Executive Advisory Board On Privacy And Security

eHI 2020 Roadmap Executive Summit: Data Access & Use Workgroup Report Summary

September 4, 2014

eHEALTH INITIATIVE
Real Solutions. Better Health.

INTRODUCTION

Change will happen only if it begins *here*.

This was the dominant theme of eHealth Initiative's (eHI's) 2020 Roadmap Executive Summit, which took place September 4, 2014 in Washington, DC. The event attracted a wide range of stakeholders who came together to form a public/private collaborative focused on creating a mutual vision of the role of health information technology (HIT) in the American healthcare system by the year 2020.

The summit consisted of a series of general sessions, topic-specific roundtables, and networking opportunities in which executives and leaders from key stakeholder groups—representing providers, payers, government regulators, vendors, and consumers—discussed ideas for the innovations necessary to enhance data exchange and streamline healthcare delivery.

Summit participants' ideas and feedback will help inform a shared vision and set of principles, strategies, and actions for improving healthcare delivery through HIT. This vision will be used to formulate key policy recommendations to be implemented at a federal level and articulate actions for the private sector to undertake. These actions and recommendations will be outlined by eHI in its 2020 Roadmap, to be released later this year.

General session

In her introduction to the Summit, Jennifer Covich Bordenick, chief executive officer of eHI, emphasized that our often-inefficient healthcare system will not improve unless the stakeholders gathered for the event take the lead.

"I ask you each to ask yourselves: 'What can I do to move the agenda forward?'" said Covich Bordenick. "It's easy to point fingers and say someone else should do it and someone else should pay for it. Today we are asking what we can *personally* do."

Covich Bordenick noted that as a non-partisan, public/private organization, eHI is in a unique position to catalyze change in healthcare delivery. After guiding the industry in the nationwide push to adopt electronic health records (EHRs), eHI is in a place to help the industry formulate long-term solutions to the challenges posed by healthcare's increasing dependence on IT-enabled solutions.

"This responsibility falls on each one of us," emphasized Covich Bordenick. "We need you to step up and establish a clear vision for the industry. We don't have one now, but this group can make it happen."

After the opening session, participants joined one of three topical roundtables to address the issues of interoperability, business and clinical motivators, and data access and use, after which they reported back to the larger group and planned future action.

Below we explore the conversations and ideas that grew out of the session on data access and use conducted by the eHI Executive Advisory Board on Privacy and Security. The board—which has thus far met four times to discuss data access and use issues with representatives of federal regulatory agencies—is made up of chief information security officers, chief privacy officers, and other c-suite executives from the payer, provider, and pharmaceutical industries. During this gathering, the board, along with non-board participants who joined the roundtable, built on its previous conversations, talking with one another and the regulators present about their top privacy and security concerns and best practices to deal with them.

DATA ACCESS AND USE ROUNDTABLE

To guide the conversation specific to the topic of data access and use, roundtable participants were furnished with a vision for securely transmitting personal health information among players across the healthcare industry:

- Consumers have confidence that their personal health information is private, secure, and used in ways that are transparent to consumers and authorized by law.
- Technological developments are adopted in harmony with policies and business rules that foster trust and transparency.
- Organizations that store, transmit, or use personal health information have internal policies and procedures in place that protect the integrity, security, and confidentiality of information.
- Policies and procedures are monitored for compliance, and consumers are informed of existing remedies available to them if they are adversely affected by a breach of security.
- Consumers trust and rely upon the secure sharing of healthcare information as a critical component of high-quality, safe, and efficient healthcare.

In opening the session, Dan Garrett, a principal at PricewaterhouseCoopers (PwC), noted that a glance at recent newspaper headlines indicates that many industries are falling short in their efforts to protect consumer privacy. Naming some of the high-profile security breaches that have made the front pages in recent months, Garrett said that the healthcare industry in particular cannot fully take advantage of IT advancements until it deals with the fundamental issue of protecting sensitive patient information. “We want and need patient data,” said Garrett, “and, more than ever, we have access to it. But the consumer is understandably nervous about letting it go. We cannot change healthcare outcomes until we address this issue.”

Taking action: Accurate patient matching

The group's conversation was structured around five market priorities identified by the Executive Advisory Board on Privacy and Security in prior meetings:

- Accurate patient matching
- Appropriate data sharing
- Data provenance
- Granular data control
- Leadership relations

Joe Greene, a principal at PwC, reminded the group that inaccurate patient matching is a problem that transcends all types of industry players and can raise significant quality of care issues. "Providers, payers, and industry vendors of all types deal with this issue every day," said Greene. "The manual fixes we currently have are incredibly inefficient and costly."

Greene reminded the group that complicating the issue is the fact that Congress has forbidden the U.S. Department of Health and Human Services from spending money to create a national identifier. "It would be easier if regulators could create such an identifier," said Greene, "but they do not have that option. So the industry needs to take the initiative to address this issue itself. This will become only a bigger problem as data sharing increases and the industry moves to consolidate more information across more channels."

Problem solved?

As the discussion got underway, there were differing opinions regarding whether the technology to ensure accurate patient matching already exists in other sectors. Several participants stated that the technology necessary to consolidate patient records across different payers, providers, and vendors is already being used in other industries. "This is eminently solvable on the technology side," affirmed one IT industry representative. "The problem is politics, not technology. Attaching a number to a person—that is not difficult, if someone has the authority to do it. Behavioral advertising has been created to produce accurate person monitoring. If they can do it, we can do it in healthcare."

This opinion was confirmed by another representative whose company fields requests to match patients with their drug prescription histories. He said that in 80% of these requests, his company is able to accurately match patients: "The algorithms are there if you collect enough information."

"So why re-create an identifier when it's already been done?" asked one provider. "We need to determine what it will take to make this type of solution commercially available."

But others took issue with such certainty. "I don't think the technology problem is solved," said another provider representative. "And we all deal with vendors who do not have patient-matching technology," added another provider. "That compounds the problem. If a patient's information is incorrect, that error is spread to all of the other organizations that have access to that person's data."

A physician present at the roundtable affirmed that clinicians consistently receive "messy, dirty" data about their patients. Many data errors are traceable to human mistakes, such as a mistyped name or number. "We need algorithms that determine if a patient is a patient in spite of these errors," said the physician. "We need

intelligent programs that can make accurate patient-matching decisions even if birthdates are a month off or if nicknames are used instead of full names."

A regional v. national solution

Several providers at the table pointed out that although Congress has prevented the creation of patient identifiers on a national scale, there is no rule forbidding local governments from doing so on a regional scale.

"Nothing is preventing individual states from creating identifiers," said one participant. "We have been working with states to test the concept of a statewide identifier. We are working with organizations to educate state legislators about the importance of this and how it can save money and increase patient safety."

A provider representative agreed that a regional approach may be a desirable alternative to a nationwide effort. He suggested that regional organizations use health information exchanges (HIEs) to share information about patients they have in common. "There is a hospital a mile and a half up the road from us," he said. "We see thousands of the same patients, and it is in our economic interest to share patient information. We can use our proximity to one another to our mutual advantage."

Achieving consumer buy-in

Several participants agreed that the industry will not be able to achieve a lasting solution to inaccurate patient matching until it has the cooperation of consumers—the ultimate authority of their own information. Participants agreed that, for now, most consumers do not see the value in giving up and tracking their personal healthcare data. For many, it is a matter of trust.

"What's in it for consumers?" asked one participant. "Right now, nothing. Will they give up personal information for cost savings? They don't see that. We need to look outside-in to determine what will make consumers do this."

"The consumer is going to drive this," agreed another participant. "They will provide and manage their information if they are rewarded with convenience and better care and cost. If we can convey this to them, organizations and policy will change."

How much is too much?

Several participants wondered whether the problem of maintaining accurate patient information is simply a matter of collecting the "right" data. One provider from a densely populated county said that there is so much identity fraud in her region that using birth dates to verify individual identity is no longer sufficient. She suggested using harder-to-obtain personally identifiable information, such as cell phone numbers, mothers' maiden names, or cities of origin.

"This would increase the probability that an algorithm will match patients almost 100% of the time," she said. "Gathering additional data elements that do not change over time will go a long way. In our state's health exchange, we push data back to patients and give them control over it."

Other participants suggested using biometric data as foolproof evidence of identity. “Would people be willing to tie a biometric to their patient identifiers?” asked one participant. “How do we make it palatable to get a quick iris scan or fingerprint? How can we get patients to trust this without fearing Big Brother?”

But one participant warned against the generation of too much personal information. “Is it the right approach to just collect more data to improve accuracy?” he asked. “Or is the creation of more and more data on individuals more likely to cause massive damage when that data is breached? We need to balance our concerns.”

Another provider suggested the use of an “exclusionary system” to both guard against the release of too much identifiable information and prevent the replication of inaccurate patient data. “Ideally,” he explained, “identifiers should work. But they should be exclusionary rather than confirmatory. You want to exclude the bad data and make sure it is not replicated. So gather additional patient identification information, but be careful how you use it; perhaps use it to identify a mismatch rather than make a match.”

“A commercially viable alternative needs to guard against ‘bad stuff’ happening to patients,” agreed another provider, referring to medical errors. “We should start with standards that can avoid harm, and then work toward full functionality.”

Taking action: Appropriate data sharing

The group started its discussion about the second of the five topics by talking about the meaning of the word “appropriate” in relation to sharing patient data among healthcare providers. Many voiced their frustration in obtaining consensus in this area within their own institutions as well as on a regional and national level. “We can agree that patient data needs to be shared for the purposes of treatment,” said one participant. “In my organization, that’s as far as I get regarding consensus.”

Several participants noted that as the industry adopts a more fully realized model of integrated care, they are struggling with demands for granular control of patient data. “As we move forward into integrated care, and as we combine information about behavioral and physical treatment, we are seeing separate fields in which we are asked to indicate patient consent to share information,” said one participant. “How deep do we go in terms of the level of consent we allow patients to select and specify?”

Another participant expressed frustration with the challenge of communicating the complex rules governing information sharing with consumers who may have difficulty comprehending such rules. “We write materials at an eighth-grade reading level because that’s what our patients understand,” said the provider. “It would be challenging to do that with complicated disclosure rules.”

A few participants remarked that the industry may be at least partly to blame for consumer confusion regarding patient data access and use. “Patients who have consented to the broader use of their information have ended up being marketed to by third parties,” said one participant. “The Federal Trade Commission is now stepping up its presence in this area because we have not done a good job of distinguishing for consumers the difference between collection and use.”

Focusing on the positive

One participant steered the conversation in another direction by suggesting that the current discussion on controlling patient information may be misguided. “We shouldn’t be talking about constricting and controlling information,” she said. “We should be talking about sharing information to support patient outcomes.” She explained that industry conversations on this topic should center on teaching the benefits of information sharing to the healthcare consumer: “Tell them who their doctors are sharing information with and how that makes things better for them from a care and cost perspective. The world is focused on controlling data. We should address how we can make it more accessible in a controlled way.”

A pharmaceutical representative agreed, adding that his industry needs to do a better job of conveying to patients the therapeutic value of sharing their information with multiple care providers. For example, he said, when pharmacies have access to all of a patient’s prescribing information, they can make care recommendations to specific physicians. “To make those tailored recommendations,” he explained, “we need to facilitate that data sharing by communicating its benefits to consumers.”

Taking action: Data provenance

In introducing this section of the discussion, Joe Greene explained that data provenance is the concept of understanding where data has originated, knowing whether it has been modified, identifying who has modified it, and recognizing how it has been modified. An additional challenge, he added, is being able to identify a "source of truth" against which data elements may be fact checked.

Several participants expressed reluctance in over-identifying data sources. Noting how many hands patient data can pass through, one participant remarked, "Details about patient data could overwhelm the data itself."

Another participant agreed, saying that tracing the genealogy of each patient data set could paralyze an operation. "We don't want to subject health data to a military level of provenance," she said. "That will add too much cost. We don't want to make usage impractical in our pursuit of complete information purity."

A physician participant shared his view as a practicing clinician that no information is completely "pure." "As an emergency room physician, I find that the number of touch points for patient data are innumerable," he said. "I cannot track all of them or completely determine what is trustworthy. It is impossible to track the reliability of all data points."

Rather, said the physician, the best effort should be made to ensure that only "vetted folks" can enter data into a system, and that such data remains unalterable. To attempt to determine the origin of all fields and then allow different people to alter them in different ways and under different circumstances is impractical. "If we design the overall system that we use for day-to-day care to that level of specification, we run the risk of being unable to do our jobs," said the physician. "We are trying to make these tools agreeable to all people and all uses simultaneously, and that's not possible."

"The ultimate adjudicator at the point of care is human judgment," added another participant. "The level of provenance will be hard to police for every point. I think we should consider provenance for only important points."

Lost in translation

Other participants pointed out that some degree of provenance is necessary for the safe provision of care. One provider noted that one of her organization's third-party vendors had once arbitrarily stripped out the identities of the specific labs used for patient tests. "The vendor did this as a design feature to reduce the information it had to manage," said the participant. "When clinicians questioned the data, we couldn't tell them where it came from."

Another participant said that she's heard that some providers do not trust data when they receive it from outside of their own institutions. Someone else added that physicians have different expectations of quality depending on the data source." If we do not track provenance, we are not giving doctors the ability to make informed decisions regarding whether to trust the information they receive."

One provider expressed concerns that patient information is often used in many different formats for various uses, causing it to become corrupted. "Our clinical information system gets requests for data from all over our organization, and provenance is lost in translation," she explained. "Our data is transformed for so many different uses, it becomes no longer reliable. "

Several other providers commented on their inability to preserve the integrity of patient data once it leaves their organizations' systems. "Everyone wants data in different forms for their different needs," said one provider. "We lose control of what happens to data when it travels outside of our system."

Another participant sympathized. "Once data leaves our system and goes to other users, there's nothing that prevents them from cutting and pasting patient information into an Excel spreadsheet," he said.

Taking action: Granular data control

The topic of granular data control, closely related to appropriate data sharing, elicited expressions of frustration from the group. “We’ll never be able to fully comply with all of our patients’ conditions regarding access to their information,” said one participant. “Some patients request to exclude specific medications from their records that may indicate the treatment of a particular disease. For example, if you have an HIV-positive patient who wants to hide his HIV diagnosis, but wants to share his medication history, a listing of the HIV drugs he is on will violate his first wish. You cannot fully pick and choose which patient information you share.”

“Bringing permissions down to the individual medication level or episode level is beyond the capabilities of EHR systems,” noted one participant. “It’s more feasible to attach permissions to the encounter level. Patients can indicate whether they are comfortable sharing their information depending on the type of office visit. Is it for a physical exam? Behavioral health? Sexual health? We can more realistically manage privacy by the *type* of encounter.”

Several other participants agreed, noting that many patients do not want specific episodes of care—such as those dealing with reproductive or psychiatric healthcare—shared beyond their treating physicians. Another provider representative noted, “Segmenting data into types—such as physical and behavioral health—that is easy to communicate. But it’s more difficult to parse what elements are allowed to be shared with whom—and many patients want to dictate that.”

Another participant suggested, “Instead of trying to navigate which specific information a patient wants to share with which specific provider, put all of a patient’s information into their record and then give them the choice of sharing all of it—or none of it—with a specified provider. The provider can then ask the patient during their encounter if they have permission to look at their records.”

“You can’t make everyone happy regarding how their information is used,” added a provider representative. “Don’t make the perfect the enemy of the good. Most people expect their providers to share their information—and assume they are doing so—so they can get competent care.”

The practice of asking patients to opt in or opt out of information sharing under various circumstances was also discussed. Sometimes, said one provider representative, patients want to *completely* opt out of sharing their information: “We get phone calls from people who do not want their information shared with anyone outside of their treating doctors, and they don’t care why sharing their data may benefit them. When physicians are not getting the full picture of what patients are taking and what tests they have had, we are setting doctors up to fail. We need to balance the decisions of patients with the provision of safe care.”

“Many patients would die if their physicians were denied their full medical and drug history,” added another participant. “In the event of an emergency, all patient information should be made available.”

One provider said that at her organization, all patient information goes into their HIE unless a patient specifically opts out of participating in it. Asked how many patients have declined to have their information entered into the HIE, the provider replied, “about four.” Other providers affirmed that they too have very low opt-out rates—mostly in the low single percentages, leading the group to agree that the problem wasn’t a large one.

Taking action: Leadership relations

Most participants agreed that, at least in their own organizations, leadership was focusing more on privacy and security than it previously had. The question, they said, was how to use this interest constructively and sustain it over the long term.

One provider argued that the answer lies in consolidating all risk management leadership and elevating it to the c-suite. “We need to focus on organizational risk in all forms,” he said. “We should take all of the people who guard against all types of risk and have them talk to one another and report to a chief risk officer. Let’s think about this as the comprehensive risk function of an organization in which we address legal, financial, privacy, and security risks together.”

The idea was attractive to several other participants, who expressed agreement with the opinion that if you give organizations a framework that embraces a united approach toward risk in general, privacy and security will be addressed as a fundamental function of the entire organization.

Another participant said that privacy and security executives should emphasize to company leadership the importance of privacy and security in conversations about risk and business principles. “Tell leadership that they need to be motivated not just by fear of compromised data, but also by the market edge they can gain by managing risk on an organizational level,” he said. “Sharing data is a necessary business function. We don’t want to spread fear within leadership, but we want to emphasize the business benefits of good data security.”

The role of physicians

The group agreed that, as the ones who interact most directly with patient data, physicians are ultimately in the best position to take a leadership role in enhancing the privacy and security of patient information. But to motivate clinicians to take a lead in information security, direction must come from above. “Until executives take security seriously, physicians will not,” said one provider. “It has to start at the top—at the c-suite.”

To empower physicians to assume a leadership role in protecting patient information, one participant suggested that a new perspective is necessary. “Some of you have said that the physicians are the obstacle,” he noted. “If we can leverage tools already out there and have physicians become the champions of those tools, we may make some progress.”

Several participants agreed, but they noted that physicians should not have to go it alone. One provider representative said that the industry has already produced physician-specific guidance and tools to help them take the lead in protecting patient data. “We should look to the American Medical Association and other organizations that have come out with security kits that providers can use,” he said. “These are accredited organizations with measures that can be leveraged by the industry as a whole.” Another participant agreed: “We should look at what is already available—standards that are out there and working.”

A physician within the group, however, reminded his fellow participants that the ease of use of many privacy and security tools is still far from ideal. He said that clinicians are often asked to use privacy and security tools that are clunky and subject to frequent malfunction. This discourages them from viewing IT-based privacy protections in a positive light. “When I am working at the hospital,” he explained, “it takes a long time to get access to our system. If there is a period of inactivity, it logs me out, and I need to start from scratch

to get access again. It's easy to say what the technology can do, but in the real-world deployment of it, it has gutted physician morale. We are fighting with computers non-stop. It is not as simple as people make it sound, and we are paying the price in decreased efficiency and a demoralized workforce."

One participant noted that this is precisely the type of clinician feedback that is missing in many parts of the industry, and leadership will not take proper note of it until the effect of IT policies on physicians and patient care are elevated to the highest levels of their organizations.

Conclusion

In summarizing the discussion on data access and use, Dan Garrett noted eHI's goal of using such collaborative conversations to articulate compelling arguments to industry leadership regarding why privacy and security should rank high on their agenda. "There are things we can do," affirmed Garrett. "We can make decisions, come to consensus, and introduce solutions to our constituents. We can articulate privacy and security principles and create a framework for their introduction."

Garrett reiterated to the group several of their suggestions regarding actions that they can take now, including taking advantage of already-proven industry best practices and tools, creating with the Office of the National Coordinator for Health Information Technology or other regulatory groups an industry-wide privacy and security framework, and working with eHI's leadership to articulate a statement of ethical industry standards to help ease consumer concerns.

Ultimately, said Garrett, "This will be about how much this all will cost, who will bear that cost, and whether leadership believes that there will be a return on their security investment. We need to build trust with our executives the same way we would with investors."

"Look around this table," one participant noted as the session was drawing to a close. "You are all healthcare consumers as well. We should not be guided by idiosyncratic, one-off opinions. We need to examine what challenges we all have in common, how we can work together to address those challenges, and articulate that to our leadership."

Acknowledgments

eHI Executive Advisory Board on Privacy & Security

Allison Viola, Vice President, Policy and Government Affairs, eHealth Initiative

Anahi Santiago, Director of Information Security and Support Services, Albert Einstein Healthcare Network

Anne Adams, Chief Compliance Officer and Chief Privacy Officer, Emory Healthcare

Barbara Gabriel, Lead Editor, Healthcare, PwC

Bill Cushing, Senior Vice President, Chief Audit Executive & Chief Risk Officer, Blue Cross and Blue Shield of Massachusetts, Inc.

Cris Ross, Chief Information Officer, Mayo Clinic

Daniel Garrett, Principal and Health Information Technology Practice Leader, PwC

Jennifer Covich Bordenick, Chief Executive Officer, eHealth Initiative

Joseph Greene, Principal, Healthcare Industry Advisory, PwC

Kathryn Marchesini, Acting Chief Privacy Officer, Office of the National Coordinator for Health Information Technology

Kathy Jobes, Chief Information Security Officer, Sentara Healthcare

Kenia Rincon, Director, Health Information Privacy and Security Practice, PwC

Kim Fleurquin, Chief Risk Officer, Sonora Quest Laboratories/Banner Health

Krishnan Chellakarai, Associate Director, IT Security & Privacy, Gilead Sciences

Mark Lantzy, Chief Information Officer, Gateway Health

Mitch Parker, Chief Information Security Officer, Chief Technology Architect, Temple University Health System, Inc.

Nadeen Siddiqui, Policy Analyst, eHealth Initiative

Peter Harries, Principal and US Health Information Privacy and Security Leader, Healthcare, PwC

Sara A. Juster, Associate General Counsel & Privacy Officer, Surescripts

Tim Thompson, Senior Vice President, Chief Information Officer, BayCare

AND

Attendees of the eHI 2020 Roadmap Executive Summit – Data Access & Use Workgroup