 2007.

### Introduction

RHIOs must maintain the privacy and security of protected health information (PHI) and must do so in a manner that complies with the Health Insurance Portability and Accountability Act (HIPAA) privacy and security standards. This is true despite the fact that these standards will not apply directly to most RHIOs, as most RHIOs will not be covered entities<sup>1</sup>. However, covered entities that participate in a RHIO by either providing data to the RHIO or obtaining data from the RHIO must comply with the privacy and security rules and will want to ensure compliance by the RHIO. Accordingly, RHIOs must build information privacy and security into both their technology and business processes.

This chapter is not intended to provide a comprehensive or in-depth discussion or analysis of the information privacy and security rule. Instead, it will highlight some key privacy and security issues that will apply to most data exchange projects, and issues that are of particularly relevance to developing RHIOs. This chapter will address the applicability of HIPAA to the formation, organization and operation of RHIOs.

---

<sup>1</sup> HIPAA defines "covered entities" as (i) a health plan; (ii) (2) a health care clearinghouse; or (iii) a health care provider who transmits any health information in electronic form in connection with standard transactions. A RHIO that serves a clearinghouse function by translating non-standard transactions into standard format transactions, as defined by the administrative simplification rule, will be a covered entity subject to the information security and privacy rules in its own right. A clearinghouse can also be a business associate of a covered entity, however.

## PRIVACY

### Background/HIPAA Analysis

The general rule is that covered entities may only use or disclose PHI for treatment, payment or health care operations. Likewise, covered entities must protect the confidentiality, integrity and availability of electronic protected health information (ePHI) that they store, maintain, transmit or receive. By definition, RHIOs are involved in transmitting and receiving ePHI between and among covered entities, and some RHIOs, depending on their structure, may also store at least some elements of ePHI. For example, a RHIO that operates a master patient index or record locator service probably will store demographic data about patients, which is a subset of ePHI. Also dependent upon the architecture of the RHIO is whether or not it will act as a business associate of covered entities, and will have to comply with business associate privacy and security requirements, as well. If the RHIO is carrying out its activities "on behalf of" one or more covered entities, and requires access to protected health information in order to carry out its activities, then the RHIO may well be a business associate, as defined by the HIPAA administrative simplification regulations, and must enter into a business associate agreement with the covered entity or entities. In our experience, most RHIOs will be business associates.

However, not all organizations that move ePHI from one covered entity to another are business associates. Organizations that act only as passive "conduits" or switches for ePHI in transit are not considered business associates under HIPAA. Examples of these organizations include the post office and overnight parcel services (for physical movement of electronic media) and internet service providers such as, Utah Health Information Network. Even a specialized switch that moves electronic protected health information in the form of encrypted messages might not be a business associate if it does not need access to protected health information in order to perform its work.

In theory, a RHIO could subcontract all of its data exchange activities to a vendor or consultant, such that the RHIO itself never had access to ePHI. In that case, the RHIO entity itself would not be a business associate of the covered entities, but its prime vendor probably would be.<sup>2</sup> Every RHIO or data interchange organization should determine whether it is a business associate to covered entities. The covered entities will insist upon this when entering into business associate agreements with the RHIO.

Another less commonly seen RHIO structure is that of an organized health care arrangement (OHCA), where a group of covered entities holds itself out to the public as a joint arrangement, and participate in joint activities including utilization review, quality assessment and improvement activities, or payment activities involving financial risk sharing. At least two benefits of organizing a RHIO as an OHCA come readily to mind: (i) in addition to other permitted uses and disclosures of PHI, a participating covered entity may also disclose PHI about an individual to another participating covered entity for any health care operations activities of the OHCA; and (ii) participating covered entities may satisfy the requirements for a Notice of Privacy Practices (NPP) by a single joint notice rather than multiple notices furnished by each individual covered entity, provided that certain additional requirements are met.<sup>3</sup>

---

<sup>2</sup> A RHIO that creates standard processes for data interchange and provides technical services to its members through a common consultant or vendor could operate in this manner.

<sup>3</sup> (1) The participating covered entities agree to abide by the terms of the NPP with respect to PHI created or received by the covered entity as part of its participation in the OHCA;

If an OHCA structure is not used, each participating covered entity must separately provide an NPP to its patients. However, since each entity presumably has a different version of the NPP, it is essential that all NPPs are coordinated with common language and descriptions of the RHIO and the joint activities, risks/benefits for patients, and uses and disclosures that will flow from participation in the RHIO. The NPP may also be the appropriate vehicle with which to offer patients the opportunity to opt-in or –out of the RHIO. Some RHIOs are using a reverse opt-in mechanism, whereby patients are notified that if they do not affirmatively opt-out, they will be automatically assumed to agree that their PHI may be included in the RHIO. This mechanism should be carefully reviewed and considered, since it has not been approved as yet by any regulatory or court decisions.

## Uses And Disclosures Of PHI

Whatever structure is ultimately decided upon for the RHIO, it may use or disclose PHI as follows:

- It may use or disclose PHI for the treatment, payment or health care operations of a covered entity;
- It may disclose PHI for the treatment activities of a health care provider;
- It may disclose PHI to a covered entity or a health care provider for the payment activities of the recipient;
- It may disclose PHI to a covered entity for health care operations activities of the recipient, if each entity either has or had a relationship with the individual who is the subject of the PHI being requested, the PHI pertains to such relationship, and the disclosure is:
  - For a purpose listed in paragraph (1) or (2) of the definition of health care operations; or
  - For the purpose of health care fraud and abuse detection or compliance.

In addition to the general rules stated above, a RHIO must develop and implement comprehensive policies and procedures governing:

- Appropriate levels of role-based access to PHI for all participants and their employees;
- Comprehensive tracking and audit controls;

---

(2) The joint notice meets the implementation specifications in paragraph (b) of § 164.520, except that the required statements may be altered to reflect the fact that the NPP covers more than one covered entity; and

(i) Describes with reasonable specificity the covered entities to which the joint NPP applies;

(ii) Describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the joint NPP applies; and

(iii) If applicable, states that the covered entities participating in the OHCA will share PHI with each other, as necessary to carry out treatment, payment or health care operations relating to the OHCA.

(3) The covered entities included in the joint NPP must provide the notice to individuals in accordance with the applicable implementation specifications of paragraph (c) of § 164.520. Provision of the joint NPP to an individual by any one of the covered entities included in the joint notice will satisfy the provision requirement of paragraph (c) of § 164.520 with respect to all others covered by the joint notice.

- Individuals' rights to agree or to object to specific uses/disclosures under certain conditions;
- Uses/disclosures for which an authorization or opportunity to agree or object is not required;
- Individuals' rights to request privacy protection and/or alternative communication methods for PHI;
- Individuals' rights of access to their PHI;
- Individuals' rights to amend their PHI;
- RHIO's accounting of disclosures of PHI;
- Mechanism for participants to coordinate special patient arrangements with the RHIO.

One of the thorniest issues surrounding the use and disclosure of PHI is whether or not a patient authorization is required<sup>4</sup>. As discussed above, most uses/disclosures are permitted without asking a patient to sign an authorization, which is considered an extraordinary step under HIPAA. However, because of uncertainty in this area, some RHIOs are using authorizations as part of their standard operating procedure. Others, as previously mentioned, are simply using the NPP as a mechanism for presuming their patients' consent or approval for participation in the RHIO. There is no single answer that will work in all situations; however, we suggest a cautious approach for this matter. If it is decided to ask each patient for an authorization, remember that: (i) a covered entity may not generally condition the provision of treatment, payment, enrollment in a health plan or eligibility for benefits on the signing of an authorization by the patient; (ii) all authorizations under HIPAA must contain an expiration date; (iii) patients must be advised of their right to revoke the authorization at any time; and (iv) the authorization must be written in plain language. So the use of authorizations will require a significant additional bookkeeping, legal and clerical component in order to assure compliance with the detailed regulatory provisions.<sup>5</sup>

There is another important consideration which must be dealt with regarding uses and disclosures of PHI, and that is the "minimum necessary" rule.<sup>6</sup> The general rule is that when using or disclosing PHI or when requesting PHI from another covered entity, a covered entity must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. Luckily, the rule does not apply to:

- Disclosures to or requests by a health care provider for treatment;
- Uses or disclosures made to the individual;
- Uses or disclosures made pursuant to an authorization under § 164.508;

---

<sup>4</sup> Keep in mind that § 164.508 requires an authorization for most uses and disclosures of psychotherapy notes.

<sup>5</sup> See § 164.508 for a detailed discussion of requirements for authorizations.

<sup>6</sup> See § 164.502(b).

- Disclosures made to the Secretary of the United States Department of Health and Human Services in accordance with subpart C of part 160;
- Uses or disclosures that are required by law, as described by § 164.512(a); and
- Uses or disclosures that are required for HIPAA compliance.

Uses and disclosures for research purposes are beyond the scope of these guidelines, and add an additional level of complexity. If such use is contemplated, it may require approval by an Institutional Review Board or privacy board, and may also necessitate specific authorizations by affected patients as well as compliance with other federal and state laws and regulations.

Finally, although it is not necessarily required by HIPAA for non-covered entities, it may be advisable to appoint a RHIO-level privacy officer to interact with the various participants' own Privacy Officers and to assure compliance with all of the rules, regulations and laws that will impact the operation and management of the RHIO. The privacy officer may also coordinate training among all of the RHIO participants, and oversee the adoption and use of the comprehensive policies and procedures (including sanctions) that will keep the RHIO functioning smoothly.

## SECURITY

This section will address organizational issues, risk assessment, safeguard selection, federated versus central security, and selected elements of the security management process.

### **Administrative Safeguards: Assigned Responsibility**

A RHIO should formally assign responsibility for information security. While there is no formal requirement in HIPAA for a business associate to appoint a security officer, formal designation of this responsibility is likely to become a practical necessity. A RHIO can either designate one individual to act as its information security officer; or it can form a working group of security officers from sponsoring organizations. The creation of a working group is more likely to be the initial option, with a dedicated security officer coming later as the RHIO develops. Even after the appointment of a security officer, a security working group may be useful when implementing safeguards and monitoring their effectiveness.

A working group composed of several security officers has the advantage of providing multiple points of view to the security management process. Additionally, if the RHIO includes more than one type of covered entity or data source, then security expertise can be drawn from each type of organization. Since data sources often have different perspectives on risk that data users (usually being more risk averse), this diversity of viewpoints and perspectives can be extremely valuable to the planning process.

### **Administrative Safeguards: Risk Assessment**

Covered entities must perform an assessment of the risks and vulnerabilities to the security of electronic protected health information, including an assessment of the likelihood and criticality of each security threat. Similarly, a RHIO also should formally assess risks arising from data exchange projects. Once the risks have been identified, the covered entities participating in the RHIO must be able to assure

themselves that they or others have “implemented security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.”<sup>7</sup>

The RHIO should assess both the likelihood and criticality of threats to the security of ePHI. Events that are extremely unlikely or that, if they occur, are not of critical significance, are a lower priority than more probable threats or unlikely events that would have extremely serious consequences.

The security analysis should take into account the types of information being exchanged and maintained. For example, if information about mental health, substance abuse or HIV/AIDS is being exchanged, a higher level of confidentiality assurance and additional business process steps may be required<sup>8</sup>. Indeed, depending on the information and the state in which the RHIO operates, it might be necessary to filter certain information out of the data stream.<sup>9</sup> The RHIO should analyze the contemplated uses and disclosures of ePHI or “use cases” under both federal and state privacy laws, especially as state privacy laws often impose additional restrictions on certain types of data or types of covered entities.

The security analysis should take into account the technology employed for patient identification and data exchange. Messaging systems that only operate when a user affirmatively elects to send a message require different safeguards than “always on” connections through portals that can be accessed by data users without human intervention at the data source.

The security analysis should consider the number and types of personnel with access to ePHI. The number of users participating in the project might dictate the need for automated tools for authorizing users, issuing and revoking credentials and auditing user activities. In addition, the number of authorized users involved is a risk factor in and of itself, which the RHIO should account for in its planning process.

Once this analysis is complete, and any conditions on the use or disclosure of PHI are identified, security safeguards should be implemented to support the permitted uses and disclosures and prevent forbidden uses and disclosures. The RHIO should prepare written risk analysis and use it as a guide in the selection and implementation of the administrative, physical and technical safeguards that are being employed to protect the confidentiality, integrity and availability of ePHI.

## **Selection and Implementation of Safeguards**

The selection and implementation of safeguards is a key element of security compliance. The selection process should take into account whether particular safeguards are required by the security rule, or are only “addressable.” Where a safeguard is “addressable” under the rule, the RHIO or its covered entities should adopt the safeguard if it is reasonable and appropriate under the circumstances. If the RHIO or covered entity chooses not to implement a safeguard, it must document why it would not be reasonable and appropriate, and implement “an equivalent alternative” measure, if reasonable and appropriate.

It may very well be that certain addressable safeguards, such as encryption for data being transmitted, are essentially required, in that no alternative safeguard will reasonably and appropriately

---

<sup>7</sup> This is the literal language of the rule, see 45 C.F.R. § 164.308(a)(1)(B).

<sup>8</sup> The security rule does not recognize any one type of PHI as deserving more protection than any other. Professional standards of practice as well as variations in state privacy and liability laws suggest otherwise.

<sup>9</sup> Filtering was used in the MEDSINFO ED Proof of Concept Project. See Health Affairs [citation].

protect the security of the information. Ideally, the RHIO's risk analysis, selection and implementation of safeguards will be clearly documented.

Some safeguards might be implemented through a federated model—that is each covered entity will have delegated responsibility for implementing the safeguard within its organization on behalf of the RHIO. This is particularly appropriate where the RHIO does not handle data itself, but uses standards and contracts to facilitate peer to peer connections among the participating organizations<sup>10</sup>. Other safeguards, such as an activity monitoring system, might be implemented on a centralized basis by the RHIO itself<sup>11</sup>. The choice between federated and central security measures will require an analysis of the information architecture, security requirements, and the capabilities of participating covered entities.

The principle of “defense in depth” may lead to the implementation of both central and federated security measures. For example, a RHIO might have centrally maintained activity logs tracking all use of a data exchange application, while each covered entity will maintain its own logs documenting its uses of RHIO resources. Investigation of a privacy breach or security incident might require the use of both central and federated activity logs.

Every data exchange project needs to consider how to manage identities and access. Will the RHIO centrally issue credentials to users, or will it allow the participating covered entities to issue credentials? What legal obligations will remain with the users, and which ones will reside at the RHIO?

The RHIO should consider roles as an element of access control. A RHIO might implement role-based access controls, and then require participating covered entities to adopt common administrative safeguards and delegate the authorization of users to each covered entity in accordance with common administrative rules or definitions.

The creation and assignment of roles requires an understanding of the business processes that will occur at the organizations using the data exchange system. For example, the RHIO must determine whether physicians will query the system directly, or will the physicians rely on nurses or administrative personnel to gather information at the point of care. The answer may vary from organization to organization, or even between departments in the same organization.

The practical ability of the RHIO to dictate the adoption of roles or other safeguards might depend on the criticality of the application or the degree to which the RHIO's proposed safeguards are consistent with safeguards that are already commonly accepted among the user community.

The RHIO should have guidelines for the auditing of activity logs, including both automated reviews of system activities, and random manual audits for security purposes.

The risk analysis and legal requirements may require the implementation of special safeguards for certain types of data. Especially sensitive information, such as HIV/AIDS, mental health or substance abuse information, may require this kind of protection. For example, this information might need to be stored in locked records that cannot be shared among providers or released to other users without human intervention.

---

<sup>10</sup> This is the model for the New England Healthcare EDI Network, which facilitates administrative transactions among its participants.

<sup>11</sup> MA-SHARE implemented a central activity log as part of the portal for the MEDSINFO ED project.

## Security Management

The RHIO should develop a security management process that allows each covered entity to comply with the rule while participating in the RHIO. This would include developing a process for security collaboration among participating organizations. If a working group of security officers has been formed, this group might continue to meet in order to compare notes on possible security threats to the RHIO, review of activity reports, or to discuss real or alleged incidents involving the data exchange systems.

Collaboration among security officers will probably require them to focus on an agreed-upon definition of security incident. The group probably will want to prioritize their limited time to deal with significant threats to the system, not just review reports that have little or no security significance.

It is almost inevitable that as a result of human error, a technical failure or a novel attack that some security incident or privacy breach will occur. It is extremely important that the RHIO has agreed upon procedures for incident response, reporting and remediation. Since the RHIO is likely to be a business associate to several covered entities, once an incident is identified, the role of reporting and remediation probably will fall to the covered entities and not the RHIO itself.

There are several good reasons for RHIOs to play a support role, but not a primary role, when incidents occur. Unless the RHIO itself is a covered entity (which could occur if the RHIO is a clearinghouse), the primary obligation of security and privacy compliance falls upon the covered entities, which understandably will want to control any process of reporting and remediation of a breach or incident. Additionally, the investigation of a breach or incident may involve additional uses or disclosures of protected health information, much of which may not even be in the possession of the RHIO. Thus, the RHIO will probably limit its role to supporting or assisting the covered entities.

## RHIO Agreements

Legal obligations relating to privacy and security must be taken into account in developing vendor and business associate agreements. RHIOs that outsource a significant portion of their data exchange activities should give considerable thought and attention to the requirements that they impose on key vendors and business associate subcontractors.

Many data exchange agreements and subcontracts simply state that each party will implement "reasonable and appropriate" safeguards. This language, drawn directly from the security rule, may be legally sufficient. However, the RHIO and its sponsors should consider carefully whether particular safeguards should be established as absolute minimum requirements for vendors.

Often, the discussion of safeguards begins and ends with technical safeguards, and a statement that "we can't dictate someone else's technology." However, not all safeguards are technical, and even the adoption of common technical safeguards defined by categories does not mandate the use of particular vendors or technologies. For example, an administrative safeguard might include a requirement that all employees handling PHI be screened against exclusion and sanction databases maintained by the Office of Inspector General (OIG), or that criminal background checks be performed.

All business associate agreements require the reporting of privacy breaches and security incidents. However, the template agreement recommended by the Department of Health and Human Services does not mandate specific timeframes for incident reports or particular content for incident reports.

Given the potential public relations and regulatory implications of a privacy breach or security incident, covered entities would be wise to ask for a very short time frame for an initial report (perhaps as short as one business day) with a longer timeframe for a written follow up report that includes a root cause analysis and discussion of remedial steps that have been or should be taken.

Vendors that play a key role in the RHIO, such as outsourcing or hosting companies, could be expected to sign agreements that are quite detailed with respect to information security. Other vendors may simply need to covenant to comply with the security rule. In every case, the criticality of the vendor's contribution to the project and the risks to security of ePHI should be considered in order to strike an appropriate balance.

RHIOs will enter into agreements with the covered entities that engage in data exchange projects—sometimes called Participant Agreements, End User Agreements or Data User Agreements. Obviously, these agreements must define the services and technology to be provided by the RHIO, economic terms and other factors, but also should set forth both parties' mutual obligations with respect to privacy and information security. Indeed the terms of these agreements are an essential part of the chain of trust that stretches from the RHIO's data sources to the data users. These agreements should set forth both the expectations of participants as data users and data sources, as well as the obligation that the RHIO must impose on the participants as part of the chain of trust.

One of the most difficult issues to think about or negotiate in data exchange agreements is indemnification from liability. An indemnification clause is a legal obligation to defend the other party to the contract from a claim asserted by a third person, and to pay any resulting settlement. For example, a provider of drug history data might say, "I will provide you with drug history data, but you have to defend me if a patient later sues me because you failed to protect the data, and the patient was injured as a result." Many risks, such as medical liability, patent infringement and others, potentially can be the subject of indemnification. While indemnification may be fair and reasonable in some circumstances, indemnification requirements can have a chilling effect on the willingness of organizations to participate in a data exchange project.

## STATE LAW ISSUES

In addition to HIPAA, each state has numerous laws which apply to the privacy of health care information. Each of these laws is a consideration in developing the rules of the network. The analysis begins with a determination of which of the state laws apply under HIPAA.

HIPAA regulations preempt "contrary" provisions of state law, with limited exceptions.<sup>12</sup> A determination of what is contrary is the first step in the HIPAA preemption analysis. Under the HIPAA regulations, a state law is contrary if a covered entity would find it impossible to comply with both the state law and with HIPAA or if complying with the state law would be an obstacle to fulfilling the requirements of HIPAA.<sup>13</sup>

Even when a state law is contrary to HIPAA, it would not be preempted when: (1) the state law is necessary to prevent fraud and abuse, to regulate insurance or health plans, to regulate health care

---

<sup>12</sup> 42 C.F.R. Sec.160.202

<sup>13</sup> 42 C.F.R. Sec. 160.202

delivery, or to regulate controlled substances; (2) the state law relates to the privacy of health information and is more stringent than the HIPAA privacy rule; (3) the state law mandates public health reporting, investigation or intervention; or (4) the state law requires health plan reporting.<sup>14</sup>

The “more stringent than” rule is known as floor preemption. State laws with privacy provisions “more stringent than” HIPAA regulations are not preempted.<sup>15</sup>

## State Health Information Privacy Laws

State laws regarding health information address a multitude of issues of interest to RHIOs: (1) To whom do such laws apply? (2) Under what circumstances may the information be transmitted? (3) What information may be transmitted? (4) What conditions apply to transmission of health care information?

Because many state laws which apply to PHI are or were written to regulate the practice of professions or the operation of facilities or health plans, they do not address PHI in the same manner as HIPAA, which is focused on the use of information. This is in part because most laws regulating healthcare preceded the HIPAA privacy and security regulations. It should be noted that several states have enacted laws which regulate health information in the insurance context.<sup>16</sup> These laws often address issues of consent and authorization, notice, amendment and other use questions. Other state laws, such as facility and health professional licensure regulations tend to address the issues of content, ownership and storage of records. Still other laws, such as mental health and sexually transmitted disease laws provide specific guidance with respect to spousal and parental access to information.

Indeed most state laws will have no direct application to RHIOs, but because of the direct application to the regulated member of the RHIO, they must be considered. Other laws may not even apply to members of RHIOs, but nevertheless exist as part of the environment in which the RHIO is being created. For example, virtually every state’s hospital licensure laws have medical record retention requirements.<sup>17</sup> By contrast state laws which regulate the transmission of information regarding sexual assault may only apply to law enforcement or rape counselors, neither of which are likely to be considered covered entities or candidates for RHIO participation.

So, in creating an inventory of applicable laws, a RHIO should first determine what laws apply to the exchange of health care information. The next step will be to determine which laws actually apply to the activities in which the RHIO is engaged, or those activities in which the RHIO’s members will be engaged. The RHIO and its members cannot be in the position of putting other members at risk of violating their licensure or other regulatory requirements.

The next level of analysis is determining what aspects or types of information may be transmitted and under what conditions. Laws that apply include, by way of example, insurance laws, genetic testing laws and disease specific laws. These laws must be compared to HIPAA privacy regulations for both contrariness and stringency to determine whether HIPAA or the state law will be applied to the transmission of health information through the RHIO. For example, a number of states have laws prohibiting medical laboratories from sending lab results to anyone other than the healthcare provider who ordered the tests.<sup>18</sup>

---

<sup>14</sup> 42 C.F.R. Sec. 203

<sup>15</sup> 45 CFR § 160.203(b)

<sup>16</sup> See e.g., 28 Tex.Admin.Code § 22.52

<sup>17</sup> See, e.g., 28 Pa.Code § 115.23

<sup>18</sup> Need citations.

These laws could inadvertently have the effect of preventing the results from being timely sent directly to the RHIO; instead introducing an extra, unnecessary step in the process.

Disease specific laws in each state provide guidance with respect to what HIPAA calls the minimum necessary rule. In practice this mean the disease specific law often defines the scope of information that may be transmitted by a provider or otherwise identified person or entity. Common examples include HIV/AIDS, mental health, and substance abuse laws.

Laws pertaining to HIV/AIDS permit diagnostic test results to be released only to the patient and then, often, only with counseling. Further transmission of patient testing information is limited to the consent of the patient or, in the absence of such consent to notify those potentially infected by the patient.<sup>19</sup> Pennsylvania law permits disclosure to twelve designated categories of persons and entities for a circumscribed set of situations. For example, one designated category and situation is the provision which states that HIV/AIDS information may be released "if it would be necessary in case of emergency."<sup>20</sup> Not just any emergency, but only those when it would be "necessary." Given that this law also provides for a private right of action for breach of the privacy rights, this sort of silly locution is a potential trap for providers. To date it has not been the source of reported decisions against those who release information for the purposes of treatment. Nevertheless, it is this sort of problematic language that will impact RHIOs in one of three ways: (1) RHIOs will proscribe the transmission of such information absent explicit consent; (2) Participants will transmit such information inconsistently; or (3) The RHIO and its participants will devote extraordinary time and resources to working through rules that apply to such information. The same sort of problematic laws exist in other disease specific laws as well.

Mental health laws contain restrictions on the transmission of different types of information. Most significantly, these restrictions often include limitations on the types of psychotherapy notes that may be transmitted as part of a claim for coverage.<sup>21</sup> For RHIO purposes, the question is what information a mental health provider may include as part of a record transmitted through the RHIO and for what purposes. Also, is the technology mature enough for such providers to distinguish electronically? In the absence of recognized limitations, will such providers participate? Extremely important in this discussion is whether the drug prescription information is included in the information shared through the RHIO as this information can indicate a mental health diagnosis indirectly.

Drug and alcohol treatment laws have the most stringent confidentiality provisions of any laws, virtually across all states. First, federal law provides that the "[r]ecords of the identity, diagnosis, prognosis or treatment of any patient" in a drug or alcohol program funded in whole or in part by the federal government(which means most of them) are confidential and may be released only if the patient has consented in advance to the disclosure or in the absence of disclosure (1) in the event of medical emergency; (2) for research, management audits, financial audits, or program evaluation; or (3) as mandated by court order.<sup>22</sup>

State laws tend to expand upon the federal confidentiality requirements. For example, the Pennsylvania Drug and Alcohol Abuse Control Act provides that patient records so obtained or patient records "relating to drug or alcohol abuse or drug or alcohol dependence prepared or obtained by a private

---

<sup>19</sup> Texas Health Code Ann. § 81.101(5)

<sup>20</sup> 35 P.S. § 7607(a)(6)

<sup>21</sup> 740 ILCS 110/6

<sup>22</sup> 42 U.S.C. § 290dd-2. See also 42 C.F.R. part 2.

practitioner, hospital, clinic drug rehabilitation or drug treatment center shall remain confidential and may be disclosed only with the patient's consent and only (i) to medical personnel exclusively for diagnosis and treatment; . . . or (ii) to government or other government officials exclusively for the purpose of obtaining benefits due the patient...[except for emergency situations for which records may be released] to proper medical authorities . . ."<sup>23</sup> Note the use of the conjunction "and" which means that even with the patient's consent drug and alcohol records may not be released beyond those two recipients. At least for RHIO purposes, the drug and alcohol rules are clear. Therein lies a fundamental conflict: the clarity of health information related laws is often inversely related to the need to transmit information. A strict prohibition is an easy rule to follow but inhibits the transmission of health care information which, after all, is the purpose of the RHIO.

What set or subset of medical records or other form of PHI may be exchanged? Each of the disease and covered entity specific state laws in some fashion define the scope of information covered.

Title XIX of the Social Security Act, and state laws which pertain to Medicaid programs also address the privacy of health care information. Federal law requires State Medical Assistance plans to "provide safeguards which restrict the use or disclosure of information concerning applicants and recipients to purposes directly connected with administration of the plan."<sup>24</sup> Federal Medicaid regulations implementing this requirement define "purposes directly related to plan administration" to include providing services for recipients.<sup>25</sup>

Under most state laws and Medicaid managed care organization contracts, identifiable health information may be shared with a provider where such information is required for treatment purposes without patient consent, so long as the recipient will treat the information confidentially and not use it for other purposes.<sup>26</sup> Medicaid law, therefore, does not inhibit health information exchange.

## **Liability and Indemnification**

RHIOs and their participants face two types of liability related to the use of health information: breach of privacy obligations and professional/medical malpractice liability.

Breach of privacy obligations may arise from case law or from specific statutory recognition of the cause of action. While the HIPAA enforcement mechanism is oversight by the Department of Health and Human Services and the Justice Department, many state laws specifically provide for private enforcement action. One of the more profound impediments to RHIO formation is the negotiation regarding the delegation of responsibility for the transmission of health care information inappropriately, and for the content of the information provided. As RHIOs are relatively new entities and the law on the topic of health care information privacy is not well developed, so the availability and cost of insurance coverage specific to such risk is uncertain. Presumably, the RHIO will require that its members maintain some sort of umbrella liability policy governing general errors and omissions which might be specifically written to include inadvertent release of health care information. Such a rule, of course, presumes that an insurer will be willing to underwrite the risk of inadvertent or inappropriate release of health information.

---

<sup>23</sup> 71 P.S. § 1690.108(c); see also 4 Pa.Code § 255.5

<sup>24</sup> 42 U.S.C. 1396a(a)(7).

<sup>25</sup> 42 C.F.R. § 431.302.

<sup>26</sup> See 55 Pa. Code § 105.3.

By contrast, the law of medical malpractice liability is very well developed. The question raised by the use of health care information transmitted in a health information exchange is who bears the liability for the content of the information exchanged, whether the consolidation of information into a common form creates medical malpractice or another form of liability (which impacts the use of experts and potentially, depending upon the state, the amount of recovery), and whether the existence of an available source of information specific to a patient creates an obligation on the part of the provider to consult that source of information.

By way of short background, the elements of any medical malpractice case are few: There must be an injury or adverse event; the standard of care, established by expert testimony, must have been breached; and the breach must be the proximate cause of the injury.

Therefore, placing health information exchange in the medical malpractice context, the question is how the standard of care will be interpreted and applied. Will the standard of care ultimately include responsibility on the part of each participant in a health information exchange to validate the information transmitted through the RHIO? Will the standard establish the responsibility of a treating provider to obtain available sources of information? Will the standard establish the responsibility of parties, such as payer to provide information to the health information exchange?

The standard of care with respect to health care provider use of available information is evolving. To the extent that the entire development of American liability law recognizes that adoption of innovations leads to developments of higher expectations and therefore higher standards of care, we can expect that the increased availability of health care information in an inexpensive and useful format will lead to a standard of care which establishes the responsibility of the provider to use such information. Innovation leads to higher standards, witness fetal monitoring and glaucoma cases (see, e.g. Helling v. Carey).

RHIOs and their participants need also be concerned that the developing standards include responsibilities for the accuracy of information in the exchange. To that end, who determines accuracy of content of health information? Who is responsible for correcting PHI? Whose version of events/diagnoses prevails? What is impact of practice enhancements on health professional liability? Or on payers which pay for performance?

To the extent that the RHIO engages in these activities, it is creating a source of liability which cannot be avoided. Ultimately such issues will not be resolved by the RHIO or its participants, but rather the responsibility for the potential liability will be negotiated as part of the participation agreement among the participants. That negotiation will result in an agreement to the parameters for responsibility for breaches of the standard of care, indemnification for actions which may implicate the RHIO and the other participants, and insurance coverage for potential losses. While it would be helpful to have a common tool to assess potential risk to each party in exchange, including the exchange or RHIO, such a tool may be too difficult to establish. It is likely to be much easier, though more expensive, for the parties to agree to bear and insure risk for own actions. This agreement would be supplemented by common insurance for collective risks as a means to allay concerns.