



**HEALTH  
CENTER  
CONTROLLED  
NETWORKS  
SERIES**

*Previously INTEGRATED SERVICES  
DELIVERY NETWORKS (ISDN) SERIES*

*For more information contact*

Jacqueline C. Leifer, Esq. or  
Adam J. Falk, Esq.  
Feldsman Tucker Leifer Fidell LLP  
2001 L Street N.W.  
Washington DC 20036  
Telephone: (202) 466-8960;  
Fax: (202) 293-8103  
Email: AFalk@ftlf.com

or

Betsy Vieth  
National Association of Community  
Health Centers, Inc.  
7200 Wisconsin Avenue, Suite 210  
Bethesda, Maryland 20814  
Telephone: (301) 347-0400;  
Fax: (301) 347-0459  
Email: BVieth@nachc.com

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is published with the understanding that the publisher is not engaged in rendering legal, financial or other professional service. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

*The Health Resources and Services Administration, Bureau of Primary Health Care (HRSA/BPHC) supported this publication under Cooperative Agreement Number U30CS00209. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of HRSA/BPHC.*

## Strategies to Minimize Legal Risks Related to Health Information Exchange

In communities across the country, health center networks<sup>1</sup> have assisted health centers in adopting health information technology (HIT), ushering in a world of electronic health record (EHR) systems, computerized physician order entry systems, and practice management systems.<sup>2</sup> As a result, some health center networks have built an HIT infrastructure that, in the future, could support the sharing of electronic health information (eHI) not only between health centers, but also with hospitals, primary care associations, local health plans, and state or local health departments.<sup>3</sup>

Some health centers also participate in local and state collaborations as part of a Health Information Network, Health Information Exchange, or Regional Health Information Organization.<sup>4</sup> These collaborations develop

- 1 Health Center Controlled Networks (HCCN) is a HRSA-funded grant program that supports the creation, development, and operation of networks of safety net providers to ensure access to health care for the medically underserved populations through the enhancement of health center operations, including health information technology. HCCN currently comprises HRSA-funded grant programs formerly known as Integrated Services Development (ISDI) Initiative, Shared Integrated Management Information Systems (SIMIS), and Information and Communication Technology (ICT). HCCN is scheduled to conclude at the end of fiscal year 2007. More information is available at [www.hrsa.gov/healthit/healthcenters.htm](http://www.hrsa.gov/healthit/healthcenters.htm).
- 2 NORC at the University of Chicago, "Final Report, Community Health Center Information Systems Assessment: Issues and Opportunities", October 2005. For definitions of health IT applications, see National Health Policy Forum's "Health Information Technology Adoption Among Health Centers: A Digital Divide in the Making?", July 23, 2007, available at [www.nachc.org/research/files/CHC%20HIT%20survey%20fact%20sheet.pdf](http://www.nachc.org/research/files/CHC%20HIT%20survey%20fact%20sheet.pdf).
- 3 NORC, at 14-15.
- 4 Foundation of Research and Education of American Health Information Management Association, "Development of State Level Health Information Exchange Initiatives," Sep. 1, 2006. More information is available at [www.staterhio.org](http://www.staterhio.org). This Issue Bulletin adopts the term "Health Information Exchange" or "HIE" to refer to any electronic data sharing activities by providers.

standards and practices for data sharing that will allow participants to securely exchange eHI. Ultimately, these smaller networks envision connecting to a larger, nationwide health information network that would support the sharing of eHI with entities in neighboring states and across the country.<sup>5</sup>

HIE offers health care organizations the potential to improve the quality and safety of health care by leaps and bounds. For example, the sharing of eHI will provide physicians with critical patient data at the point of care, reduce the duplication of medical services, and allow more meaningful public health reporting, bioterrorism surveillance, and clinical data analysis.<sup>6</sup> Indeed, the Bureau of Primary Health Care has encouraged health centers to adopt IT whenever practical so as to provide timely access to information and the capacity to communicate with other providers, agencies, and organizations.<sup>7</sup>

Nevertheless, HIE raises significant legal issues related to the privacy and security of medical information. For example, if a patient's medical information is inappropriately disclosed, then a health center may face penalties from the Federal government.<sup>8</sup> In addition, health centers and networks could be liable if a patient sustains injuries due to the disclosure of incomplete or inaccurate medical information.

To assist health centers and health center networks in structuring the exchange of eHI in ways that would address those legal concerns, this Information Bulletin:

- ◆ Discusses the issues raised by HIE under Federal privacy and security requirements for health information;
- ◆ Explains how potential liability for adverse events can result from HIE between health centers and network participants; and
- ◆ Describes strategies that health centers and health center networks can use to comply with Federal privacy and security requirements and manage potential liability associated with HIE.

---

5 In 2005, the U.S. Department of Health and Human Services awarded contracts to four groups of health care and health IT organizations to develop architecture prototypes for developing a Nationwide Health Information Network ("NHIN"). More information is available at [www.hhs.gov/healthit](http://www.hhs.gov/healthit).

6 J. Walker et al., "The Value of Health Care Information Exchange and Interoperability," *Health Affairs*, Jan. 19, 2005, available at <http://content.healthaffairs.org/cgi/content/full/hlthaff.w5.10/DC1>; Brailer, David J., "Interoperability: The Key to the Future Health Care System," *Health Affairs*, Jan. 19, 2005, available at <http://content.healthaffairs.org/cgi/content/full/hlthaff.w5.19/DC1>.

7 Bureau of Primary Health Care, Policy Information Notice 98-23 (Health Center Program Expectations), at 32.

8 This Information Bulletin addresses legal requirements under Federal law. State law may impose more stringent legal requirements, particularly as it relates to mental health information, alcohol and substance abuse treatment, and HIV/AIDS status.

---

## LEGAL ISSUES RAISED UNDER FEDERAL PRIVACY AND SECURITY LAWS

HIE can raise novel legal issues under privacy and security laws. For example, suppose two health centers establish an electronic communications portal so that each health center has access to the electronic medical records of the other. In general, privacy laws permit providers to share health information without first obtaining the patient's permission so long as the disclosure is for treatment purposes. In this case, however, each health center has allowed the other to access medical records of its patients without regard to the intended use of the information. As a consequence, patient information may be subsequently disclosed for activities that are not authorized under the relevant privacy requirements. Furthermore, if the health centers do not implement adequate precautions to safeguard the exchange of health information, then the portal may raise concerns under the relevant security requirements as well.

By understanding the legal framework that exists for health information, health centers and health center networks can structure sharing and safeguarding eHI to comply with applicable privacy and security requirements. In the example above, the health centers might have avoided the privacy and security issues altogether if they had not

given each other unfettered access to all of their medical records. For instance, the health centers could have limited disclosure to only the eHI needed for treatment purposes when a patient was seeking treatment at the other health center.

## Federal Privacy Requirements

### HIPAA Privacy Rule

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule governs the use and disclosure of a patient's individually identifiable health information (protected health information or PHI) and imposes administrative requirements for managing and tracking the disclosure of such information.<sup>9</sup> The Privacy Rule seeks not to impede the flow of health information but to ensure that an individual's PHI is properly protected in the process of delivering high quality health services and promoting public health.<sup>10</sup>

**Covered Entities** — Because the Privacy Rule is part of HIPAA's administrative simplification provisions seeking to require health care organizations to use standardized formats and codes to conduct claims transactions, HIPAA only applies to health care organizations which engage in certain electronic claims transactions. Such health care organizations are called "covered entities" and include the following:

- ◆ Health care providers that engage in electronic claims transactions,
- ◆ Health plans (that necessarily engage in claims transactions), and
- ◆ Health care clearinghouses that process or facilitate electronic claims transactions.

Health centers qualify as covered entities because they are health care providers (defined as persons or organizations that furnish, bill or receive payment for health care in the normal course of business) so long as they directly or indirectly submit electronic claims. In contrast, health center networks (if they do not independently meet the definition of a health care provider) would not qualify as a covered entity unless they engage in claims transactions. For example, if the network receives PHI as a health center's billing agent and is involved in the processing of claims, then it would likely meet the definition of a health care clearinghouse and qualify as a covered entity. Alternatively, if the network is a

risk-bearing entity (e.g., a health insurer or HMO), then it would be considered a health plan and qualify as a covered entity.

If a health center network does not qualify as a covered entity, then it is not directly subject to HIPAA's privacy requirements. However, the network may still need to comply with HIPAA's privacy requirements as a "business associate" if it provides a service on behalf of one or more health centers (which are covered entities) and the service involves the use of PHI. In such case, the covered entities must enter a specific agreement with the network called a business associate agreement. This agreement will specify the permitted uses and disclosure of PHI, prohibit all other uses and disclosures, and require safeguards for the protection of PHI.<sup>11</sup>

#### **Use and Disclosure of PHI** —

Unless authorized in writing by the individual, use and disclosure of PHI is prohibited except if it is for one of the allowed purposes under the Privacy Rule.<sup>12</sup> The three pri-

9 45 C.F.R. pt. 164 subpt. E. Protected Health Information (PHI) includes any information that can identify an individual, including demographic information, as well as any information for which there is a reasonable basis to believe it can be used to identify the individual. *Id.*

10 DHHS Office of Civil Rights Privacy Brief: *Summary of the HIPAA Privacy Rule* (May 2003) at p. 1.

11 The business associate agreement should also impose security requirements for safeguarding PHI.

12 It is worth noting that, although disclosures of PHI for treatment, payment and health care operations may be made without authorization, the Privacy Rule nevertheless permits (but does not require) the covered entity to obtain consent. *See* 45 C.F.R. § 164.506(b).

mary purposes that do not require a patient's authorization for disclosure of PHI are: (1) treatment; (2) payment, and (3) health care operations. However, even for disclosures of PHI for payment and health care operations, the Privacy Rule limits the circumstances under which PHI

may be used or disclosed without authorization. For example, under the "minimum necessary standard", a covered entity must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purposes of the use, disclosure, or request.<sup>13</sup>

Subject to appropriate business associate agreements with each health center, health center networks could support disclosures between health centers for treatment activities by providing the necessary HIT infrastructure to store and maintain an electronic health record system on behalf of the network's health centers. In this regard, the network would be functioning as a business associate to store health information created by a health care provider, and each health center, as a covered entity, would be permitted to use and disclose PHI to the network, as the health center's business associate, for treatment. Thereafter, pursuant to the terms of its business associate agreement, the network could redisclose PHI, on behalf of one health center to another health center that requested it for treatment purposes.

Furthermore, health center networks could take on additional roles related to quality improvement and assessment; population-based activities relating to improving health or reducing health costs; and care management and care coordination. Those activities fall within the definition of health care operations. A covered entity that participates in an "organized health care arrangement" may disclose PHI about an individual to another covered entity that participates in the organized health

### Activities for which Disclosure is Permitted without Written Authorization

**Treatment** means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers related to a patient; or the referral of a patient for health care from one health care provider to another.

**Payment** means the activities such as eligibility determinations, adjudication, risk adjustment, billing, claims processing, collection, and utilization review undertaken by: (1) a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits; or (2) a health care provider or health plan to obtain or provide reimbursement for the provision of health care.

**Health Care Operations** means any of the activities related to the covered entity's functions including quality assessment and improvement; population health activities, care management, and care coordination; professional competence and performance reviews, credentialing, accreditation, and licensing; health insurance underwriting, premium rating and benefits contracting; legal, medical, and audit services; and business planning, management and administration, including grievances, customer service, and development activities. In contrast, disclosures to or by request to a health care provider for treatment can be shared without regard to the minimum necessary standard. Consequently, health centers, as covered entities, may use and disclose PHI for their own treatment activities and those of other health care providers.<sup>14</sup> This would allow two health centers to establish an electronic communications portal to share electronic PHI so long as the information was disclosed (and used) for treatment activities only.

<sup>13</sup> 45 C.F.R. § 164.502(b)(2)(i).

<sup>14</sup> 45 C.F.R. § 164.506(c)(1)-(2).

care arrangement for any health care operations activities of the organized health care arrangement.<sup>15</sup> If a health center network qualified as an organized health care arrangement, then the health centers could disclose PHI to the network for any health care operations activities related to network, subject to the minimum necessary requirement.

## Health Center Implementing Regulations

Although the health center implementing regulations (42 C.F.R. § 51c.110) do not limit the purposes for which a health center may use patient information, the regulations do impose strict confidentiality requirements on disclosures of such information. The health center implementing regulations provide that patient information may not be disclosed without the patient's consent "except as may be required by law or as may be necessary to provide service to the individual, or to provide for medical audits by the Secretary [of DHHS] or his designee."<sup>16</sup>

In the context of sharing eHI, this means that the implementing regulations would probably only permit a health center to disclose eHI if the disclosure was necessary to provide care to a specific patient.

Consequently, even though the HIPAA Privacy Rule permits disclosures for payment and operations without authorization, those purposes would not be sufficient for disclosures under the implementing regulations. Unless the health center first obtained the patient's consent, the health center would need to show that the disclosure of eHI was necessary to provide service to the patient.

As a result, the implementing regulations may prevent health centers and health center networks, to the extent networks conduct activities on behalf of their health centers, from sharing eHI to conduct certain activities without obtaining patient consent. For instance, if two or more health centers desired to share eHI for the purpose of conducting quality improvement or other population health activities,

then the health centers would need to first obtain patient consent for those purposes.

## Other Privacy Laws and Regulations

Aside from privacy requirements under HIPAA and the health center implementing regulations, health centers and health center networks should be mindful that other Federal laws and regulations exist which may afford even greater privacy protections to eHI. For example, regulations known simply as "Part 2" provide special confidentiality protections to patient records maintained in connection with the performance of any Federally assisted alcohol and drug abuse treatment program.<sup>17</sup>

Because Part 2 is written in particularly broad language, health centers could find themselves subject to strict non-disclosure requirements. For example, Part 2 defines Federal assistance to include a recipient of funds even if those funds are not limited to the provision of substance abuse or alcohol treatment. In addition, a program may qualify as alcohol and drug treatment program under Part 2 even if it does not provide diagnosis or treatment but only refers patients for treatment.

Moreover, HIPAA does not preempt state privacy requirements that provide greater confidentiality protections to patients.<sup>18</sup> Consequently, health centers and health center networks may be subject to more stringent state laws that require consent prior to disclosure

15 45 C.F.R. § 164.506(c)(5). An "organized health care arrangement" includes an organized system of health care in which more than one covered entity participates and in which the participating covered entities: (i) hold themselves out to the public as participating in a joint arrangement; and (ii) participate in joint activities that include at least one of the following: (A) Utilization review; (B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or (C) Payment activities, if the financial risk for delivery health care is shared, in part or in whole, pay participating covered entities through the joint arrangement, and if PHI created or receive by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administrating the sharing of financial risk. *See* 45 C.F.R. § 160.103.

16 42 C.F.R. § 51c.110.

17 42 C.F.R. pt. 2.

18 45 C.F.R. pt. 164 subpt. E.

of certain health information. For example, some states have additional protections for information relating to sexually transmitted diseases, including HIV/AIDS, and alcohol and substance abuse treatment as well as for mental health records and genetic information.

## Federal Security Requirements

Recognizing that security is a necessary prerequisite for privacy, HIPAA requires covered entities to ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits.<sup>19</sup> Specifically, covered entities must protect against any reasonably anticipated threats or hazards to the security or integrity of such information and protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule.<sup>20</sup> Further, covered entities are required to ensure that its workforce complies with the security requirements.<sup>21</sup>

To safeguard confidentiality, the HIPAA Security Rule requires covered entities to take certain security measures to protect PHI.<sup>22</sup> In contrast to the Privacy Rule (which

simply requires covered entities to “reasonably safeguard” PHI as “appropriate”), the HIPAA Security Rule (which applies only to PHI in electronic form) establishes 43 categories of safeguards which must be implemented as “reasonable and appropriate” to protect PHI. These safeguards are not technical specifications but rather policies and procedures that seek to maintain the integrity of PHI and prevent a use or disclosure that is prohibited.

The Security Rule categorizes safeguards as administrative, physical, or technical. These safeguards arise from regulatory “standards” and the “implementation specifications”

which supplement the standard. Under the Rule, covered entities must use a flexible approach in implementing these safeguards, which takes into account:

- ◆ Size, complexity, and capability of the covered entity;
- ◆ The covered entity’s technical infrastructure, hardware, and software security capabilities;
- ◆ The costs of security measures; and
- ◆ The probability and criticality of potential risks to electronic protected health information.<sup>23</sup>

### Security Rule Safeguards

**Administrative Safeguards** are administrative actions, and policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity’s workforce in relation to the protection of that information.

**Physical Safeguards** are physical measures, policies, and procedures to protect a covered entity’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

**Technical Safeguards** means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

<sup>19</sup> 45 C.F.R. § 164.306(a)(1).

<sup>20</sup> 45 C.F.R. § 164.306(a)(2)-(3).

<sup>21</sup> 45 C.F.R. § 164.306(a)(4).

<sup>22</sup> 45 C.F.R. Part 164 Subpart C.

<sup>23</sup> 45 C.F.R. § 164.306(b).

To comply with the Security Rule's implementation specifications, health centers and health center networks are required to conduct a risk assessment to determine the threats or hazards to the security of PHI and implement measures to protect against these threats and such uses and disclosures of information that are not permitted by the Privacy Rule. These measures should include access controls that require the user's identity to be authenticated (*i.e.*, measures to confirm the user's identity), and that the user is authorized to receive PHI prior to any information being disclosed. On a regular and periodic basis, these measures should be audited to ensure that only permitted disclosures were made.

## MANAGING LEGAL RISKS CREATED BY HEALTH INFORMATION EXCHANGE

Health centers and health center networks, by virtue of their involvement in the exchange of eHI, are likely to observe deficiencies that currently exist in medical records systems as well as gaps in current standards for privacy and security of health information. This is not because eHI is qualitatively different from paper-based health information. Rather, it is because electronic data sharing will reduce the barriers to sharing health information, thereby increasing the rate in which such information is exchanged.

For example, HIE will allow a provider to obtain eHI almost

instantaneously from another provider. Contrast this to a paper-based system, where a provider may not have taken the time and effort to obtain the same health information. In a paper-based system, it was probably faster to repeat a test than to request the results of a previous one from another provider. Thus, providers who participate in a health information network are likely to request eHI, not only for urgent or emergency situations, but also in many routine situations where they would not have previously requested health information from another provider.

This additional sharing of health information will likely increase the exposure of health centers and health center networks to liability under Federal and state privacy statutes, state common law, and professional licensing agencies. To illustrate, this section explains how potential liability can result from HIPAA violations and medical malpractice actions.<sup>24</sup> Finally, this section will offer several strategies for minimizing exposures to liability.

## Sources of Legal Liability

### HIPAA

A violation of the HIPAA Privacy and Security rules can result from either of the following: (1) performing an act which is prohibited by HIPAA (*e.g.*, unauthorized disclosure) and (2) failing to perform an act which is required by HIPAA

(*e.g.*, implementation of security safeguards). Due to the sheer number of health information exchanges, health centers and health center networks that engage in electronic data sharing should expect some number of impermissible uses or disclosures of health information, despite reasonable efforts to prevent them.

Such HIPAA violations may result in the imposition of civil or criminal penalties. In regard to civil violations, the Office of Civil Rights (OCR), a component of the U.S. Department of Health and Human Services, investigates potential civil violations and, where appropriate, assesses penalties on covered entities. OCR has authority to assess up to \$100 per violation per day, with a maximum of \$25,000 per violation in any calendar year.

In addition, the U.S. Department of Justice investigates and prosecutes potential criminal violations. Criminal penalties may be imposed on a covered entity which knowingly obtains or uses PHI for a purpose not permitted under HIPAA, or knowingly obtains PHI by using a false identifier. Criminal penalties range from one year in prison and a \$10,000 fine per violation to up to 10 years in prison and a \$250,000 fine per violation.

Accordingly, it is essential for any health center that uses a network or some other third party to manage its eHI to determine, in advance, which party will be legally responsible (and liable for any fines) resulting from unauthorized use or dis-

<sup>24</sup> Aside from medical malpractice, there may be other sources of liability under state law based on privacy statutes, state common law, or through professional disciplinary actions.

closure. That decision may depend, in part, on which party is responsible for implementing privacy and security measures to prevent unauthorized use or disclosure. Because that party would be in the best position to manage the risk of unauthorized disclosure, it should probably be the one that is legally responsible for any fines arising from an impermissible disclosure.

## Medical Malpractice

Medical malpractice, based on a body of state law known as “torts”, occurs when a physician breaches the standard of care and that breach is found to be the proximate cause of an injury. The standard of care is often influenced by expert witnesses, whose dueling testimony describes the care that would be exercised by the average practitioner of the same specialty in the same situation. Tort law is state-specific, not Federal, and therefore each state can reach a different answer on the appropriate standard of care.

In some states, violating patient confidentiality requirements can also be grounds for a medical malpractice action or a professional licensure action. However, health centers, and health center networks (based on a theory of vicarious liability), may also face legal exposure to medical malpractice actions on the basis of how eHI is used (or fails to be used) in clinical decision-making.<sup>25</sup> Consider the following scenarios that arise from the use of electronic medical records:

**Scenario # 1:** A patient’s electronic medical record is disclosed to a physician but the record omits certain key information about a patient’s drug allergies. The patient sustains injuries. Did the physician that created the electronic medical record have a duty to provide accurate and complete information?

**Scenario # 2:** A patient’s electronic medical record identifies the patient’s drug allergies but the treating physician neglects to consult it. The patient sustains injuries. Did the treating physician have a duty to consult the patient’s electronic medical record?

The first scenario presents the legal question of whether there is a duty to provide accurate and complete medical records. Given the lack of uniform requirements for medical record keeping, health center and health center networks should consider adopting their own standards for maintaining the accuracy of eHI. This may involve implementing certain processes to ensure that the medical records are kept up-to-date and that known health risks, if relevant, are displayed prominently on eHI disclosed to other providers. At the same time, it may be helpful to include a reminder with eHI dis-

closed to other providers that a patient may have additional health risks that are not mentioned or included on the disclosed eHI.

The second scenario presents the legal question of whether there is a duty to consult available medical records. Courts have issued mixed opinions.<sup>26</sup> As a result, health centers should consider adopting internal procedures addressing when it is appropriate to request eHI from other providers and whether such eHI must be reviewed and acted upon. Many providers already have systems in place to ensure that the results of laboratory tests and other diagnostic tools are reviewed in a timely fashion. As HIT adoption increases among providers, the standard of care may evolve to include a duty to consult eHI.

## Strategies for Minimizing Legal Risks

This section provides key strategies that can be used by health centers and health center networks to manage the legal risks associated with sharing eHI. Ideally, these strategies would be implemented prior to forming networks to share eHI with other health centers and providers. These strategies include the following:

<sup>25</sup> Health centers that receive federal grant funds are eligible for medical malpractice coverage under the Federal Torts Claim Act.

<sup>26</sup> Compare *Primus v. Galgano*, 329 F.3d 236 (1st Cir. 2003) with *Suniga v. Eyre*, 2004 WL 16839 (Tex. App. Jan. 21, 2004) and *Susnis v. Radfar*.

## Address legal issues during the formation and organization of the network.

There is broad variation among health organizations in interpreting and applying Federal and state privacy and security requirements. According to a recent national study, there is particular variation regarding the application and interpretation of consent requirements.<sup>27</sup> This is due to a misconception that the Privacy Rule requires patient consent for disclosure for treatment purposes, differing state laws (some of which require consent to disclose health information in all circumstances), professional ethical obligations to obtain patient consent, and organizational decisions to require consent as a measure to reduce risk of liability for wrongful disclosure.<sup>28</sup>

Because the interpretation and application of privacy and security requirements will influence the technical processes for sharing eHI, reconciling differing interpretations of legal requirements should occur early on in the formation of a health information network. In our experience, it is far easier to integrate privacy and security protections into a developing network than to incorporate protections into an established network.

To this end, state privacy laws should be reviewed by legal counsel and, if there is ambiguity, interpretations should be confirmed with appropriate state regulators and licensing boards. These requirements should then be integrated with HIPAA and other applicable

Federal requirements, such as the health center implementing regulations. Finally, these requirements should be compared with any organizational commitments to increase privacy protections (such as a health center's own privacy policies) and measures to reduce the risk of liability.

Once the applicable privacy and security requirements are addressed, health center and health center networks may wish to attempt to simplify them (consistent with privacy protections) so that a clearer framework can be used for establishing the system specifications of the HIT network. For example, one of the most challenging issues relates to implementation of the Privacy Rule's minimum necessary standard, in which a covered entity must establish policies to limit information used and disclosed to that which is reasonably necessary for the purpose. However, the Privacy Rule explicitly exempts this standard from applying to uses and disclosures to providers for treatment purposes. Consequently, health centers and health center networks may decide to implement one process for disclosures of eHI related to payment or operations and another process for disclosures for treatment purposes.

## Obtain buy-in from all stakeholders, including consumers.

Although the legal requirements set parameters for many decisions, health centers and health center networks will still need to resolve many issues on their own, such as when HIPAA permits covered entities to obtain consent, but does not actually require it. In making those decisions, it is a good idea to consult stakeholders—which would include any individual or organization that could be adversely affected by the disclosure (or lack of disclosure) of eHI. Here, stakeholders may include patients, clinical staff, health centers, primary care associations, community providers, hospitals, and managed care organizations.

These stakeholders should be consulted in the process of establishing the health information network. By carefully addressing the concerns raised by stakeholders, not only will the process improve managing disclosures of eHI, but it will build trust, knowledge, and understanding and provide a source of public support. If, at some point, an impermissible disclosure of eHI occurs, stakeholders can help withstand the negative attention and reaffirm the benefits of establishing a network to store and manage eHI.

27 DHHS, Agency for Healthcare Research and Quality, "Privacy and Security Solutions for Interoperable Health Information Exchange: Assessment of Variation and Analysis of Solutions," June 30, 2007, at 3-1. This report was a summary of 34 separate reports on the major areas states have identified as presenting challenges to the privacy and security of electronic health information exchange and potential solutions to those issues.

28 *Id.*

One of the stakeholders should be the patients of the health centers. Because health centers are governed by a consumer majority, it will be somewhat easier for health centers and health center networks to seek the opinions of patients. However, because patients will change over time, it is essential that new patients of health centers become aware that the health center participates in HIE or a network and that the patient's health information may be shared with other health care providers.

Consequently, health centers and health center networks may wish to consider obtaining patient consent, even if not required under applicable legal requirements. To this end, health centers participating in a HIE, HIN, or other network that shares eHI may want to develop a common notice of privacy practices (NPP) that informs patients that the health center will disclose certain eHI to third parties and other health care providers.

At a minimum, the NPP should address:

1. A Record Locator System,<sup>29</sup> if applicable;
2. Notice of the provider's participation in a health information network;
3. *General* consent to disclose eHI to other providers;
4. *Specific* consent to disclose specific eHI to specified providers;
5. Specific types of records (*e.g.*, HIV, mental health, and substance abuse records); and
6. Patient requested restrictions.

### Develop formal data sharing agreements.

Many of the legal risks and perceived legal barriers can be addressed through the use of formal data sharing agreements between health centers and the health center network. The agreements should address privacy and security requirements, ownership or licensing of eHI, and liability.

In particular, the data sharing agreements should define the authorized uses of eHI obtained from the network. This may depend on whether the eHI involves the health center's own PHI, whether it involves disclosure of eHI to another provider, and whether that other provider is a network participant. For example, if the eHI involved the health center's own PHI, then, as its business associate, it could disclose eHI back to the health center for any allowed purpose. In contrast, if the eHI involved disclosure to another non-network provider, then it could only make the disclosure for treatment purposes.

Although the health center network will likely be developing the privacy and security standards on behalf of the health centers, the data sharing agreement should include a proper business associate agreement between the network and each health center. This will require the network to use or disclose eHI consistent with the Privacy Rule and under the terms of the network's data sharing agreement.

Most importantly, the data sharing agreement should determine which party will be responsible for certain types of unlawful or negligent conduct. From an economic perspective, loss should be allocated to the party in the best position to prevent or deter it. If the network "houses" the eHI and implements privacy and security safeguards related to it, then the network is probably in the best position to prevent HIPAA violations related to impermissible disclosures. Accordingly, the network may be the appropriate party to be responsible for HIPAA violations.

In contrast, the health centers (or more precisely, the health centers' providers) will create and receive eHI. Consequently, the health centers are probably in the best position to develop standards for medical records and to ensure the accuracy and completeness of any disclosed eHI. Additionally, health centers are best positioned to manage their internal procedures for ensuring that eHI is consulted and acted upon. Thus, the individual health centers may be the appropriate party to be responsible for negligent conduct or medical malpractice arising from the use or failure to use eHI.

### Actively manage the security of shared eHI.

To ensure that a health center network that shares eHI does not place its members at risk of violating

<sup>29</sup> A Record Locator System is a system that manages patient identity and allows a provider to locate another provider who has a medical record associated with a specific patient. Even if the provider does not disclose the patient's medical record, a provider must still disclose the patient's name and other identifying information to create a searchable record within the locator system, thereby involving disclosure of PHI.

licensure or other regulatory requirements, the network (in collaboration with its participating health centers) should adopt standards for privacy and security on behalf of the health centers. These standards should fully comply with the standards and implementation specifications of the HIPAA Security Rule, covering all 43 categories of safeguards described in the Rule.

Because written standards do not implement themselves, however, the network will likely be legally responsible for managing and implementing those safeguards. To satisfy these legal obligations as well as to provide the maximum protection to its members, the network should take an active role in managing the network's security. To this end, it may be useful to view the network's role across four functional areas: (1) Managing User Identity and Authentication; (2) Access Controls; (3) User Training; and (4) Auditing and Monitoring Access and Disclosures.

**Managing User Identity and Authentication** — The network should have a process for identifying health center staff who may become authorized users and access eHI on the network. These individuals may include not only physicians but also other clinical staff (e.g., physician assistants, nurse practitioners, nurses). Thereafter, there must be a process for “authorizing” such users by which they are given passwords and methods are established for authenticating their identities from various points of access to the network for eHI.

**Access Controls** — The key objective of access controls relate to ensuring that only authorized users can access eHI. This requires secure transmission of eHI that protects the data in transit from inappropriate interception or modification. In addition, access controls relate to restricting or limiting an authorized user's access to certain eHI contained in the patient's medical record. For example, a patient's mental health records may be screened off unless the patient has given specific consent for disclosure to specified providers. To limit disclosure, some currently available technologies used to manage eHI can segregate certain types of data so that it is screened off from particular users.

**User Training** — In an environment of eHI, it is easy to overlook appropriate administrative and physical safeguards that have nothing to do with technology. However, the lack of such safeguards, particularly within health care organizations, can not only present significant security and privacy risks, but also create mistrust among patients and increase liability concerns. To this end, user training ensures that users understand their responsibilities for controlling access to eHI, follow policies to safeguard passwords and prevent unauthorized access to eHI, and know how to transmit information securely to patients and other health care providers.

**Auditing and Monitoring Access and Disclosure** — Auditing and monitoring access and disclosure

involves the development and regularly scheduled use of an appropriate audit program that addresses potential privacy and security risks and is based on an established set of audit criteria that match the organization's needs. In other words, it requires the network to recognize its own vulnerabilities for ensuring privacy and security and then audit those areas retrospectively to determine if any individuals or organizations accessed information contrary to the network's standards for ensuring privacy and security.

---

## CONCLUSION

The Bureau of Primary Health Care expects health centers to have medical records systems that, while protecting patient confidentiality, promote documentation and support the delivery of quality health care.<sup>30</sup> Health information technology, such as electronic health records, can improve health care quality, reduce unnecessary duplication of medical services, and support the delivery of coordinated health care.

To this end, health center networks can support health centers in adopting HIT and developing standards for HIE. Furthermore, by adopting the strategies described in this Information Bulletin, health center networks can assist health centers in the critically important task of managing the legal risks and maintaining the privacy and security of electronic health information.

---

<sup>30</sup> Bureau of Primary Health Care, Policy Information Notice 98-23 (Health Center Program Expectations), at 20.



National Association of Community Health Centers, Inc.®

7200 Wisconsin Avenue, Suite 210

Bethesda, MD 20814

Telephone: 301-347-0400

Fax: 301/347-0459

Website: [www.nachc.com](http://www.nachc.com)