Executive Advisory Board On Privacy And Security

Data Access and Use: Addressing Privacy and Security Challenges to Move Information Across the Healthcare Ecosystem

June 25, 2014

eHEALTH INITIATIVE
Real Solutions. Better Health.

Introduction: Monitoring data access and use

On June 25th, twenty-one representatives of the payer, provider, and pharmaceutical industries as well as four representatives of federal regulatory agencies came together in Washington, DC for the fourth meeting of the eHealth Initiative (eHI) Executive Advisory Board on Privacy and Security. The chief information security officers (CISOs), chief privacy officers (CPOs), and other c-suite executives who make up the Advisory Board had previously met three times to articulate their top privacy and security concerns and discuss best practices. During this meeting, the group concentrated on data access and use and discussed the challenges of maintaining privacy and security as information moves across the healthcare ecosystem.

At the start of the meeting, Jennifer Covich Bordenick, CEO of eHI, reminded the group that the board's purpose is to engage industry leaders and federal regulators in closed-door sessions during which they can talk openly about current and evolving industry challenges. She noted that this interaction can help bridge gaps in understanding among industry leadership and regulators so they can work together to respond to the daily security and privacy challenges presented by rapidly evolving technologies in the healthcare sector.

"Right now there is a window of opportunity open to us in that there are multiple vacant leadership positions in federal regulatory agencies," noted Covich Bordenick. "This president's administration wants our input into what that leadership should look like, and it is proactively soliciting our opinion."

Covich Bordenick added that input from the eHI Executive Advisory Board on Privacy and Security would be incorporated into the organization's forthcoming "2020 Roadmap," which will help build a multi-stakeholder, public/private solution to evolving issues in four focus areas: incentives, interoperability, care delivery, and data access and use. The last area, data access and use, was the focus of the June 25 meeting.

THE QUEST FOR "REASONABLE" SECURITY

A CONVERSATION WITH FEDERAL POLICY LEADERS

In introducing the federal regulators joining this session of the Advisory Board, Joseph Greene, a principal with PwC, explained that determining the appropriate use of patient data requires industry leaders to ask themselves multiple questions, including:

- How can I ensure that access to patient data is legitimate and intended for a specific use?
- How can I effectively monitor data use?
- How can I put an approval chain for individual use into place?
- How can I best train individuals on proper data usage?

As an example of the fallout from inappropriate data usage, an attorney from the Federal Trade Commission (FTC) mentioned a medical transcription services company that the FTC recently brought a case against for inadvertently making individual patient medical files publicly available due to inadequate security procedures. In the FTC's settlement with the company, regulators required that it create an information security program, scale its program to meet privacy and security requirements, and conduct regular audits.

To help companies implement safeguards before such action is taken against them, the FTC representative referred the Advisory Board to the FTC's data security tools located on its Bureau of Consumer Protection website (http://business.ftc.gov/privacy-and-security/data-security). There, businesses can find guidance on topics such as peer-to-peer file sharing, mobile application development and marketing, and medical identity theft risks and safeguards. One FTC representative noted that the agency understands that any company can suffer a breach, and the government does not expect "perfect" security from healthcare organizations. Rather, said the representative, the agency looks for reasonable security. For example, the representative said that effective employee training in privacy and security is vital, especially given the proliferation of personal electronic devices. The representative noted that unencrypted laptops are stolen each day in this country, needlessly exposing sensitive patient information to misuse.

Regarding the FTC's recent initiatives, the representative mentioned a panel the agency hosted in May on the security of consumer-generated and controlled health data, such as that generated by mobile health and fitness devices such as Fitbit. This data — which represents an increasing amount of patient information being generated outside of traditional healthcare facilities — is proliferating with the rapid introduction of mobile consumer health devices in the marketplace.

The representative said that while the panel affirmed that these devices represent a tremendous amount of innovation and potential health benefit, there is also significant risk that the personal health information generated by the devices will be shared in ways consumers may not

anticipate. The attorney acknowledged the challenge the industry faces in providing adequate notice to consumers about who will have access to their health information and how that information will be used.[1]

Consumer-friendly disclosures

Participants agreed that current industry disclosures are often long and filled with legal jargon, making them unintelligible for many consumers, indicating an unmet industry need for "short, transparent" consumer disclosures. Several people added that simply ensuring that application developers adopt disclosure policies is not enough. One participant noted that a recent Apple disclosure for a new mobile device is 327 pages long. "Who is going to read that?" he asked. "Even two pages is too long." Another participant volunteered, "I've tried to read those things, and they are essentially contracts. You need a lawyer to decipher them."

Other participants agreed that "short-form" disclosure policies are much needed in the industry, particularly when many consumers are reading text on the small screens of their smart phones. One person noted that language can be another barrier to consumer comprehension. "Many consumers speak languages other than English," he said. "We cannot enforce compliance if it is not understood by the user. More and more people who do not speak English are coming to this country every day."

Sobering statistics indicate inadequate safeguards

Another FTC representative discussed the findings of an FTC "privacy rights clearinghouse" study that evaluated the privacy policies of 43 free and paid health and fitness mobile applications (apps).[2] The FTC found that 26% of the free apps and 40% of the paid apps did not have a privacy policy, and 39% of the free apps and 30% of the paid apps sent consumer data to someone not disclosed by the developer. Only 13% of the free apps and 10% of the paid apps encrypted all data connections between the apps and the developers' websites. These troubling results led the FTC to conclude that health and fitness apps do an inadequate job of protecting user privacy.

In a related FTC "snapshot study" gauging the amount of information-sharing among health and fitness applications that generate personal health data, the FTC evaluated 12 apps and two wearable devices.[3] The agency found that the apps transmitted individual consumer information to 76 different third parties. That information included consumer-specific identifiers and information such as exercise routines, dietary habits, and symptom searches.

---

[1] More information about the FTC's panel, "Consumer Generated and Controlled Health Data" can be viewed at http://www.ftc.gov/news-events/events-calendar/2014/05/spring-privacy-series-consumer-generated-controlled-health-data (accessed July 7, 2014)

[2] Federal Trade Commission Spring Privacy Series, "Consumer Generated and Controlled Health Data," May 7, 2014. http://www.ftc.gov/system/files/documents/public_events/195411/consumer-health-data-webcast-slides.pdf, slide 24. (accessed July 7, 2014)

[3] Ibid. Slides 27-35.

The FTC representative said that while many consumers have indicated that they generally do not care how their data is shared by the developers of the applications they use, they may feel differently when it comes to their personal health information. Consumers may be uncomfortable with marketers, researchers, and insurers sharing their health data without their consent. If the healthcare industry educates consumers about the multiple ways their information can be used, the industry may be able to recruit consumer allies in its attempts to curb unobstructed patient information transfer.

In response to these findings on the lack of privacy controls on popular healthcare-related consumer apps, Joseph Greene from PwC noted, “These days, it doesn’t take a whole lot to start a company besides launching an app.” With that in mind, Greene asked the regulators present, “How do we put processes into place to educate these companies about their responsibilities to protect consumer information?”

One FTC representative replied that thus far the market’s response to the need for consumer privacy and security varied significantly. Likening the app market to the “wild, wild west,” she suggested that one approach may be to encourage developers to think about security as they are creating products, rather than treating privacy considerations as an afterthought.

The other FTC representative reminded the group that federal guidance on transparency and disclosure has existed for years. The FTC’s guidance on the privacy and security considerations for mobile devices was issued several years ago, giving consumers some idea of how the information they share may be used by third parties. Nevertheless, it is not enough for companies to simply state that they are “following industry standards and putting protections into place.” Such statements should be followed by concrete documentation regarding how and under which circumstances consumer information is used.

The buck stops where?

One provider expressed his anxiety over what he perceives as the “blurring line” between the patient information contained in physician-generated electronic health records (EHRs) and new, consumer-generated health information. For example, he said, an app or wearable fitness device may generate personalized information that may be of interest to the patient, although not of much interest to the physician. Will organizations now be put into the position of monitoring how their patients’ devices interact with the health records that organizations are responsible for maintaining?

“If we decide to accept personal health information from patients’ apps, do we get to choose which apps to accept?” asked the participant. “These are all-new third parties that we have not personally vetted. Will we be stuck working with them? Will we be responsible for the information they produce?”

A representative from the Office of the National Coordinator for Health Information Technology (ONC) noted that this situation is the product of a free market, and it’s up to that market to determine the rules. The representative noted that in a different industry sector, one

organization — which has since dissolved — did attempt to develop a product that screens different apps for adequate security measures. In the healthcare sector, she said, there may be more of an appetite for such a tool. “We need a private-market solution,” said the representative. “The government can act as the convener in these cases, but industry should provide a practical solution.”

One provider participant noted that even if the industry does come up with something like a code of conduct for privacy and security, some companies will do the least amount possible to obtain a seal of approval. “We need to put our vendors through the wringer to make sure they follow the same processes we do,” he said.

Data access and use scenarios

What should we share, how should we share it, and who should we share it with?

In a discussion structured by a series of practical data access and use scenarios distributed by eHI, the Advisory Board's moderators asked participants to share their opinions regarding how and under which circumstances they would approve the sharing of patient data.

Mick Coady, principal at PwC, began this part of the meeting by asking the providers present how comfortable they are sharing their patients' information with the pharmaceutical companies that conduct research in their hospitals. One provider who represents an academic medical center (AMC) said that pharmaceutical companies are a presence in his hospitals every day, and he feels comfortable freely sharing information with them because he knows his institutional review board (IRB) has fully vetted their activities beforehand. "We have a good vetting system in which we do a full privacy review before we accept any pharmaceutical presence," said the provider. "We tell them that they will have to meet our standards."

Another provider noted that her health system does not generally grant pharmaceutical companies full access to hospital networks. She said that, like the AMC, all pharmaceutical research programs must first clear the health system's IRB. "We are very prescriptive about what they can and cannot get access to," she said. "As long as all of our reviews are thoroughly conducted and all permissions approved, we are comfortable sharing information." The provider also noted that there can be widely varying levels of information-sharing, requiring different types of consent: "Each case is different and should be individually considered."

Another provider shared that her organization has the ability to limit information access to specific patient data and limit the time pharmaceutical companies have access to that data. "We have gotten some pushback from some pharmaceutical company monitors whose legal departments do not want them signing our confidentiality agreements," she noted. "But if that is the case, they will not be given access to our patient records." Another participant said that before deciding to partner with a pharmaceutical company, her organization first asks if sharing such information will benefit its patients, community, mission, or bottom line. She noted that the patient information her organization possesses is valuable. "It is an asset that we want to protect," she asserted.

Several providers noted that de-identifying patient information may allow them to share patient data more widely with those who request access for research purposes, although one provider characterized the costs of de-identification as "huge," noting that such costs would be passed onto the requestors. Several participants commented on the substantial cost and manual processes required to give external parties such as pharmaceutical researchers limited access to patient medical records. Fulfilling such requests usually entails pulling data out of the providers' own systems and creating unique data sets for the pharmaceutical companies to use.

Cooperation breeds competency

Many Advisory Board members voiced their support for the development of industry-wide privacy and security standards for the healthcare sector. An ONC representative noted that the White House has launched a national strategy to help the industry create trusted, protected identities in cyberspace for individual consumers. The National Strategy for Trusted Identities in Cyberspace (NSTIC) is working collaboratively with the private sector, advocacy groups, public sector agencies, and other organizations to improve the privacy, security, and convenience of online transactions. The representative said that NSTIC is now conducting pilots that are testing identity-proofing and authentication in healthcare settings.

Several participants said they welcomed such initiatives to standardize privacy and security efforts across the private sector. "All of us develop our own privacy standards internally," noted one participant. "It would really help us to know what other organizations are doing. Right now, we solve a lot of our problems during industry conference calls, during which we learn about one another's different privacy and security policies. That communication is crucial for us."

Providers and payers representing international organizations added that cross-border standards in particular would be helpful to them. "To move data among different countries, we have tried to come up with common consent language regarding privacy and security," said one participant. "It is difficult to obtain regulatory consensus among several nations." She also noted that as the industry perceives how much more cost-effective standardized privacy and security standards are, there will be more will to create them. "It will benefit industry as a whole," she explained. "We need to incentivize collaboration rather than competition."

Whose data is it, anyway?

When it comes to patients' electronic access to their own medical and billing information, the answers are no less complicated. Walking the line between giving patients what they say they want and making that information comprehensible to them can be very difficult, several participants agreed. One participant noted that sharing information with patients is confusing enough using paper. "A patient has a small procedure done, and then gets bills from 16 different people," he said. "That's confusing enough. If we start giving them access to electronic billing information that includes detailed data such as ICD-9 codes, we are not helping them better understand their care."

The ONC representative agreed that the industry needs to keep ease of use top of mind when deciding how to provide patients access to their information. As an example, she cited the meaningful use directive that patients must have electronic access to their lab results. She said that the intention of this directive is to ensure that patients always receive their results, and providers must ensure that they do so in a way that patients can easily understand.

One participant noted that the healthcare industry should take a page from the banking industry's approach to customer service. "In banking, your average consumer is not managing multiple financial relationships online and having to understand each one," he said. "If you have a loan, a credit card, and a mortgage, you can seamlessly connect among the three, even if

they are hosted by different companies, without having to log on repeatedly. You do not notice that you are traversing different networks." Similarly, patients are serviced by a variety of providers and payers. "We now have the technology to comprehensively service patients in the same way," said the participant. "We just need the will to do it."

In a subsequent discussion on the possibility of realizing a federated identity for patients that would link their personal information across multiple, distinct identity management systems, participants played with the idea of basing that identity on consumers' Yahoo or Google accounts. "Right now, we as consumers already federate our own identities by combining our Google, Yahoo, Amazon, and Paypal accounts," said one participant. Matt Lawson, director at PwC, opined that it's "not a stretch to think that a few years down the road, healthcare companies may be using social identities such as Facebook and Google identities to obtain additional authentication information from their patients."

What would you fix first?

Prioritizing our priorities

The final session of the day consisted of an interactive exercise that began with Mick Coady of PwC asking each participant to name the top two things they would like to fix regarding data access and use in their organizations. A lively conversation followed, with several participants naming far more than two items on their wish list. Everything from the ability to grant vendors customized access to patient information to the creation of universal online patient identities to the formulation of industry-wide privacy and security standards was cited by participants.

Once everyone had shared his or her "wish list," moderators grouped the items into five themes, which they listed on large pieces of paper hung throughout the room. Participants were given color-coded stickers and asked to use those stickers to indicate which of the themes and sub-themes were most important to them. Once they had done so, the moderators led a discussion on their most pressing concerns. The following five concerns were given the highest priority:

1. **Appropriate Data-Sharing:** Individual organizations struggle to monitor the flood of patient information that they originate and receive each day. When they must share that information with other organizations that also provide care and services to the same patients, determining who needs to access what specific information can become quite difficult.

   One participant said that she has come across information in her organization's system without knowing its origin. Another participant said he is alarmed when personal health information his organization produces winds up somewhere else without his knowledge. "This happens more and more," he said. "I need to know how third parties get that information. Right now, I don't always know."

2. **Accurate Patient Matching:** When there are multiple entries for the same patient and confusion about who has the right to enter new data, information can quickly become unreliable. Participants overwhelmingly agreed on the importance of being able to accurately match individual patient identities with their data. One provider said that she located her own identity in her health system's database eleven times. "We have employees who reconcile IDs all day," she said. "They do nothing else."

   One payer representative acknowledged that it is not only providers that have this problem. "This happens across the healthcare system," he said. "We all have the ability to make errors. And then we all compound the error by sharing information." Several participants noted that once patient duplicates are detected, there remains the question of which "version of the truth" to trust. "Do you follow what Medicare says?" asked one participant. "What a private insurer says? What an EHR indicates?" Reasons for duplicate entries can vary widely, such as typing errors, intentional errors, and common birthdates and names, just to name a few.

The ONC representative reminded the group that while Congress does not allow Health and Human Services (HHS) to spend money to create a national patient identifier, the ONC has made recommendations on how to standardize data elements. Ultimately, she said, the industry will have to take the lead on such an initiative.

3. **Emphasizing Data Security to Leadership**: Participants overwhelmingly agreed that effective security can be an important business enabler. “Data security should be addressed from both an operations and a go-to-market approach,” said Coady. Several participants said that, in the aftermath of the now-infamous Target security breach, they have seen a renewed interest in data security from their organizations’ leadership. “The more breaches make the news, the more our leadership wants to know what we are doing to prevent that from happening to us,” said one participant. “We need to keep the issue top of mind for them.”

4. **Data Provenance:** The ONC representative said that her agency commissioned an “environmental scan” on the issue of data provenance in 2013. She explained that “data provenance” refers to the ability to obtain information about the origins of clinical data and the processing and transitions that the data has undergone. The ONC’s environmental scan focused on determining how organizations can retain provenance as systems aggregate data from multiple sources and records are exchanged. Currently, there is no dominant provenance model within the HIT community and no uniform way of handling data provenance when sharing data.

   One participant raised the idea of a “credit watch” for personal health information as a possible solution. Just as there are companies that help consumers guard against financial fraud by monitoring their credit reports, so too could there be an organization that monitors an individual’s health information and warns him or her if it is tampered with or accessed inappropriately. This could also be of use to healthcare organizations attempting to protect the integrity of their patients’ information. “The problem is when a patient’s information goes outside of the parameters of your organization,” said the participant. “Then you should get some notice that has happened.” “Patient information is so valuable,” agreed another participant. “I want it to stay within my environment.”

5. **Granular Data Control:** “There are so many different entities that are requesting access to our data for legitimate reasons, but our systems are not flexible enough to grant access to that data appropriately,” said one participant. “I struggle to remain flexible enough to enable the business.” Several other participants agreed with this sentiment, saying that they need vendors to enhance systems that process medical records so that access to sensitive data can be customized based on a user’s specific needs. Currently, the group agreed, industry-wide inflexibility in customizing data access is a barrier to the free flow of information.

FINAL THOUGHTS

Peter Harries, principal at PwC, closed the meeting by reminding those present that securing sensitive patient information is not only the right thing to do by those we care for, but also an essential thing to do for an organization's integrity and continued success.

"Our clients ask us, 'How do I convince my CEO of the need to appropriately fund privacy and security measures? How do I secure organizational commitment to that spending?'" The answer, said Harries, is to continually remind industry leadership of the consequences of underfunding and understaffing privacy and security controls. Sharing ideas with one another, he affirmed, is the first step.

"We have important work to do in shaping policy and learning from one another," said Harries. "Outlets like this one in which we have the opportunity to freely talk to each other and hear from policy makers can help us make significant headway in accomplishing our goals."

The Executive Advisory Board on Privacy and Security will meet again on September 4, 2014. The group will take a deeper dive into the five concerns that were given the highest priority:

1. Appropriate data-sharing
2. Accurate patient matching
3. Emphasizing data security to leadership
4. Data provenance
5. Granular data control

Results from the September 4, 2014 meeting will be used to develop eHI's 2020 Roadmap.

eHI Executive Advisory Board on Privacy & Security

Acknowledgments

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, Associate VP for CTAC; Chief Compliance 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.

Cora Han, Senior Attorney, Division of Privacy & Identity Protection, Federal Trade Commission

Guy Turner, Sutter Healthcare, Chief Data Security Officer

Hilary Wandall, AVP, Compliance and Global Privacy, Merck

Jac Howard, Catalyst Artist

Jared Ho, Attorney, Mobile, Federal Trade Commission

Jeff Hoover, Partner and US Health Industries Risk Assurance Leader, PwC

Jennifer Covich Bordenick, Chief Executive Officer, eHealth Initiative

Joseph Greene, Principal, Healthcare Industry Advisory, PwC

Joseph Johnson, Chief Information Security Officer, CHS Health Services

Joy Pritts, Chief Privacy Officer, Office of the National Coordinator for Health Information Technology

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

Kathy Jobes, Chief Information Security Officer, Sentara Healthcare

Keith Henkell, Information Security Officer, CenterLight Health System

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

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

Mark Lantzy, Chief Information Officer, WellCare

Marilyn Zigmund Luke, Senior Counsel and Compliance Officer, America's Health Insurance Plans

Mark Savage, Director of Health IT Policy and Programs, National Partnership for Women & Families

Michael Rozmus, Chief Information Officer, Sentara Rockingham Memorial Hospital Medical Center

Mick Coady, Principal, Health Information Privacy and Security Practice, PwC

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

Nadeen Siddiqui, Policy Analyst, eHealth Initiative

Nalneesh Gaur, Director, Healthcare, PwC

Phil Curran, Chief Information Security and Privacy Officer, Cooper Health University Healthcare

Ralph Lange, Director, Enterprise Infrastructure, Availity

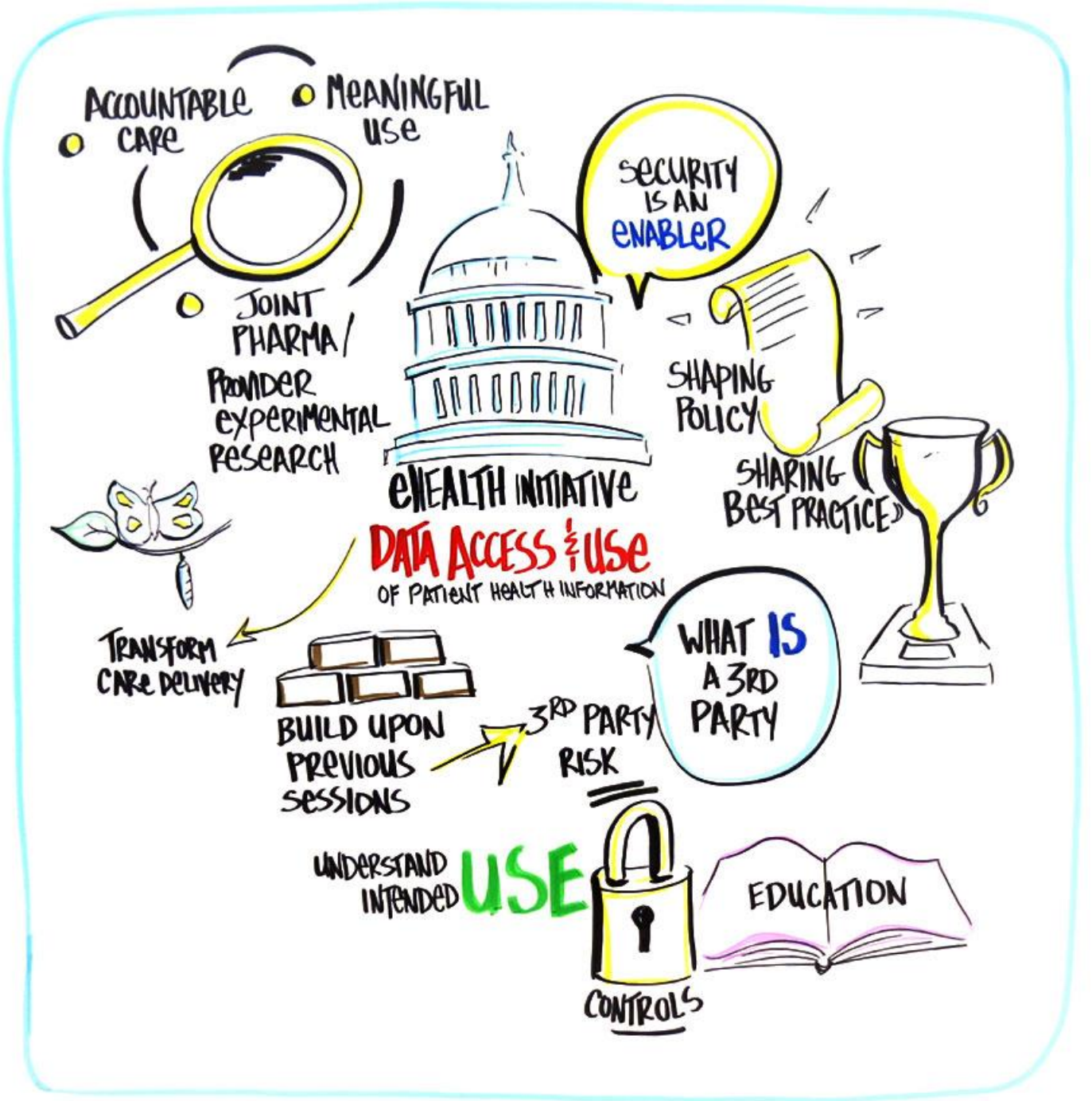
Robbie Higgins, Chief Information Security Officer & Chief Technology Architect, Abbvie

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

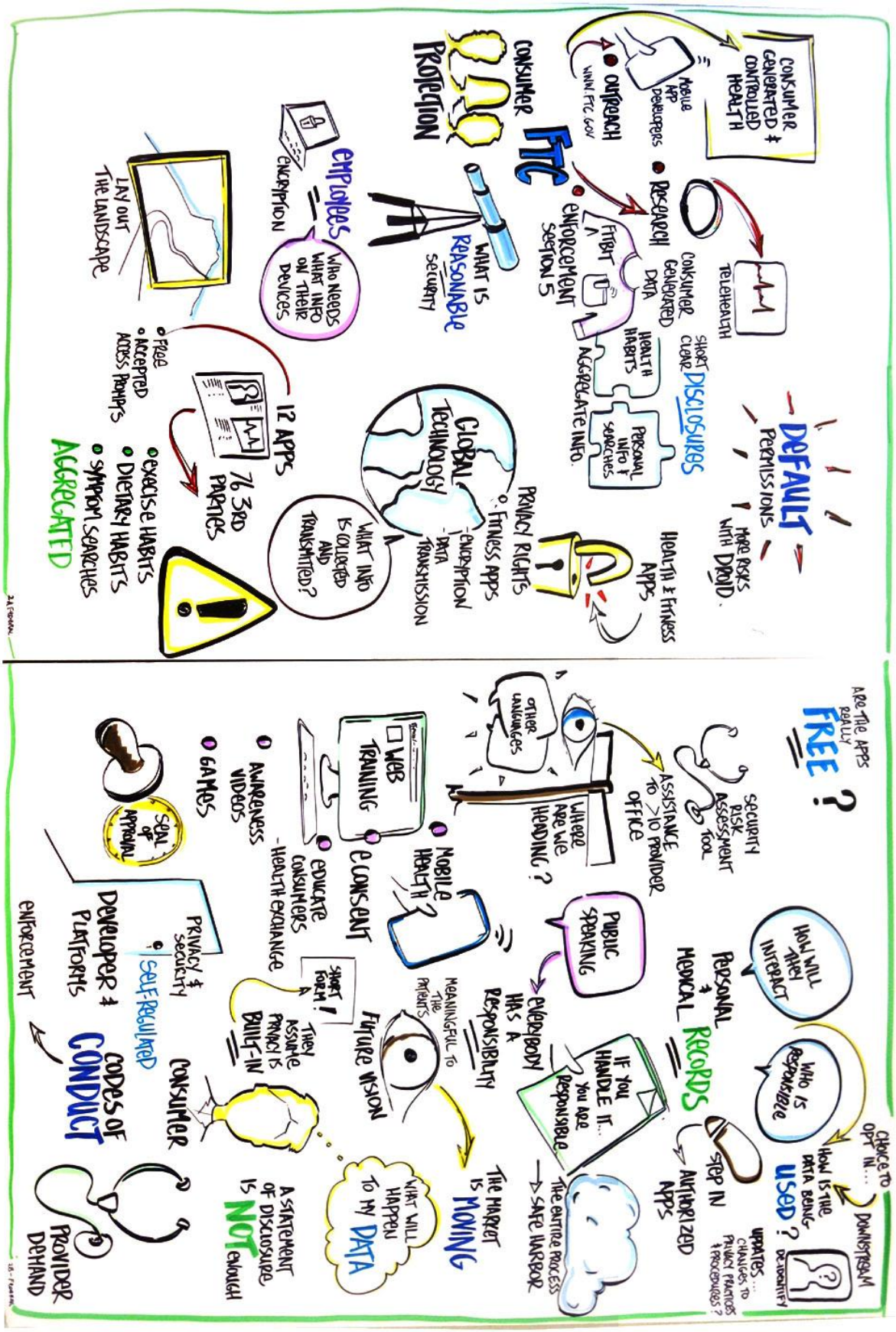
Spencer Mott, Chief Information Security Officer, Amgen

Pieces from Jac Howard, Catalyst Artist

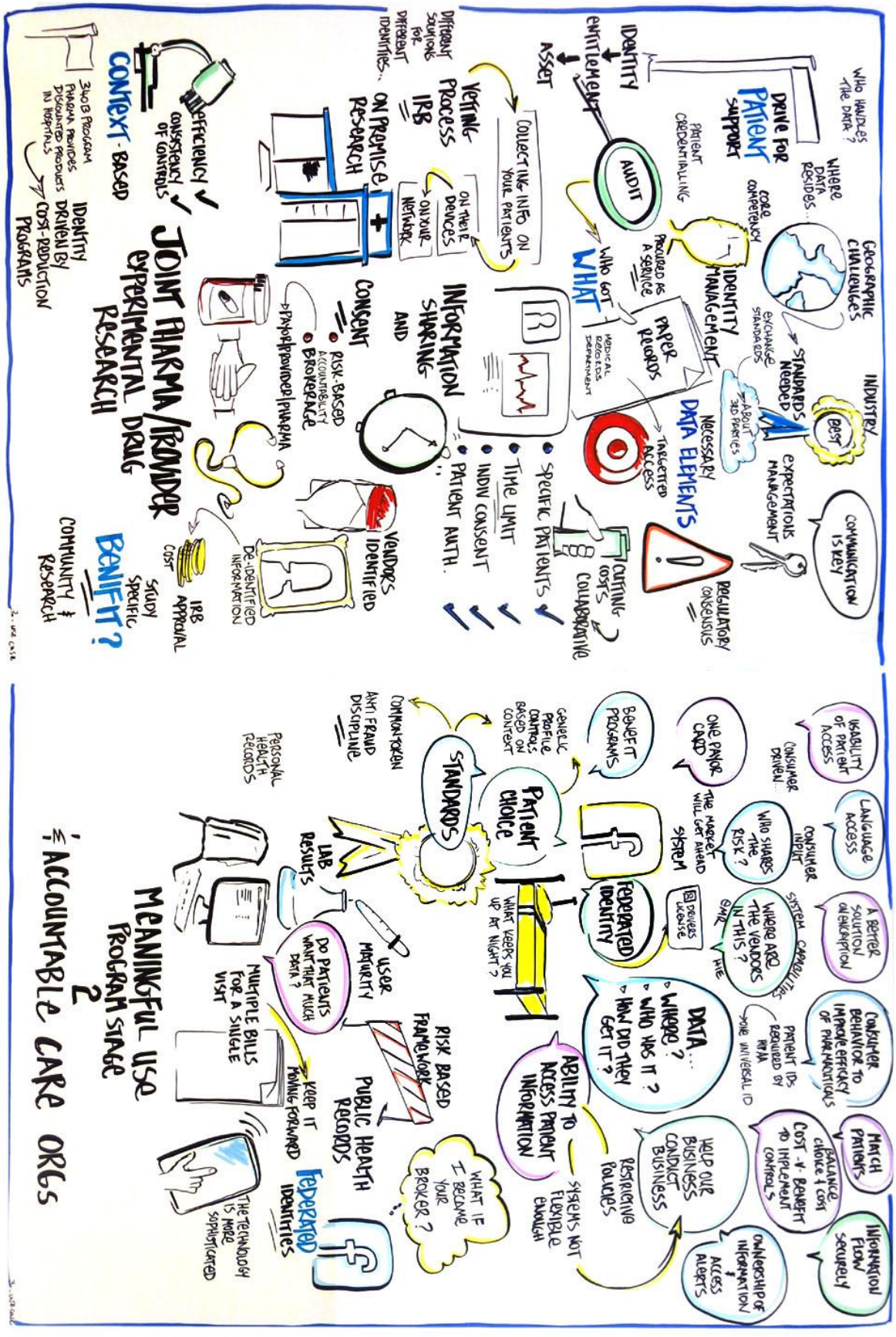
Introduction:



Conversation with Federal Policy Leaders:



Use Cases:


WHO HANDLES THE DATA?
DRIVE FOR PATIENT SUPPORT
WHERE DATA RESIDES...
CORE COMPETENCY
PATIENT CREDENTIALING
AUDIT
IDENTITY MANAGEMENT
PROCURED AS A SERVICE
WHO GOT WHAT
PAPER RECORDS
MEDICAL RECORDS DEPARTMENT
GEOGRAPHIC CHALLENGES
EXCHANGE STANDARDS
STANDARDS NEEDED
INDUSTRY
BEST
ABOUT 3RD PARTIES
NECESSARY DATA ELEMENTS
TARGETED ACCESS
EXPECTATIONS MANAGEMENT
COMMUNICATION IS KEY
REGULATORY/CONSENSUS
CUTTING COSTS
COLLABORATIVE
IDENTITY ENTITLEMENT ASSET
COLLECTING INFO ON YOUR PATIENTS
ON THEIR DEVICES
ON YOUR NETWORK
VERIFIC PROCESS IRB
DIFFERENT SOLUTIONS FOR DIFFERENT IDENTITIES...
ON PREMISE RESEARCH
INFORMATION SHARING AND CONSENT
RISK-BASED ACCOUNTABILITY BROKERAGE
PAYOR/PROVIDER/PHARMA
SPECIFIC PATIENTS
TIME LIMIT
INDIV CONSENT
PATIENT AUTH.
VENDORS IDENTIFIED
DE-IDENTIFIED INFORMATION
IRB APPROVAL
STUDY SPECIFIC
COST
JOINT PHARMA/PROVIDER EXPERIMENTAL DRUG RESEARCH
BENIFIT?
COMMUNITY & RESEARCH
EFFICIENCY
CONSISTENCY OF CONTROLS
CONTEXT-BASED
IDENTITY DRIVEN BY COST-REDUCTION PROGRAMS
3HOB PROGRAM
PHARMA PROVIDES DISCOUNTED PRODUCTS IN HOSPITALS
MEANINGFUL USE PROGRAM STAGE 2
ACCOUNTABLE CARE ORGS
USABILITY OF PATIENT ACCESS
CONSUMER DRIVEN...
LANGUAGE ACCESS
CONSUMER INPUT
WHO SHARES THE RISK?
THE MARKET WILL GET AHEAD
ONE PAYOR CARD
BENEFIT PROGRAMS
GENERIC PROFILE CONTROLS BASED ON CONTEXT
PATIENT CHOICE
STANDARDS
COMMON TOKEN
ANTI FRAUD DISCIPLINE
PERSONAL HEALTH RECORDS
A BETTER SOLUTION ON ENCRYPTION
SYSTEM CAPABILITIES
WHERE ARE THE VENDORS IN THIS?
SAML
NTE
DRIVERS LICENSE
FEDERATED IDENTITY
WHAT KEEPS YOU UP AT NIGHT?
DATA... WHERE? WHO HAS IT? HOW DID THEY GET IT?
ABILITY TO ACCESS PATIENT INFORMATION
SYSTEMS NOT FLEXIBLE ENOUGH
RESTRICTIVE POLICIES
HELP OUR BUSINESS CONDUCT BUSINESS
WHAT IF I BECAME YOUR BROKER?
RISK BASED FRAMEWORK
PUBLIC HEALTH RECORDS
FEDERATED IDENTITIES
THE TECHNOLOGY IS MORE SOPHISTICATED
CONSUMER BEHAVIOR TO IMPROVE EFFICACY OF PHARMACEUTICALS
PATIENT ID'S REQUIRED BY HIPAA
SOME UNIVERSAL ID
MATCH PATIENTS
BALANCE CHOICE & COST
COST-V-BENEFIT TO IMPLEMENT CONTROLS
INFORMATION FLOW SECURELY
OWNERSHIP OF INFORMATION + ACCESS ALERTS
LAB RESULTS
USER MATURITY
DO PATIENTS WANT THAT MUCH DATA?
MULTIPLE BILLS FOR A SINGLE VISIT
KEEP IT MOVING FORWARD

Prioritization of Findings: