The IOM New Health System and HIPAA: Same Sheet of Music?

Nancy Grey Stetson, BSN, MA, RN, FHIMSS

ABSTRACT

HIPAA and the IOM New Health System may be singing the same song, but there are some flat notes in a few verses. The HIPAA Privacy rules are the area where there is the most opportunity to sing in unison, but the need for data collection, storage, and dissemination required in the IOM New Health System warrants significant discussion and planning in the HIPAA preparation to bring the two into harmony.

KEYWORDS
HIPAA
IOM New Health System
Privacy
Protected Health Information (PHI)
Information technology
Electronic medical record
Workflow process
Delivery of healthcare process

In the midst of finalizing the HIPAA Privacy rules, the Institute of Medicine (IOM) report, Crossing the Quality Chasm: A New Health System for the 21st Century, was issued. What this means is that two major initiatives to, at a minimum, improve the effectiveness and efficiency of the healthcare system in the United States will need to be accomplished before the end of this decade. This article explores where these initiatives are similar, where they are diverse, and how they can be implemented at the same time.

On first reading the executive summary of this most recent IOM report, I was struck with the following thoughts:

- The IOM New Health System is primarily clinically focused, whereas HIPAA is primarily financially focused. These areas are not normally considered together or by the same stakeholders for major planning or implementation initiatives. There is a concern that we will go down the HIPAA path (since its implementation dates start earlier than the IOM New Health System) and find that we have to rework some areas to accomplish the IOM initiatives.
- The IOM New Health System projected implementation needs should be incorporated into the HIPAA readiness assessment and gap analysis.
- The IOM New Health System is heavily information technology (IT) driven, and HIPAA is heavily process driven. Information system purchases, modifications, or upgrades need to be considered early on for the IOM New Health System.

History of the Initiatives

HIPAA really has as its roots the healthcare reform activities of the...
Original Contributions

early 1990s, where there was an impetus to utilize health maintenance organizations to lower cost, increase and simplify access to care, and improve the quality of care. There was a major push for preventative programs, such as mammography, to monitor and maintain a state of health. Part of this healthcare reform initiative was to reach out to the population as a whole, not just the sick population. The healthcare reform efforts grew into the Health Insurance Portability and Accountability Act (HIPAA) of 1996. What we currently refer to as HIPAA is really the Administrative Simplification portion of the HIPAA legislation (Title II, Subtitle F). “The administrative simplification part of HIPAA is aimed at reducing administrative costs and burdens in the healthcare industry by adopting and requiring the use of standardized, electronic transmission of administrative and financial data.”

The IOM’s Committee on the Quality of Health Care in America was formed in June 1998 to develop a strategy that would lead to a substantial improvement in the quality of healthcare over the next 10 years. Its charge was based on the growing concern that the healthcare delivery system itself needs to be changed to deliver safe, quality care based on scientific knowledge. In his opening statement at a Public Briefing on March 1, 2001, William Richardson, president, W. K. Kellogg Foundation, and chair, Committee on Quality of Health Care in America, summed it up: “Between the care we have and the care we could have lies not just a gap, but a wide chasm.”

Major Premise

Both HIPAA and the IOM New Health System have improving the effectiveness and efficiency of the healthcare system in the United States as a basic premise.

The HIPAA initiative is to improve efficiency and effectiveness of the healthcare industry by:
- Protecting the security and privacy of transmitted information
- Reducing paperwork
- Reducing overall cost of healthcare by standardization of code sets and transactions

The IOM New Health System initiative is to improve the healthcare system as a whole by concentrating on six key aims. Healthcare should be:
- Safe
- Effective
- Patient-centered
- Timely
- Efficient
- Equitable

While the premise is the same — effective and efficient — the approach for each is very different. HIPAA has financial aspects as its basic foundation, while the IOM New Health System has the clinical delivery of care as its foundation. This is the first area where there is some discordance in this songbook. Early in its executive summary, the IOM New Health System report states: “What is perhaps most disturbing is the absence of real progress toward restructuring healthcare systems to address both quality and cost concerns...”

“\textit{What is perhaps most disturbing is the absence of real progress toward restructuring healthcare systems to address both quality and cost concerns...}”

While the overall strategic plan for the organization might call for an automated tool to enhance operations, the same project teams do not always perform clinical and financial system selections. There is a strong possibility that an organization will implement solutions to become HIPAA compliant without regard to the clinical solutions needed to address the IOM New Health System initiative. This will be an expensive and time-consuming endeavor, with much duplication of effort if the organization will indeed need additional tools to address the clinical issues. It would behoove organizations to take the IOM New Health System initiative into account when performing their HIPAA assessment and gap analysis.

Examples to Consider in Preparing for HIPAA and the IOM New Health System

The IOM recommendations section below and Figure 1 detail the IOM New Health System recommendations along with their HIPAA implications. The following are a few examples of items to consider.

\textit{Computer-based Patient Records (CPR).} While the IOM New Health System does not mandate the implementation of a full-blown CPR, it very much embraces the need for a strong technological infrastructure. In preparing for HIPAA, a healthcare organization may invest a substantial amount of effort developing or revising its policies and processes to protect information, for instance, in the paper record. This same organization may realize that, in order to support IOM, it will be necessary to implement some form of an electronic medical record to assist in the collection and communication of Protected Health Information (PHI), for example, for the IOM-identified chronic conditions.

\textit{Consents.} The development and implementation of consent forms is an expensive and time-consuming process. In order to be HIPAA compliant, consent forms have to address how organizations will protect and disclose PHI. The patient must acknowledge their understanding of how their PHI will be used by the organization. For the IOM New Health System, this PHI will be the source for evidence-based care processes to affect the outcomes of that care, in particular for the identified focused chronic conditions. The consent form needs to address the disclosure of PHI for both treatment and outcomes purposes.

Additionally, there is a real risk of HIPAA noncompliance by identifying...
the patient population with chronic diseases for IOM. This alone could open a legal, as well as an associated monetary, barrier to compliance with HIPAA and the IOM New Health System. Organizations will, in effect, be singling out certain patients — whether by ICD-9 or DRG code or some other diagnostic indicator — for inclusion in this data collection. The organizations need to decide if these people will be required to sign a separate consent to utilize their PHI for IOM purposes.

**Release of Information.** The very act of collecting data for the IOM New Health System and using it for outcomes generation and management is in conflict with the HIPAA Privacy rules, particularly in regard to the HIPAA requirement to de-identify PHI. A significant portion of the data elements that HIPAA considers to be identifiable is demographic in nature. De-identifying the data to comply with HIPAA may impact the value of the information for evidence-based clinical decision making.

Organizations will also need to consider the PHI for the IOM requirements in defining their minimal necessary release of information policies and procedures for HIPAA. Who's going to get it? What are they going to get? What authorizations or consents do they need? Whose responsibility is it to get the authorization?

**Decision Support.** It is very likely that organizations will need to implement clinical decision support tools to assist in gathering, interpreting, maintaining, and generating outcomes information for the IOM New Health System requirements. It is probable that, if any decision support tools are to be utilized to comply with HIPAA regulations, they will be financial in nature, and not the same as those used for clinical decision support. This again is an area for organizational strategic planning to include needs for both IOM and HIPAA early on. It may be necessary to perform a system selection for one or both of these tools. While the IOM New Health System recommendations state the desire to integrate the clinical and financial support systems, it will be imperative to plan at a minimum for the interaction of an organization's core systems with both.

**IOM Recommendations**

The IOM has embraced the 1998 Advisory Commission on Consumer Protection and Quality in the Health Care Industry in its 13 recommendations for improving the healthcare system in this country in the 21st century. While we have had some time to begin to plan for implementing HIPAA, the IOM New Health System was only recently introduced. Let's take a look at these IOM recommendations in the light of the HIPAA rules.

**Recommendations 1, 2, and 3.**

Improve the health and functioning of the people of the United States with the six major aims of safe, effective, patient-centered, timely, efficient, and equitable healthcare. To assess the progress on these aims, the Department of Health and Human Services (HHS) is to establish monitoring and tracking processes. To achieve this, data will need to be collected and monitored. This collection and monitoring would fall under the HIPAA Privacy rules of Protected Health Information (PHI). De-identifying the data to comply with HIPAA may impact the value of the data for evidence-based clinical decision making.

**Recommendation 4.** The IOM has set rules to guide the healthcare system redesign:

- Continuous healing relationships. Patients should have access to care “24/7” over the Internet, by telephone, and by other means, in addition to face-to-face visits. HIPAA Privacy and Security rules need to be considered here.

---

**Figure 1. The IOM New Health System & HIPAA Comparison**

<table>
<thead>
<tr>
<th>IOM RECOMMENDATION</th>
<th>HIPAA IMPLICATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1, 2, and 3 – Establishing 6 Aims: Safe, Effective, Patient-Centered, Timely, Efficient, and Equitable</td>
<td>Privacy Rules</td>
</tr>
</tbody>
</table>
| #4 - Rules to Guide the Healthcare System Redesign | • Privacy Rules  
• Security Rules  
• Privacy: Consents  
• Privacy: Amendments  
• Privacy: De-identification  
• Non-IT Focus  
• Privacy: Minimum Necessity |
| #5 – 15 Priority Conditions | • Non-IT Focus  
• Privacy Rules |
| #6 - Health Care Quality Innovation Fund | • Privacy Rules  
• Security Rules  
• Privacy: Minimum Necessity  
• Privacy: Business Associate  
• Transaction & Code Sets |
| #7 – Challenges | • Privacy Rules  
• Security Rules  
• Privacy: Minimum Necessity  
• Privacy: Business Associate  
• Non-IT Focus |
| #8 – Evidence-based Care | • Privacy Rules  
• Security Rules  
• Privacy: Business Associate  
• Transaction & Code Sets |
| #9 - Eliminate Handwritten Clinical Data by the End of the Decade | • Non-IT Focus |
| #10 - Examine Current Payment Policies | • Transaction & Code Sets  
• Privacy Rules |
| #11 - Develop Payment Method Options that Support Quality Improvement | • Transaction & Code Sets  
• Privacy Rules |
| #12 & 13 - Preparing the Workforce | • Privacy Rules |
• Care will be customized, based on patient needs and values. This customization would need to be addressed with HIPAA-compliant consents.

• The patient will maintain control over healthcare decisions that affect them. From a HIPAA perspective, this control may not be able to be accomplished even with the consent process and the amendment rights. There are also privacy concerns here regarding the release of information affecting the quality of care: either being withheld at the patient’s request or disclosed by the caregiver without the patient’s approval.

• Patients should have access to their own medical information and to clinical knowledge. This is addressed in the HIPAA Privacy rules.

• Clinical decisions should be evidence-based. As in recommendations 1 through 5 above, evidence-based data are dependent on collection and evaluation of data, which falls under the HIPAA Privacy rules of PHI. De-identifying the data to comply with HIPAA may impact the value of the data for evidence-based clinical decision making.

• The care system should be safe. IT will play a large role in increasing patient safety. A recent article in Advance for Health Information Executives states, “The need to reduce medical errors is among one of the primary influences of the acceptance and implementation of EMRs. EMRs can help reduce mistakes in transmitting doctors’ orders and warn of drug interactions — the most common errors...” William Bates, MD, president and CEO of BAI Clinical Software, said in this article, “The intrinsic benefits of EMRs alleviate physician frustrations with paper-based methods including concerns with legibility, inability to access records remotely, inefficiency, and an inability to look at patient trends....”

HIPAA differs from the IOM in that, with the exception of the Transactions and Code Sets and some portions of the Security rules, HIPAA is not IT dependent. HIPAA addresses privacy in all media, not just electronic. But a major premise in the IOM report is that IT has to be employed for the initiative to be successful. Specific to EMR (electronic medical records), the IOM New Health System report says, “A fully electronic medical record, including all types of patient information, is not needed to achieve many, if not most, of the benefits of automated clinical data. Sizable benefits can be derived in the near future for automating certain types of data, such as medication orders.”

With this approach — automating certain types of data — there are some risks to consider:

• Who decides which data are to be automated?

• If these data fall under the HIPAA de-identifiable data elements, how do you get the data you need without jeopardizing the patient’s PHI?

• Automating only portions of the data can lead to fragmentation and inconsistencies — two undesirable outcomes.

From a software developer’s perspective, I would project that one of two possibilities will occur: a resurgence of the Computer-based Patient Record (CPR) efforts, which began in the early 1990s with the first IOM report The Computer-Based Patient Record: An Essential Technology for Health Care, or a proliferation of niche software automating various portions of the patient record, to a large extent based on the expertise of the developer (e.g., lab management information system developers focusing on lab results).

Even though the HIPAA rules do not call for automating the patient record, there are beginning to be instances where this is indeed occurring. The North Carolina Healthcare Information and Communications Alliance (NCHICA) has adopted “The Paperless Person-Centered Health Records Resolution.” NCHICA took this route because it feels that utilizing a paperless record will assist patients in accessing their health information. NCHICA also feels that this resolution will enhance communication between providers in a secure manner.

• The health system should make information available to patients and their families that allows them to make informed decisions. If this information is regarding how a health plan is performing, there may be HIPAA privacy implications if the data are gathered from patient identifiable information.

• The health system should anticipate patient needs. This, too, would be a privacy issue — knowledge of previous desires is required to anticipate needs, and this means collecting PHI data in some fashion.

• The health system should not waste resources or patient time. Both HIPAA and IOM are interested in increasing efficiency and effectiveness.

• There should be more cooperation among clinicians to ensure an appropriate exchange of information and coordination of care. The HIPAA minimum necessity portion of the Privacy rules addresses this need, and there may be a business partner agreement concern here as well. But the IOM report also states, “Personal health information must accompany patients as they transition from home to clinical office setting to hospital to nursing home and back.” This is a security consideration as well as a privacy concern from a HIPAA perspective.

**Recommendation 5.** To effectively implement these guidelines, the IOM committee recommends concentrating on the top 15 chronic conditions that affect the U.S. population. The committee feels that “Carefully designed, evidence-based care processes, supported by clinical information and decision support systems, offer the greatest promise of achieving the best outcomes from care for chronic conditions.” This is a key differentiation between HIPAA and the IOM: IOM is heavily dependent on IT to achieve its objectives, whereas, with the exception of the Transaction Sets and portions of the Security rules, HIPAA
is not IT intensive. IT tools will be essential to monitor, track, and determine resource usage (personnel and healthcare dollars) to identify areas to substantially improve quality in these 15 chronic conditions.

There are HIPAA privacy concerns here in regard to gathering the necessary data.

**Recommendation 6.** The IOM committee recommended that Congress establish a Health Care Quality Innovation Fund — $1 billion over three to five years — to support projects that communicate the need for rapid and significant change in the healthcare system and to help initiate the transition.\(^{13}\) There are no particular HIPAA implications with this recommendation.

**Recommendation 7.** The Agency for Healthcare Research and Quality has been asked to develop workshops to explore the challenges that organizations will need to address to meet the quality initiative:\(^{14}\)

- Redesign care processes for coordinated care across the care settings — from a HIPAA perspective, this is a privacy as well as a security issue.
- Improving the information infrastructure to ensure communication of individual PHI to clinicians who need it. This is a HIPAA privacy issue with specific consideration to be given to the minimum necessity portion of the Privacy rules. Who is to decide what kind of information is to be communicated to what party to ensure the patient’s condition is adequately represented to effect maximum quality resolution? There are also potentially Business Associate implications depending on the relationship between the infrastructure owner and the infrastructure supplier.
- Training and certification for users — not only from an information systems perspective, but also from a culture and knowledge-base viewpoint. Both HIPAA and the IOM New Health System require that attention be given to training.
- Coordination of care across the continuum. This is another area where the IOM New Health System will utilize IT tools such as the Computer-based Patient Record (CPR) and the Internet to ensure that patient data are accessible to those persons who need and are authorized to have the data. HIPAA may impact this coordination effort with security and privacy restrictions.
- Enhancing the effectiveness of teams. Team practice has been a methodology for patient care for a number of years, but it is usually discipline-specific (nursing, respiratory care, etc.). What is needed to improve the quality of the healthcare delivery system is a care system where care is a team effort. Communication of the care practices, whether automated or electronic, will fall under the HIPAA Privacy, Security, and, potentially, Transaction and Code Sets rules.

**Recommendation 8.** Currently there are inconsistencies in what is believed to be best practices and how these best practices are communicated to clinicians and patients. In its report, the IOM has recommended that the secretary of HHS, in cooperation with the public and private sector, establish a comprehensive program aimed at making scientific evidence more useful and accessible to clinicians and patients. The IOM committee expects that the program will focus on the identified priority conditions. In addition, it will include ongoing analysis of the medical evidence, identification of best practices, development of decision support tools to assist clinicians and patients in applying the evidence, and development of quality measures.\(^{15}\)

The data to feed the clinical decision support tools will depend upon PHI to build enough information to make decisions. This PHI falls under the HIPAA Privacy rules. The guidelines and best practices will need to follow the HIPAA Security and Privacy rules, and may potentially require a Business Associate agreement. It is to be expected that the Internet will play a significant role in the communication of, and as a resource for, evidence-based guidelines. The U.S. government, as well as HIPAA, is addressing concerns around privacy and the use of the Internet. Measuring quality and outcomes is also a privacy issue, as well as having the infrastructure and security to support these functions.

The IOM committee has stated, “The development and application of more sophisticated information systems is essential to enhance quality and improve efficiency.”\(^{16}\) The committee goes on to say that these information systems must bring together financial, clinical, and administrative transactions to achieve patient safety through decreasing and/or preventing errors, an outcome of which will be positively influencing the confidence that the U.S. population has in their system of care. As mentioned before, the emphasis on technology and infrastructure is a key differentiation between HIPAA and the IOM report.

**Recommendation 9.** Utilize a strong information infrastructure to eliminate most handwritten clinical data by the end of the decade. It is this presumption that strikes at the difference between HIPAA and the IOM report. Even in the Transaction standards, there is nowhere that HIPAA takes for granted that all information sharing will be done electronically. It only mandates that if transactions are electronic, they must follow the HIPAA standards. It is in this recommendation that there is the biggest opportunity for risk between HIPAA and the IOM New Health System.

There is a strong possibility that an organization will implement solutions to become HIPAA compliant without regard to the clinical solutions needed to address the IOM New Health System initiative. This will be an expensive and time-consuming endeavor, with much duplication of effort if the organization will indeed need additional tools to address the clinical issues. It would behoove organizations to take the IOM New Health System initiative into account when performing their HIPAA assessment and gap analysis. At this point, a decision can be made as to whether or not an automated system selection is going to need to take place, either for HIPAA, for IOM, or for both. Planning for both together rather than one at a time only makes good business sense. In order for this planning to occur, the right players need to be made aware that the HIPAA and IOM initiatives are concurrent endeavors.


**Recommendation 10.** Examine current payment policies. “The current healthcare environment is replete with examples of payment policies that work against the efforts of clinicians, healthcare administrators, and others to improve quality.” The IOM committee suggests that payment methods should give providers the chance to share in the benefits of quality improvement. The methods should also encourage healthcare providers to measure and disclose quality information; consumers can then use this information to choose the provider that best meets their needs. This recommendation will be directly impacted by the HIPAA Transactions Sets, as well as the collection and dissemination of PHI from a privacy perspective.

**Recommendation 11.** Centers for Medicare and Medicaid Services (CMS) and the Agency for Healthcare Research and Quality will develop payment method options that support quality improvement. This recommendation will also be directly impacted by the HIPAA Transactions Sets, as well as the collection and dissemination of PHI from a privacy perspective.

**Recommendations 12 and 13.** Preparing the workforce to perform in the new healthcare system. The committee recommends that “a multidisciplinary summit of leaders within the healthcare professions should be held to develop strategies for restructuring clinical education, and to assess the implications for provider credentialing programs, funding, and sponsorship of education programs for health professionals.” They also recommend that the Agency for Healthcare Research and Quality provide funding to assess how regulatory and legal systems can be modified to support the changes needed for the new 21st century healthcare delivery system and for the caregivers and the organizations that will be implementing these initiatives. Inherent in the HIPAA rules are adjustments to processes to increase efficiency. This will also require training and change management to incorporate these modifications into the daily workflow.

**So, are the IOM New Health System and HIPAA on the same sheet of music?**

Based on the discussions above, it seems that HIPAA and the IOM New Health System are singing the same song, but with some flat notes in some verses. Clearly, the HIPAA Privacy rules are the area where there is the most opportunity to sing in unison. But the need for data collection, storage, and dissemination required in the IOM New Health System warrants significant discussion and planning in the HIPAA preparation to bring the two into harmony.

**IT Tools and Infrastructure.** A discordant area is in the level of need for IT tools and infrastructure. The IOM New Health System is heavily dependent on IT to achieve its objectives, whereas, with the exception of the Transaction Sets and portions of the Security rules, HIPAA is not IT intensive. IT tools will be essential to monitor, track, and determine resource usage (personnel and healthcare dollars) in the IOM initiatives. The IOM New Health System will utilize IT tools such as the Computer-based Patient Record (CPR) and the Internet to ensure that patient data are accessible to those persons that need and are authorized to have the data.

A key initiative of the IOM New Health System is improving the information infrastructure to ensure communication of individual PHI to clinicians who need it, and to patients who request it. The IOM New Health System will utilize a strong information infrastructure to eliminate most handwritten clinical data by the end of the decade. Even in the Transactions standards, there is nowhere that HIPAA takes for granted that all information sharing will be done electronically. It only mandates that if transactions are electronic; they must follow the HIPAA standards.

**HIPAA and the IOM New Health System Solutions.** Establishing this strong IT infrastructure with the tools to support it is where there is the biggest opportunity for risk between HIPAA and the IOM New Health System Report. There is a strong possibility that an organization will implement solutions to become HIPAA compliant without regard to the clinical solutions needed to address the IOM New Health System initiative. This will be an expensive and time-consuming endeavor, with much duplication of effort if the organization will indeed need additional tools to address the clinical issues. It would behoove organizations to take the IOM New Health System initiative into account when performing its HIPAA assessment and gap analysis. At this point, a decision can be made as to whether or not an automated system selection is going to need to take place, either for HIPAA, for IOM, or for both. Planning for both together rather than one at a time only makes good business sense. In order for this planning to occur, the right players need to be made aware that these initiatives are concurrent endeavors.

**Strategies for Accomplishing Both Within the Same Time Frame**

To a large extent, the strategies that an organization employs depend on that organization’s culture. The following are some guidelines to consider:

**Planning for HIPAA and the IOM New Health System.**

Throughout this article, there is the recommendation to include the IOM New Health System initiative in the planning for HIPAA. Ideally this would be done at the very beginning of the preparation for HIPAA implementation. But, by the time that this article is published, many, if not most, organizations will be completing their HIPAA assessment, gap analysis, and policy and procedure review, at least for the Transaction and Code Sets.
rules. My recommendation is to include the IOM New Health System initiatives in the gap analysis and subsequent presentation to the executive committee. Identify and engage a clinical champion who has been involved with the medication error and safety initiative to participate in this presentation. Reviewing policies and procedures for the HIPAA Privacy rules will be another opportunity to bring clinicians into the mix.

Incorporating Both Initiatives into the Organizational and Information Systems Strategic Plans. More than likely, the HIPAA implementation was incorporated into the organization’s, and perhaps the information systems’, short- or long-term strategic plans. But it is just as likely that the IOM New Health System initiative was not part of these plans, although the IOM safety initiatives may have been. From an organizational perspective, the impetus for the IOM New Health System will most likely come from the clinician or compliance arenas. HIPAA will come from the financial side of the organization, at least for the Transactions Sets. The IS strategic plan will more likely address primarily the HIPAA Security rules. These areas are not normally considered together or by the same stakeholders for major planning or implementation initiatives.

The challenge is to get these players together to form a plan that will meet the overall needs of the organization as well as the patients (and employees) it serves. One method to accomplish this is to have multidisciplinary representation on the various committees that develop the strategic plan. Seek out and engage or several clinician champions who are aware of the issues regarding delivering safe, effective, and quality care. Encourage their participation in an initiative that directly impacts the care delivery system, e.g., revising the consent forms for HIPAA.

Summary

- HIPAA is data focused; IOM is IT focused.
- HIPAA has a financial basis; IOM has a clinical basis.
- HIPAA concentrates on workflow policies and procedures; IOM concentrates on the delivery of healthcare process.
- It would behoove organizations to take the IOM New Health System initiative into account when performing its HIPAA assessment and gap analysis. At this point, a decision can be made as to whether or not an automated system selection is going to need to take place, either for HIPAA, for IOM, or for both.
- De-identifying PHI data to comply with HIPAA may impact the value of the information for the IOM evidence-based clinical decision making.

About the Author

Nancy Grey Stetson, BSN, MA, RN, FHIMSS, has over 30 years experience in the healthcare industry spanning the provider, vendor, and consulting arenas. Currently a project manager for MedPlus, Inc. in Cincinnati, Ohio, she has previously served on a corporate healthcare system’s HIPAA task force and on the CPRI workgroup for design.

References

7 See reference 4, p. 16.
9 See reference 4, p. 9.
10 See reference 4, p. 10.
11 See reference 2.
12 See reference 4, p. 12.
13 See reference 2.
14 See reference 4, p. 16.
15 See reference 4, p. 18.
16 See reference 2.