EXECUTIVE ADVISORY BOARD ON PRIVACY & SECURITY

INTEGRATING PRIVACY & SECURITY INTO ORGANIZATIONAL STRATEGY AND CULTURE

eHEALTH INITIATIVE
Real Solutions. Better Health.

Introduction

As the adoption and use of information technology within healthcare continues to advance, digitizing sensitive patient information also increases at a rapid pace. The increased use of health information technology to capture, store, and use sensitive patient information has greatly increased the importance of effective privacy and security programs for healthcare organizations.

To ensure the healthcare industry keeps patient information safe with opportunities to access it—and mishandle it—multiply daily, the Centers for Medicare and Medicaid Services (CMS) and the Office of the National Coordinator for Health Information Technology (ONC) regularly issue and update privacy and security regulations that healthcare entities must implement to remain compliant with the law. These regulations—perceived by the industry as alternately burdensome and vital—aim to help healthcare entities protect sensitive patient information from cyber threats, data breaches, and identity theft.

To address the safety and security issues that necessitate these protections and predict what further safeguards may be needed, eHealth Initiative (eHI) convened a gathering of the Executive Advisory Board on Privacy and Security (Advisory Board) —comprised of chief information officers, chief information security officers, chief privacy officers, and other c-suite-level executives from the healthcare industry —in Washington, DC, on December 3, 2013. Key leadership from CMS and ONC joined the conversation to gain a better understanding of issues the health industry is facing, but also an opportunity to provide updates on their programs.

During a previous meeting of the Advisory Board in May 2013, members gathered to discuss their top privacy and security concerns and identify and share their solutions to collective challenges. The Advisory Board agreed that transforming their organizations' cultures to integrate privacy and security into their organizational framework is necessary to ensure the integrity of electronic health information. For this meeting, Advisory Board members narrowed the focus of their discussions to discuss the importance of initiating a culture shift in their organizations to secure a commitment to privacy and security from the tops of their organizational hierarchy down to their end users.

Rather than approach privacy and security measures as separate requirements that their organizations must meet, Advisory Board members discussed the efforts of some provider, payer, and pharmaceutical companies to make privacy and security an integral and foundational element of their overall strategies. Consistent themes emerged regarding not only the challenges these organizations are facing, but also similar issues that patients and consumers are grappling with.

Industry panel discussion: Creating a Culture of Privacy and Security

Advisory Board members agreed that privacy and security need to be integral and foundational elements of an organization's overarching strategy, ones that mesh with the converging healthcare industry and make guarding patient privacy part of the day to day workflow. They recognized that, for this to happen, a culture shift needs to originate at the top of an organization with its board of directors and trickle down to promoting awareness among all stakeholders including staff and patients.

By building collaborative relationships within their organizations' communities, healthcare organizations integrate privacy and security into their overall infrastructures rather than isolate them as separate initiatives. But this should not be a one-directional effort by an organization's privacy and security professionals. Rather, it needs to be a bi-directional effort that allows end users, patients, executives, and other stakeholders to share their experiences and challenges to create a common approach to protecting consumer and patient information.

Some Advisory Board members shared examples of how they have personally addressed privacy and security within their organizations. These approaches often required creative thinking to effectively engage specific communities and create a culture that prioritizes privacy and security. One member shared his experience of meeting with other staff, including physicians and division leaders, to gain a better understanding of his organization's day-to-day privacy and security needs. Another board member hosted a privacy and security skills quiz and rewarded winners with prizes. Another leveraged a "Cyber Security Awareness Month" to feature lively, interactive activities to educate staff members. Yet another member created a seminar on how employees can protect their children from online threats, and explained to staff how the same tactics can be used to protect sensitive information at work. And, finally, one member established a work day in which employees were encouraged to shred unnecessary documents and clear unused hard drives.

Different Industry Perspectives

Three Advisory Board members who served as representatives of the provider, payer, and pharmaceutical industries formed a panel in which they discussed privacy and security concerns specific to their sectors.

The **pharmaceutical** executive indicated that his industry becomes more reliant on electronic information each year. Since this information ranges from credit card details to patients' genetic data, it is difficult to create a unified privacy and security policy that can successfully secure vastly different types of data and the various methods through which it is transmitted. The executive emphasized that consistent messages from senior leadership articulating an organization's privacy and security approach, policies, and procedures is one of the best guards against inadvertent—or purposeful—data compromise.

An executive with a healthcare **provider** stated that his industry is facing possible security threats posed by the personal mobile devices clinicians are bringing into the workplace. Many of these devices are not securely integrated into the workplace systems with which they connect, exposing patient information to threats against which organizations have no safeguards. In response to this risk, the panelist said that his organization has adopted a policy that does not permit the introduction of unapproved personal devices into their network—although it can never fully guard against this.

Other provider concerns include security implications resulting from the dramatic increase of electronic health records (EHRs) within provider settings, exponentially increasing the number of opportunities to compromise sensitive patient information. The panelist pointed out to the group the healthcare industry has evolved from using a linear, analog mode of communication to one that is a networked system of data exchange incorporating patient information from multiple providers. This has given rise to an avalanche of state and federal regulations to which providers must now adhere, including many under HIPAA and the EHR incentive program "meaningful use."

The **payer** executive expressed his hope that organizations in his sector embrace privacy and security safeguards as market differentiators rather than as difficult tasks that are often addressed as an afterthought. Being proactive and integrating security safeguards into an organization's core structure, rather than being reactive and addressing privacy only when an organization proves vulnerable, can be a key industry differentiator. The panelist said his company's leadership has embraced privacy and security as an opportunity to create a strategic advantage. They have worked to proactively anticipate risks specific to their companies and address them before information can be compromised. Doing so has enabled them to promote themselves as having an advantage over their competitors in the realm of privacy and security safeguards.

Creating Policy to Support the Integration of Privacy and Security Practices: Key Priorities

Privacy and Security Focus Areas From OCR and ONC

Key leadership from the Office for Civil Rights (OCR) in the US Department of Health and Human Services and the Office of the National Coordinator for Health Information Technology (ONC) joined the Advisory Board members for an open discussion in which the policymakers offered clarity about audit procedures, data governance, risk assessments, and liability. The OCR and ONC leaders provided an overview of their agencies' efforts to promote privacy and security as an opportunity to improve patient care, and they shared with the group their priorities for 2014.

Advisory Board members expressed their concern about unclear privacy and security regulations, saying they are not always sure who will be held accountable if a privacy or security breach occurs. The average cost of a patient information breach can reach $10 million, but Advisory Board members said these amounts are often arbitrary and depend on the nature of the organization that experienced the breach. They also expressed uncertainty about audits, asking for clarification about how organizations are selected for auditing.

Also of concern, said several board members, is ownership of patient data, particularly in regard to the potential for patient-generated data contained in EHRs. As more patients personally enter information into their EHRs, who has ownership of that data, and who may change it? Other specific topics that were addressed by the Advisory Board which requires additional attention, focus, and guidance were data at rest encryption and multi-factor authentication. The consensus was that healthcare organizations are in need of further guidance, standards, and frameworks to be able to adhere to changing regulations.

Office for Civil Rights

An OCR representative presented the Advisory Board with an overview of the office's key priorities for the coming year. Rather than creating new privacy and security policies, she said, in 2014 OCR will consolidate and fill in the gaps of existing privacy and security regulations. Four specific issues she addressed were:

- **Risk Assessments for HIPAA Security Rule:** Advisory Board members identified the HIPAA Security Rule as challenging and in need of more clarity. The Security Rule requires healthcare entities to protect against any anticipated threats to the security of their electronic health information by conducting risk assessments of their security measures. The OCR representative said the agency has developed and will continue to develop use cases and work with ONC to provide the tools healthcare organizations need to accurately perform their risk assessments. She also indicated the audit perspective will be shifting away from Privacy and more towards the Security Rule.

- **Audits**: OCR is required by the Health Information Technology for Economic and Clinical Health (HITECH) Act to periodically audit healthcare organizations to ensure that covered entities and their business associates (BAs) are complying with HIPAA's privacy rule, security rule, and breach notification standards. OCR performed a pilot audit program in 2011, and it is now establishing a permanent approach. In response to the Advisory Board's request for more clarity regarding audits, the OCR representative said the agency will aggregate summary reports to share some best practices with the industry. She said that a sample of entities across the healthcare industry, including BAs, will be selected for audits. The agency recognizes that it is more challenging for small providers to perform accurate risk assessments, and it will take that into account as they produce a risk auditing tool customized for small providers.

- **Business Associates**: Individual healthcare organizations subject to HIPAA regulations are held liable for HIPAA compliance of their BAs. In response to board members' requests for additional clarity regarding their liability for their contractors' security measures, the OCR representative acknowledged the need to implement necessary training and education to make BAs fully aware of HIPAA rules. She stated that healthcare organizations are ultimately responsible for making their BAs aware of their privacy and security obligations.

- **Rights of Individual Access**: Consumers are becoming more engaged with their health information through new technology pathways such as mobile applications and patient health portals. Advisory Board members expressed concern about the implications of this trend and asked about any HIPAA measures that may apply. The OCR representative said the agency is looking to adapt HIPAA requirements to address this concern.

Office of the National Coordinator for Health Information Technology

The Advisory Board was also joined by a representative from the ONC Privacy Office who elaborated on her office's focus for 2014. She said that ONC has a global perspective on information security that allows it to integrate privacy and security measures at all points of healthcare information exchange.

- **Patient Matching Identification**: Advisory Board members are concerned that standards for patient matching have not yet been issued by the ONC. The ONC representative acknowledged that patient matching is currently performed in silos, creating privacy risks when payers and providers exchange electronic patient information. She said that the ONC's Patient Matching Initiative, launched in September 2013, will survey the methods payers and providers currently use to establish standards for matching patients with their health information.

- **Data Provenance**: The healthcare industry needs a process to track, monitor, and tag the increasing amount of patient health information that is aggregated into individual health records. The ONC representative said her agency will prioritize this issue of data provenance in 2014 through its Standards and Interoperability Framework. She said the agency's goal is to track where health information originates and tag it as patient-generated or physician-generated data as records change hands throughout the healthcare system.

- **New Technology and Medical Devices**: Healthcare mobile applications and other devices are creating jurisdictional overlap among governmental oversight bodies, including the OCR, ONC, Food and Drug Administration (FDA), and the Federal Communications Commission (FCC). The ONC and OCR representatives said they recognize the complexity of the situation and the need for simplicity within the regulation process. They are looking into how to standardize the regulatory process and make it easier to connect with other systems.
- **Meaningful Use**: Stage 2 of the "meaningful use" requirements will take effect in 2014, and the rules for Stage 3 will be published in 2014 as well. The ONC representative said that her agency will work on surveying the program's participants to ensure that the security of patient health information is addressed and properly managed.

Moving Forward and Recommendations for Industry

Through their discussions, Advisory Board members identified several key areas that need addressing for the industry to move forward. Among them:

Third-Party Risk Management: Through its "meaningful use" program, the HITECH act launched widespread adoption of EHRs and information technology among healthcare organizations nationwide. While this holds great potential to improve healthcare, it also introduces new security risks when handling electronic patient data.

The Patient Protection and Affordable Care Act (PPACA), signed into law by President Obama on March 23, 2010 further accelerated the adoption and implementation of health information technology by introducing new models of care delivery aimed at improving care coordination. As these new models encourage various stakeholders to exchange patient information, coordinate care, and collaborate, they are leading to an increase in the number of third-party relationships among organizations in the industry. Federal regulators require healthcare organizations to effectively manage these new relationships to minimize privacy and security risks, as indicated by providers' new liability for their BAs' HIPAA compliance.

Healthcare organizations also face significant sanctions if the technology products they use cannot adequately secure and protect patient data. Payers and providers are dependent on their vendors to create products that enable the secure storage, analysis, and exchange of health information. Technology products should make the right thing to do the easy thing to do.

Enterprise Risk Management: As the industry becomes more integrated, healthcare organizations must take a holistic, systematic approach to identifying, assessing, managing, and responding to the complex privacy and security risks facing them. To effectively embed privacy and security into an organization's culture and workflows, the entire organization needs to be held accountable for securing patient information. To accomplish this, an organization's compliance or information security department should not operate apart from other departments. Organizations across the industry should adopt an enterprise risk management approach that embraces privacy and security as a proactive, continuous, and system-wide effort.

Creative Solutions for Training and Awareness: Organizations across the industry should embrace privacy and security efforts as positive opportunities to improve quality and patient care. Organizations should implement sufficient training and education to ensure all employees and affiliates are aware of an organization's approach to privacy and security. Organizations can supplement these efforts with creative solutions, such as establishing a cyber-security month or hosting games and competitions to raise awareness about the importance of information security. Employees in all departments across an organization should be comfortable discussing their privacy and security concerns with management.

Privacy and Security as a Strategic Advantage: Healthcare organizations should leverage their privacy and security efforts as a way to promote and market themselves within industry. Organizations that effectively manage risk and protect patient information can leverage this as a strategic advantage and market differentiator. Success in protecting patient health information can distinguish an organization to patients and consumers, and, in doing so, encourage leadership to support privacy and security policies.

Acknowledgments

Cathy Beech, CISA CRISC, Chief Information Security Officer, The Children's Hospital of Philadelphia

Jennifer Covich Bordenick, Chief Executive Officer, eHealth Initiative

Bryan Cline, PhD, Chief Information Security Officer, Vice President, CSF Development and Implementation, HITRUST

Mick Coady, Partner & Co-Leader, Health Information Privacy & Security Practice, PwC

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

Brian DuPerre, Vice President & Deputy General Counsel; Chief Privacy Officer, UnitedHealthcare

Kim Fleuquin, Chief Risk Officer, Sonora Quest Laboratories

Karen Graham, Chief of Operations, Summit Medical Group

Nalneesh Gaur, Director, Health Industries Advisory, Privacy/Security, PwC

Peter Harries, Principal, Healthcare, PwC

Robbie Higgins, Chief Information Security Officer and Chief Technology Architect, AbbVie

Joseph Johnson, Chief Information Security Officer, CHS Health Services

Thien Lam, Director, IS Security and ISO, BayCare Health System

Ralph Lange, Director of Enterprise Infrastructure, Availity

Mark Lantzy, Chief Information Officer, WellCare

Maurice Andrew Malcolm, Former Information Systems Security Officer, University of Maryland Medical System

Mike Matteo, Chief Information Officer, Centerlight Health System

Susan McAndrew, JD, Deputy Director, Health Information Privacy, Office for Civil Rights, US Department of Health and Human Services (HHS)

Ronald Mehring, Director, Information Security, Texas Health Resources

Spencer Mott, Chief Information Security Officer, Amgen

Acknowledgments (Cont.)

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

Joy Pritts, Chief Privacy Officer, Office of the National Coordinator for Health Information Technology, US Department of Health and Human Services (HHS)

Terry Rice, Associate Vice President, IT Risk Management & Chief Information Security Officer, Merck

Laura E. Rosas, JD, MPH, Privacy and Security Professional, Office of the Chief Privacy Officer, Office of the National Coordinator for Health IT (ONC)

Cris Ross, Chief Information Officer, Mayo Clinic

Tim Thompson, Chief Information Officer, BayCare Health System

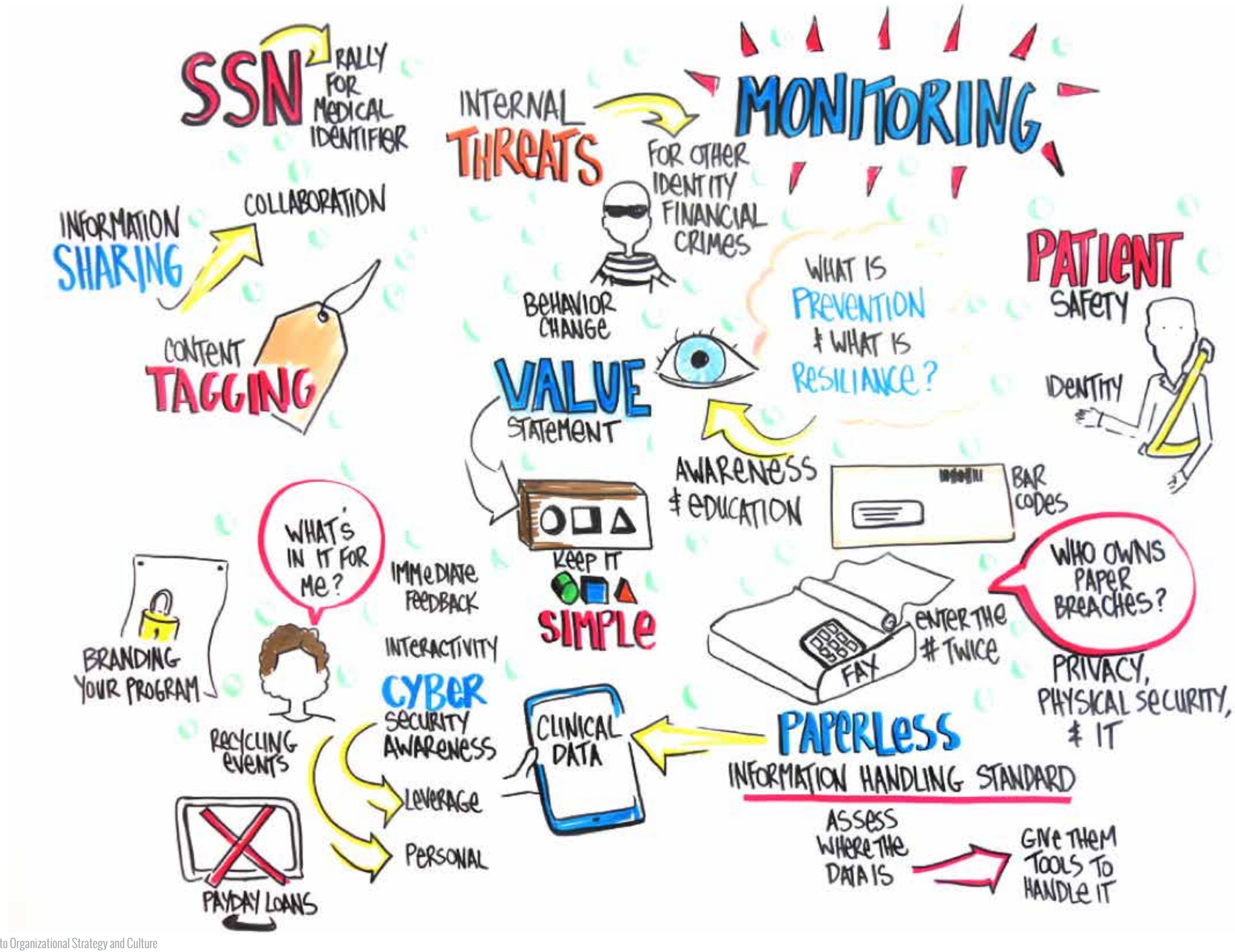
Amanda Titiliuc, Chief Information Officer, Summit Medical Group

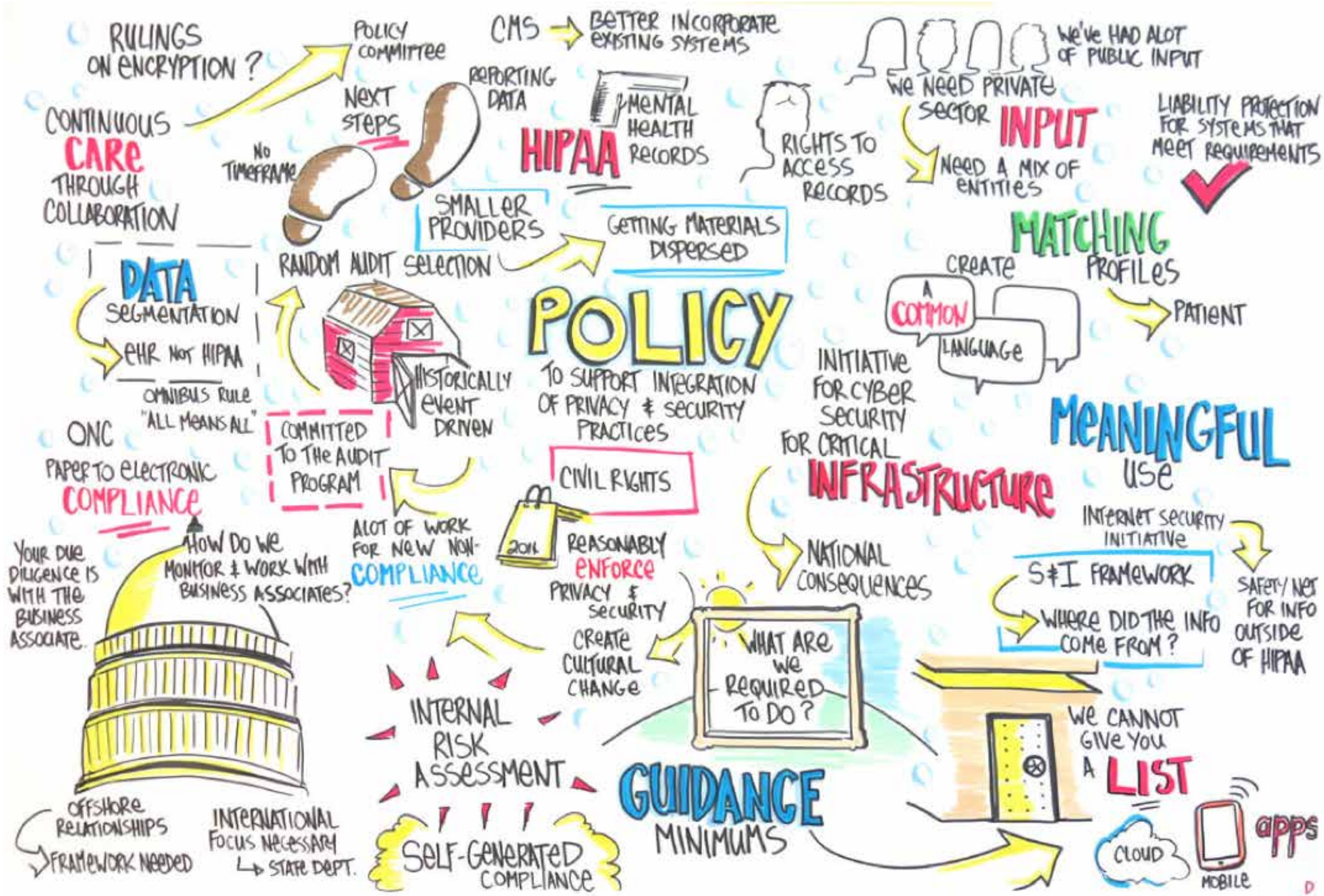
Allison Viola, MBA, RHIA, Vice President, Policy and Government Affairs, eHealth Initiative

Patricia Washington, Division Chief Information Officer; Chief Technology Officer; Blue Cross Blue Shield of Massachusetts, Inc.

Artwork Depicting Discussion During the Executive Advisory Board on Privacy and Security Meeting


BEST PRACTICE
ENTERPRISE RISK MGMT
TRAINING
AUDIT
3RD PARTY RELIANCE
GREATER RELIANCE ON SYSTEMS
INCREASE IN CREDIT CARD DATA
CONTENT TAGGING
COMPARATIVE DATA
SINGLE PAYOR
PATENTS
PHARMA
CONSOLIDATION
COST REDUCTION
EMERGING MARKETS
directtrust.org
HOW DO WE ENGAGE THE CONSUMER?
SCALE
OWNERSHIP OF THE DATA
GOVERNANCE ON WHAT LEAVES THE ORGANIZATION
PRIVACY & SECURITY IS AN ENABLER
PAYOR
50% REACTIVE
50% PROACTIVE
AKE THE RIGHT THING TO DO, THE EASY THING TO DO."
MONITORING
LEVERAGE TECHNOLOGY
END USERS
PHISHING TRAINING & CAMPAIGN
JUST-IN-TIME
TRAINING
EDUCATION
WE NEED
SYSTEMIC SOLUTIONS
VENDORS
COLLABORATION
DE IDENTIFICATION
RE
MEANINGFUL HEALTH INFO EXCHANGE
PROVIDER
ERM
THREAT MAP
VULNERABLE
ANALOGUE TO DIGITAL TO NETWORKED
SEGMENTED


SSN
RALLY FOR MEDICAL IDENTIFIER
INTERNAL THREATS
FOR OTHER IDENTITY FINANCIAL CRIMES
MONITORING
INFORMATION SHARING
COLLABORATION
CONTENT TAGGING
BEHAVIOR CHANGE
VALUE STATEMENT
WHAT IS PREVENTION & WHAT IS RESILIANCE?
PATIENT SAFETY
IDENTITY
AWARENESS & EDUCATION
BAR CODES
KEEP IT SIMPLE
WHAT'S IN IT FOR ME?
IMMEDIATE FEEDBACK
INTERACTIVITY
CYBER SECURITY AWARENESS
LEVERAGE PERSONAL
BRANDING YOUR PROGRAM
RECYCLING EVENTS
PAYDAY LOANS
CLINICAL DATA
FAX
ENTER THE # TWICE
WHO OWNS PAPER BREACHES?
PRIVACY, PHYSICAL SECURITY, & IT
PAPERLESS
INFORMATION HANDLING STANDARD
ASSESS WHERE THE DATA IS
GIVE THEM TOOLS TO HANDLE IT


RULINGS ON ENCRYPTION ?
POLICY COMMITTEE
CMS → BETTER INCORPORATE EXISTING SYSTEMS
CONTINUOUS CARE THROUGH COLLABORATION
NEXT STEPS
REPORTING DATA
MENTAL HEALTH RECORDS
HIPAA
No TIMEFRAME
RIGHTS TO ACCESS RECORDS
WE NEED PRIVATE SECTOR INPUT
WE'VE HAD ALOT OF PUBLIC INPUT
NEED A MIX OF ENTITIES
LIABILITY PROTECTION FOR SYSTEMS THAT MEET REQUIREMENTS
SMALLER PROVIDERS
GETTING MATERIALS DISPERSED
RANDOM AUDIT SELECTION
DATA SEGMENTATION
EHR NOT HIPAA
OMNIBUS RULE "ALL MEANS ALL"
POLICY
TO SUPPORT INTEGRATION OF PRIVACY & SECURITY PRACTICES
MATCHING PROFILES
CREATE A COMMON LANGUAGE
PATIENT
HISTORICALLY EVENT DRIVEN
ONC PAPER TO ELECTRONIC COMPLIANCE
COMMITTED TO THE AUDIT PROGRAM
CIVIL RIGHTS
INITIATIVE FOR CYBER SECURITY FOR CRITICAL INFRASTRUCTURE
MEANINGFUL USE
ALOT OF WORK FOR NEW NON-COMPLIANCE
2014
REASONABLY ENFORCE PRIVACY & SECURITY
NATIONAL CONSEQUENCES
INTERNET SECURITY INITIATIVE
S&I FRAMEWORK
WHERE DID THE INFO COME FROM?
SAFETY NET FOR INFO OUTSIDE OF HIPAA
YOUR DUE DILIGENCE IS WITH THE BUSINESS ASSOCIATE
HOW DO WE MONITOR & WORK WITH BUSINESS ASSOCIATES?
CREATE CULTURAL CHANGE
WHAT ARE WE REQUIRED TO DO?
INTERNAL RISK ASSESSMENT
GUIDANCE MINIMUMS
WE CANNOT GIVE YOU A LIST
OFFSHORE RELATIONSHIPS
FRAMEWORK NEEDED
INTERNATIONAL FOCUS NECESSARY
↳ STATE DEPT.
SELF-GENERATED COMPLIANCE
CLOUD
MOBILE
apps