Deloitte.

Electronic Medical Records

San Francisco ISACA Chapter

January 19, 2012

Audit . Tax . Consulting . Financial Advisory.

Disclaimer

This training presentation is provided solely for educational purposes and, in developing and presenting these courses, Deloitte is not providing accounting, business, financial, investment, legal, tax, or other professional advice or services. This training presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decisions or actions that may affect your business or to provide assurance that any decision or action will be supported by your auditors and regulators. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte, its affiliates, and related entities shall not be liable for any claims, liabilities, or expenses sustained by any person who relies on these courses for such purposes.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Agenda

- Industry Challenges – Trends in Security and Privacy
- Update on Meaningful Use (MU), Health Insurance Portability and Accountability Act (HIPAA), and Health Information Technology for Economic and Clinical Health Act (HITECH)
- Security and Privacy Requirements
- Electronic Health Record (EHR) Technology Certification
- Security Risk Analysis Approach and Methodology/Audit Considerations
- Emerging Trends


Industry Challenges –
Trends in Security and Privacy

Data breaches are top concern among executives

- Per a recent Gartner research brief, Data Breaches are the #1 issue out of their Top 5 issues for 2011 – 2012. Some key points include:
  - "Whether or not you are legally required — notifying about breaches has become a good practice. Do not assume that you can hide the incident.."
  - "Compartmentalize personal information, restrict access, **encrypt data when transmitting it across public networks**, **encrypt data on portable devices, and encrypt data in storage to protect it from users who have been given too much privilege**, from rogue administrators and from hackers."
  - "Document how you protected personal information, and have this documentation ready in case of a breach.."

Source: "*Top 5 Issues and Research Agenda 2011 – 2012: The Privacy Officer*", Gartner, 14 June 2011

*"On average, it is estimated that data breaches cost benchmarked healthcare organizations $2,243,700." **

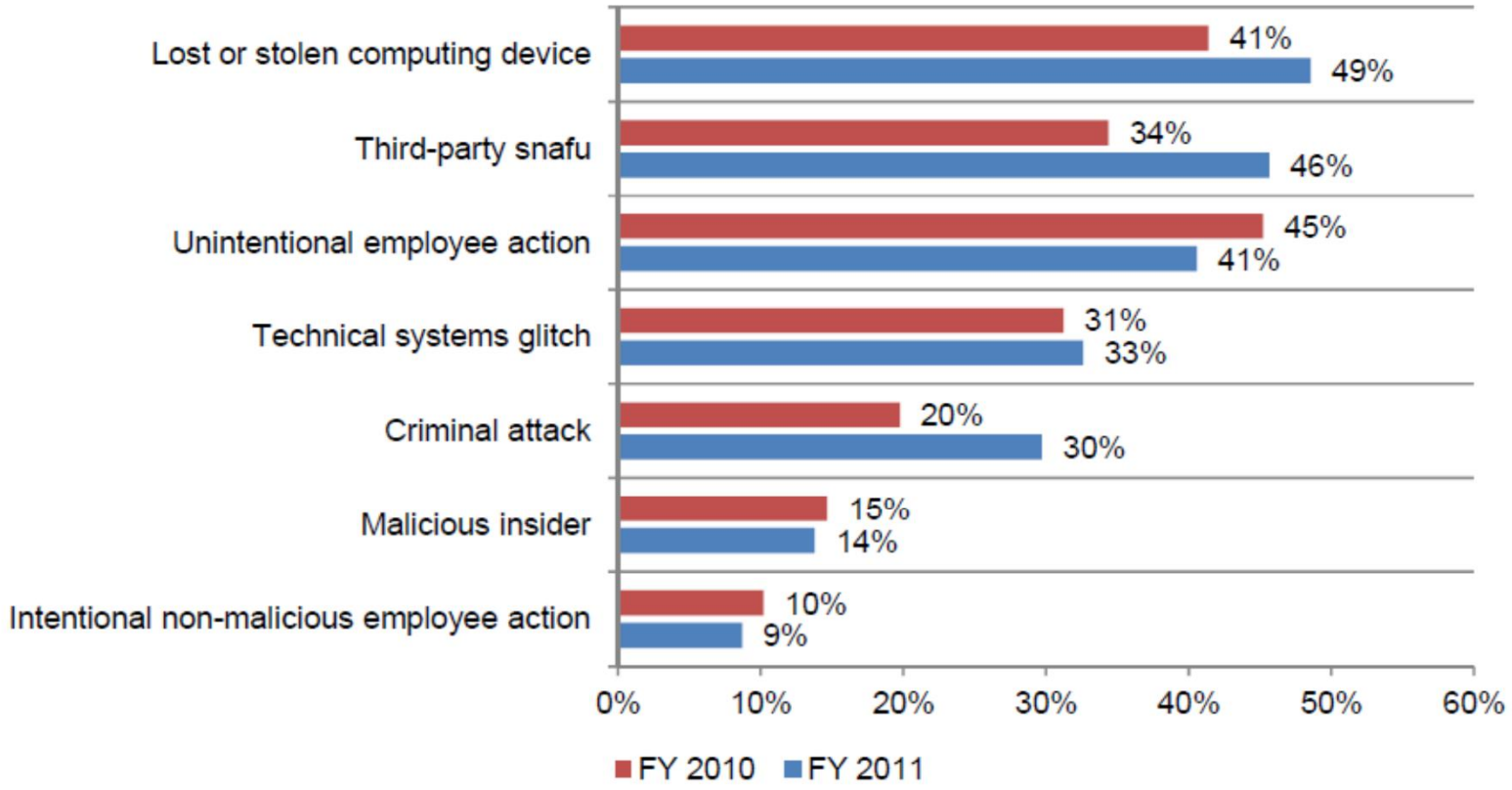
**Ponemon Institute LLC, Second Annual Benchmark Study on Patient Privacy & Data Security, December 2011*

"…the number of data breaches among healthcare organizations participating in the 2010 and 2011 studies is still growing—eroding patient privacy and contributing to medical identity theft."

**Ponemon Institute LLC, Second Annual Benchmark Study on Patient Privacy & Data Security, December 2011*

The top 5 reasons underlying data breaches

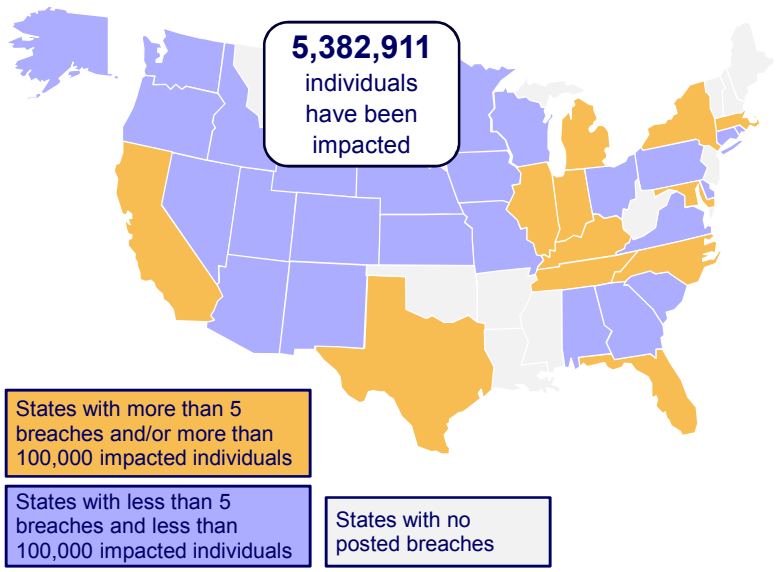
Bar Chart 2: Nature or root causes of the data breach incident
More than one choice permitted

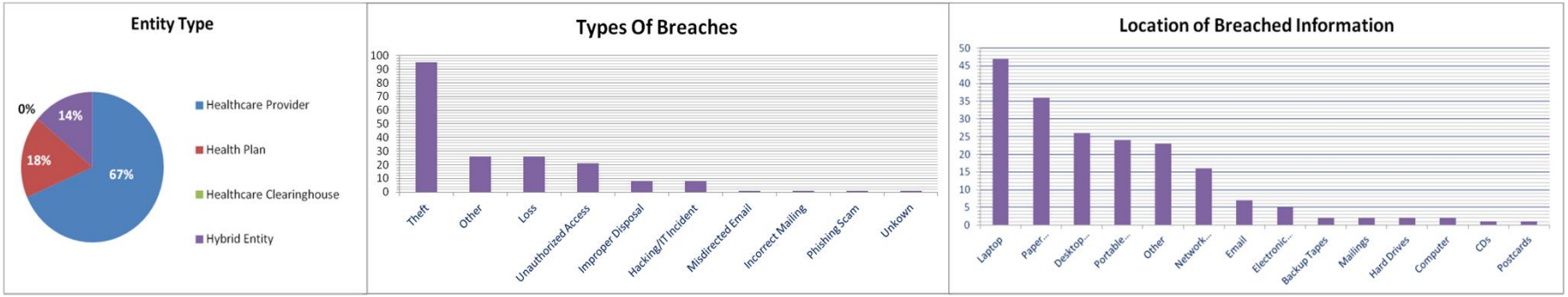


**Ponemon Institute LLC, Second Annual Benchmark Study on Patient Privacy & Data Security, December 2011*

Industry trends: data breach perspective

- The number of individuals impacted by breaches reported to the Department of Health and Human Services (HHS) is steadily increasing. According to the HHS Website for Breaches Affecting 500 or More Individuals, **165 data breaches of unsecured PHI in 39 states** have been reported **between September 2009 and September 2010***
- **Business associates were involved in 19%** of the reported breaches
- **Theft (58%)** and **Loss(16%)** were the two major causes of breaches involving unsecured PHI
- Breached information was stored in **laptops (28%), paper records (22%), desktop computers (16%) and portable devices (15%)**



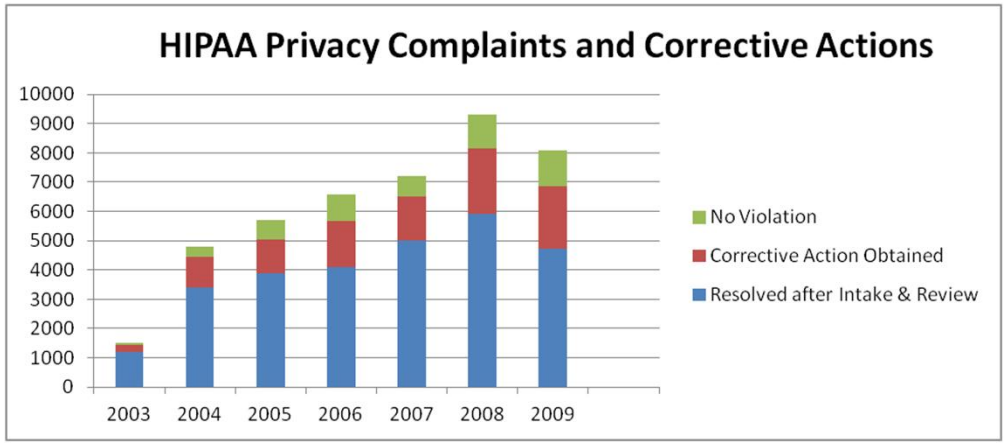


Theft of and unauthorized access to laptops, computers, paper records, and portable electronic devices (e.g., USB Drives) are "lo-tech", yet significant causes of PHI data breaches for which organizations are being reported.

*Based on data published by HHS as of September 20, 2010.

Industry trends: enforcement

There have been steady trends of increasing HIPAA Privacy and Security enforcement over the years*. Since 2003, the Office of Civil Rights (OCR) has been responsible for enforcing the Privacy Rule, and on July 27, 2009, the office became responsible for enforcing the Security Rule. The following are statistics and summary relating to its HIPAA enforcement activities:



Highlights of Privacy and Security Rule Enforcement

- Since October 2009, HHS has received approximately 166 complaints alleging violation of the Security Rule
- During this period, 59 Security Rule complaints were closed after investigation and appropriate corrective action
- As of August 31, 2010 OCR had 174 open Security Rule complaints and compliance reviews
- Corrective actions resulted from **21%** of total Privacy Rule complaints

Top 5 issues in investigated cases, which resulted in corrective actions*:

1. Impermissible Uses and Disclosures
2. Safeguards (security controls as defined in the HIPAA Security Rule)
3. Access
4. Minimum Necessary
5. Complaints to Covered Entity

* Based on data published by the Office for Civil Rights ("OCR") of the Department of Health and Human Services as of September 20, 2010.

Q&A

- What other security and privacy trends do you consider to be “on the list” for management to address?

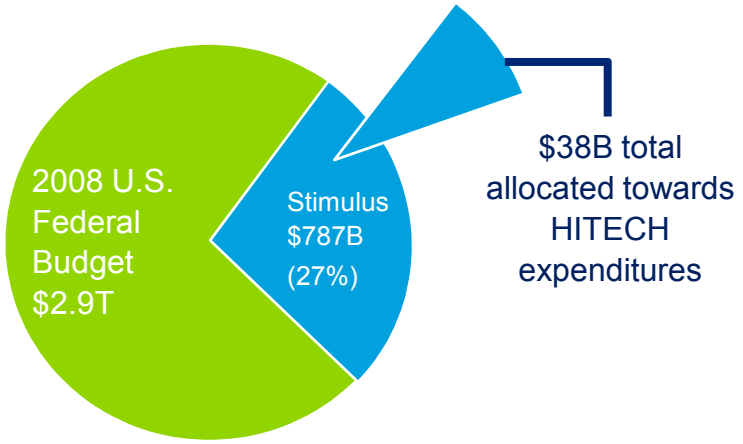
- What good practices would you share to improve and mature security incident response capabilities – from identification to triage to reporting?


Update on Meaningful Use,
HIPAA, and HITECH

Overview of the American Recovery and Reinvestment Act (ARRA) & HITECH

Facts and figures

- First major initiative of the Obama Administration
- Appropriates $787 billion across a broad spectrum of government programs
- Many Health and Human Service (HHS)/labor funds are passed down to states through existing mechanisms
- Health IT funding includes incentives and appropriations from the **Health Information Technology for Economic and Clinical Health Act** (HITECH) Act and other health IT initiatives such as telehealth



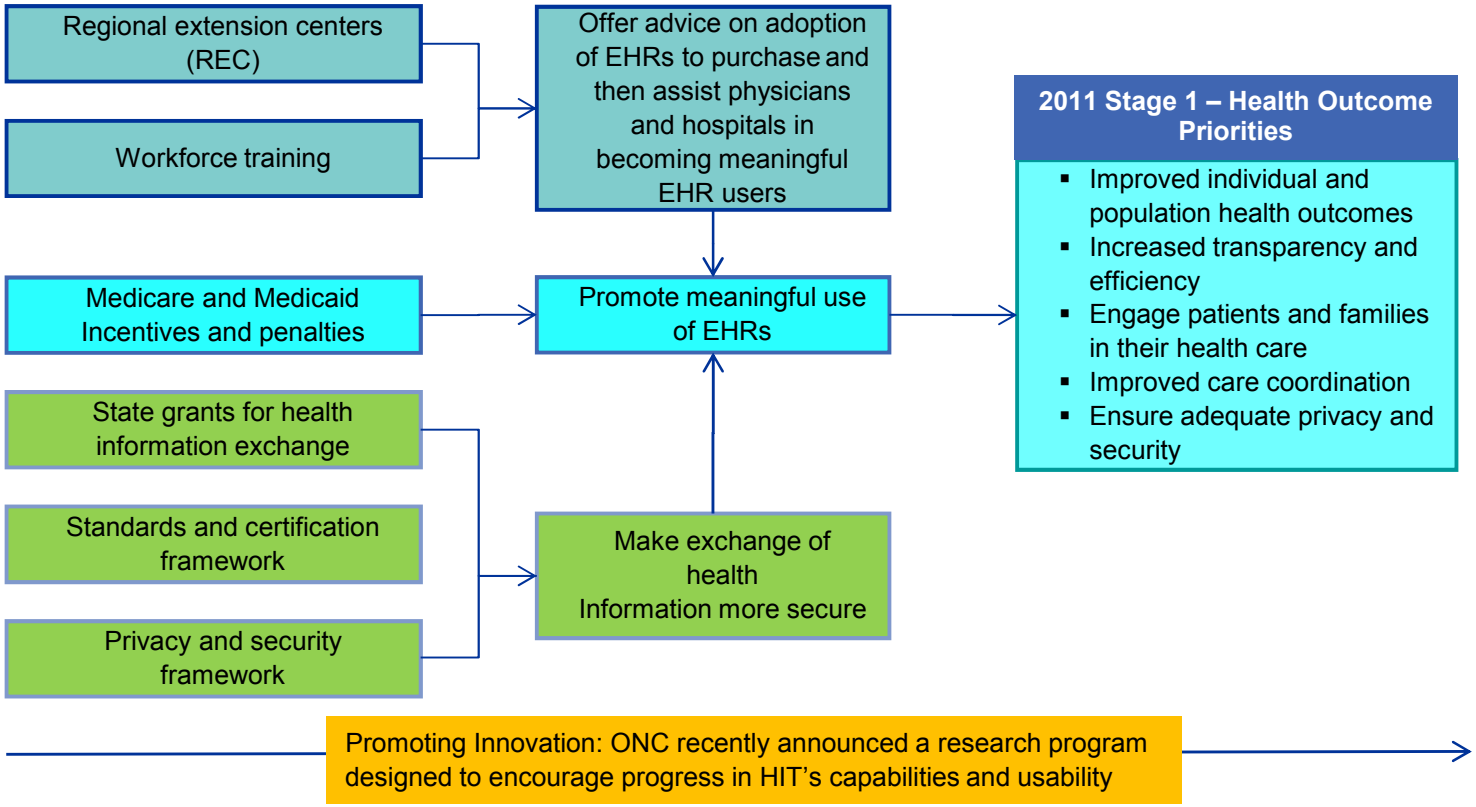
HITECH priority areas include:

- Electronic Health Records (EHR)
- Health Information Exchanges (HIE)
- Security and Data Privacy
- Outcome Registries
- Promotion of Health Information Technology (HIT) Standards and Interoperability

- ARRA includes the HITECH Act to accelerate the adoption of interoperable electronic health records and other HIT, as well as to promote HIE
- The legislation includes provisions intended to shore up public confidence in the use of EHRs and personal health records (PHRs) by beefing up enforcement of and expanding the scope of activities covered by HIPAA Privacy and Security Rules

The HITECH framework supports achievement of Meaningful Use

The HITECH Act program focuses on attaining meaningful use of EHRs as a pathway toward improved health system performance. The attainment of meaningful use depends, in turn, on adoption of EHRs and the development of security and private pathways for exchanging health information. Adoption and exchange will be supported by a variety of HITECH Act initiatives

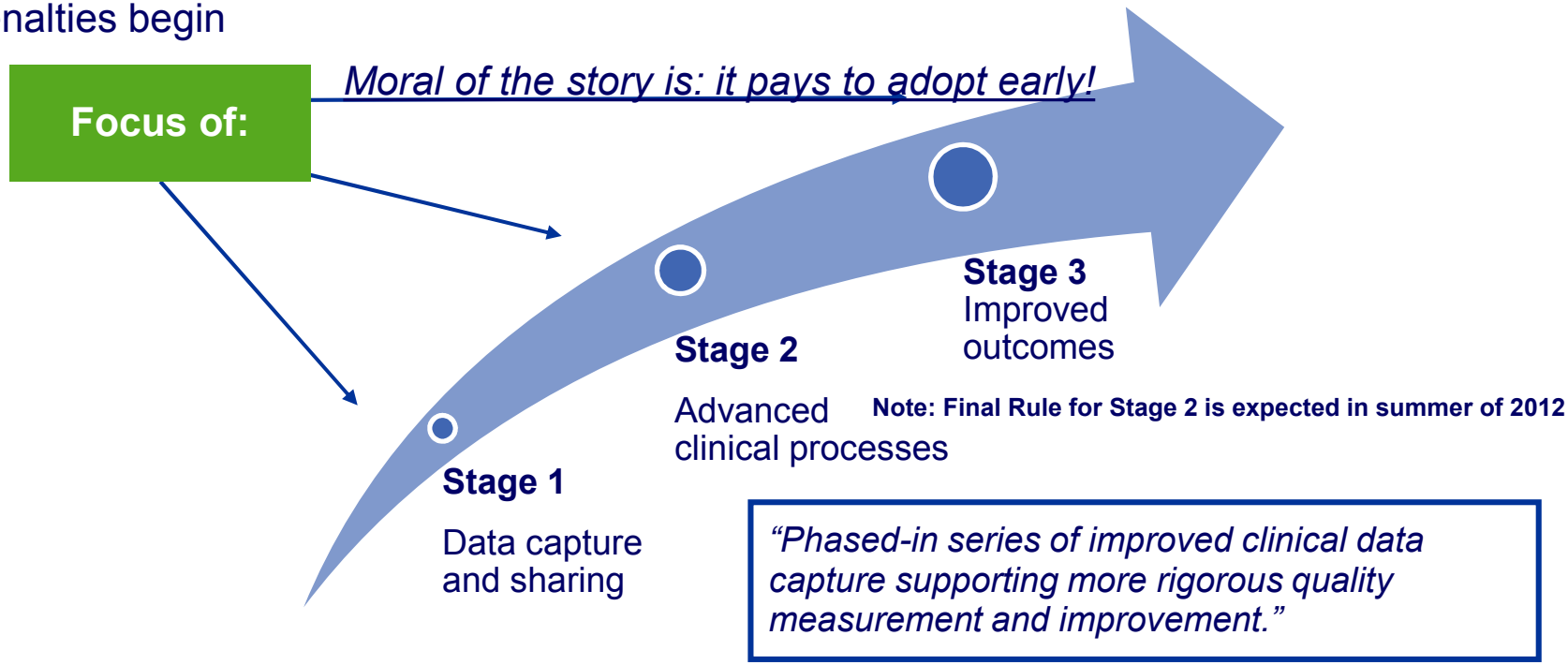


Adapted from The New England Journal of Medicine; David Blumenthal, M.D., M.P.P. "**Launching HITECH"**

ARRA/HITECH is *not* about technology…it's about improving outcomes through the *application and use* of technology. Meaningful Use is derived from this concept.

Staging of meaningful use

- The stages of Meaningful Use represent a graduated approach to arriving at the ultimate goal. Thus, the goals for "Stage 3" Meaningful Use criteria represent overarching goals which, Centers for Medicare and Medicaid Services (CMS) believes, are attainable in the future
- Meaningful Use regulations will be further defined/refined in an "escalator" type approach in bi-yearly stages: 2011, 2013, 2015
- As regulations increase in specificity over time, incentive payments decrease until penalties begin



Connecting for Health, Markle Foundation "Achieving the Health IT Objectives of the American Recovery and Reinvestment Act" April 2009

Meaningful Use stage 1 measures overview

Final Meaningful Use rules have been relaxed and allow flexibility rather than define Meaningful Use objectives and measures as strictly "all-or-nothing." The criteria below define both the "core set" and "menu set" of Meaningful Use objectives outlined in the Final Rules:

"Core set" of Meaningful Use objectives

- Use Computerized Physician Order Entry (CPOE)
- Implement drug-drug and drug-allergy interaction checks
- Generate and transmit prescriptions electronically
- Record patient demographics
- Maintain up-to-date problem list
- Maintain active medication list
- Maintain active medication allergy list
- Report vital signs and chart changes
- Record smoking status for patients 13 years or older
- Implement one clinical decision support rule
- Report clinical quality measures to CMS or States
- Electronically exchange key clinical information among providers and authorized entities
- Provide patients with electronic copy of their health information
- Provide patients with clinical summaries and discharge summaries
- Protect electronic health information created or maintained by certified EHR

Must meet all objectives

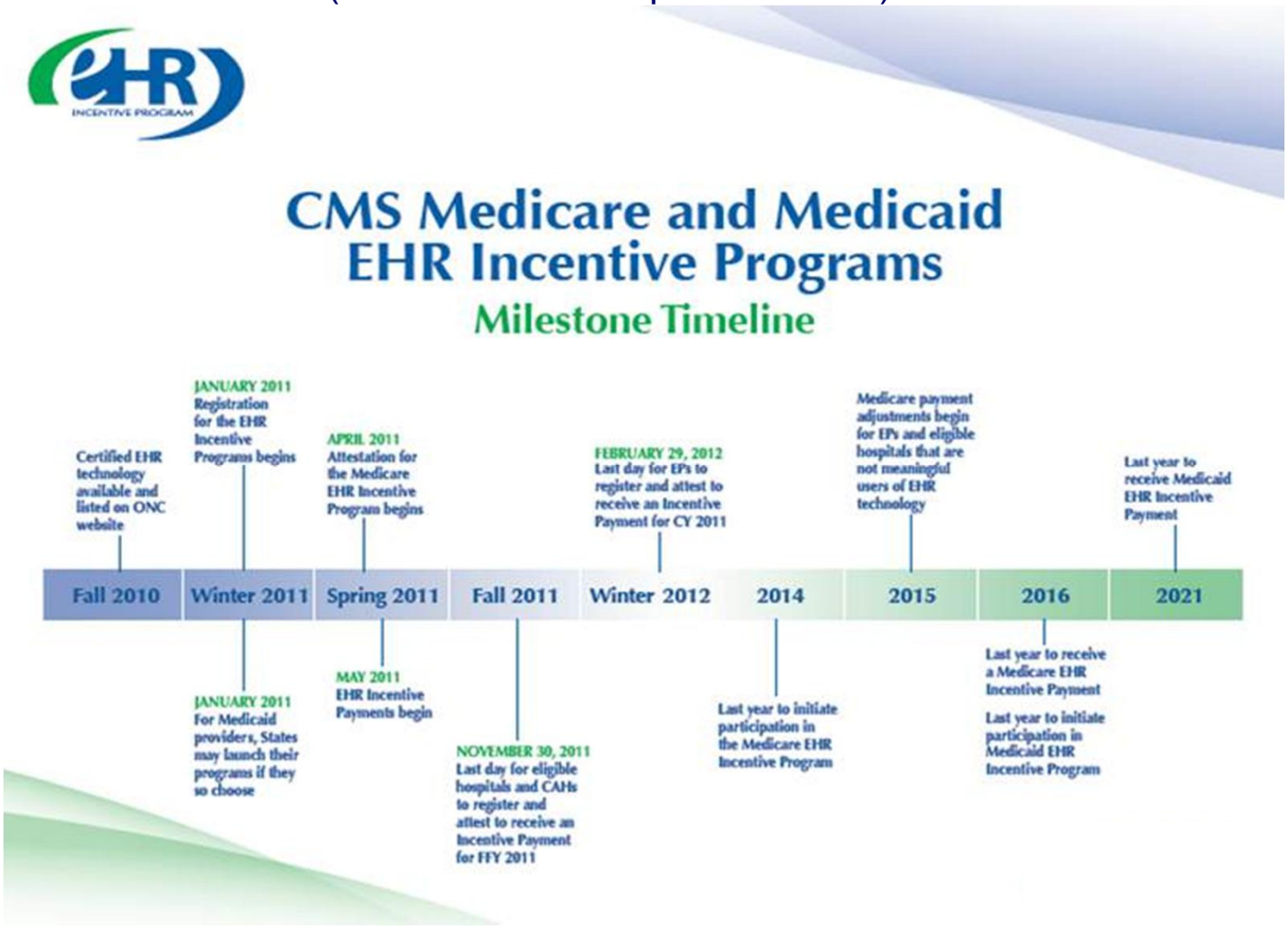
"Menu set" of Meaningful Use objectives

- Implement drug-formulary checks
- Incorporate clinical laboratory test results into EHRs
- Generate lists of patients by specific conditions
- Use EHR to identify patient-specific education resources
- Perform medication reconciliation between care settings
- Provide summary of care record for patients referred/transitioned to another provider
- Submit electronic immunization data to registries or information systems
- Submit electronic syndromic surveillance data to public health agencies
- Additional choices eligible hospitals (EHs) (record advance directives for 65 y/o above; electronic data on lab results to public health agencies)
- Additional choices for eligible professionals (EPs) (reminders to patients for preventive and follow-up care; provide patients with timely electronic access to their health information)

Can defer "5" for Stage 1
(ALL of these become "core set" in Stage 2)

What is the timeline for Eligible Hospitals?

Dates for the Hospital **EHR** Incentive Program for both Medicare and Medicaid are based upon the Federal Fiscal Year (October 1st — September 30th)



HIPAA modifications

On July 8, 2010, the Office for Civil Rights (OCR) released a notice of proposed rulemaking (NPRM), revising the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Enforcement rules in accordance with HITECH provisions. Modifications exist under different phases in the regulatory rule-making process

NPRM published July 14, 2010 (with a 60 day comment period ending September 13, 2010), modifies:

- HIPAA Security Rule
- HIPAA Privacy Rule
- Enforcement Rule

As of August 2, 2010, Rule remains in effect. HHS has withdrawn the rule from OMB review and final rule will be modified and issued in the coming months

- Breach Notification Rule

HIPAA modifications

1. Redefines Business Associates

Business Associates (BAs) redefined

- Note that all definitions apply even if the Covered Entities /Business Associate fails to enter required Business Associate Agreement (BAA)
  - Patient Safety Organizations (PSOs)
  - Health Information Organizations (HIOs) and E-Rx Gateways
  - Vendors offering personal health record (PHR) to one or more individuals on behalf of a covered entity
  - A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate

Compliance & Enforcement

- BAs must directly comply with
  - HIPAA Security Rule administrative, physical, and technical safeguards and documentation requirements
  - Adhere to BAAs
  - HITECH's privacy-related requirements
- BAs are subject to HIPAA civil and criminal enforcement and penalties, in addition to contractual liability

Extend to Subcontractors

- BAs must obtain satisfactory assurances from subcontractors on Privacy and Security protections in the form of a BAA. Covered entities are not required to obtain BAA from subcontractor (Chain of Trust concept)

Proposed HITECH Act modifications

2. Modifies enforcement requirements and penalties

Enforcement

- The NPRM implements a number of HITECH enforcement provisions that were not included in the previously released Interim Final Rule on enforcement
- The NPRM also proposes to make regulatory changes necessary to implement HITECH's imposition of civil money penalty liability on BAs
- The NPRM defines the terms "reasonable cause," "reasonable diligence" and "willful neglect," which relate to the various penalty levels under HIPAA's Enforcement Rule

Compliance Timeline

- Comply with HITECH statutory provisions that became effective on February 18, 2010
- CEs and BAs will have a **grace period of 240 days from publication of a final rule** to come into compliance with the changes
- The NPRM includes transition provisions that permit CEs, BAs and BA subcontractors to continue to operate under existing contracts for up to **one year beyond the compliance date** of the final rule

Proposed HITECH Act modifications

3. Updates HIPAA Privacy Rule

Marketing of PHI	▪ **Marketing** updates include: revise the exceptions to marketing to better distinguish the exceptions for treatment communications from those communications made for health care operations; add a definition of "financial remuneration"; provide that health care operations communications for which financial remuneration is received are marketing and require individual authorization; provide that written treatment communications for which financial remuneration is received are subject to certain notice and opt out conditions; provide a limited exception from the remuneration prohibition for refill reminders; and remove the paragraph regarding an arrangement between a covered entity and another entity in which the covered entity receives remuneration in exchange for protected health information
Sale of PHI	▪ Provides new restrictions on marketing using PHI and payment for PHI ▪ **Sale**: Requires a covered entity to obtain an authorization for any disclosure of protected health information in exchange for direct or indirect remuneration. This authorization must state that the disclosure will result in remuneration to the covered entity; Exceptions generally follow statutory requirements; Prohibits downstream disclosure for remuneration unless separate authorization in place
PHI for deceased individuals	▪ Codifies Period of Protection (50 years); requests comments on this timeframe ▪ Discusses Disclosures About a Decedent to Family Members and Others Involved In Care

Proposed HITECH Act modifications

3. Updates HIPAA Privacy Rule

Health Operations	▪ Modifies the definition of “health care operations” to include a reference to patient safety activities ▪ Communication by a covered entity or business associate that is about a product or service and that encourages recipients of the communication to purchase or use the product or service shall not be considered a health care operation and will now be considered marketing ▪ CEs/BAs may no longer receive payment for any communication now considered to be marketing, change from HIPAA
Research	▪ Compound Authorizations: discusses concerns with Compound Authorizations, and circumstances where they are allowed ▪ Authorizing Future Research Use or Disclosure : discusses allowing authorizations that include future research; makes clear it would not alter an individual’s right to revoke the authorization for the use or disclosure of protected health information for future research at any time; specifically request comment on proposed changes
Disclosure of student immunizations	▪ HHS now regards disclosure of immunization records to schools to be a public health disclosure ▪ Once disclosed to school, information is protected by FERPA rather than HIPAA

Proposed HITECH Act modifications

3. Updates HIPAA Privacy Rule

Notice of Privacy Practices (NPP)	▪ Describes the uses and disclosures of protected health information that require an authorization ▪ Other uses and disclosures not described in notice made only with individual authorization ▪ Authorizations requires for marketing and fundraising ▪ Soliciting comments on whether NPP should contain discussion of CEs obligation re breach notification
Limited data set/minimum necessary	▪ Requires covered entities to consider a limited data set as the minimum necessary for a particular use, disclosure, or request of protected health information, and requires the Secretary to issue guidance to address what constitutes minimum necessary under the Privacy Rule ▪ Requires that a covered entity or business associate that discloses protected health information for public health activities or research in limited data set form is also excepted from the authorization requirement ▪ Requesting comment on guidance needed

Proposed HITECH Act modifications

3. Updates HIPAA Privacy Rule

New Patient Rights

- Extends Patient Access to EHR & Patient Right to Restrict Disclosures
- Requires a covered entity to agree to a restriction on disclosure to a health plan if: (A) the disclosure is for the purposes of carrying out payment or healthcare operations and is not otherwise required by law; and (B) the protected health information pertains solely to a health care item or service for which the individual, or person on behalf of the individual other than the health plan, has paid the covered entity in full
- Clarifies that if a restriction placed on a disclosure to a health plan, the covered entity is also prohibited from making such disclosure to a business associate of the health plan

Fundraising

- Requires CEs to provide individuals with a clear opportunity to opt out of receiving fundraising communications and by requiring that an opt out be treated as a revocation of authorization under the Privacy Rule
- Requires CEs to inform individuals in its notice of privacy practices that it may contact them to raise funds for the covered entity
- Requires that fundraising materials sent contain a description of how the individual may opt out of receiving future fundraising communications
- Requires that a CE may not condition treatment or payment on an individual's choice with respect to receiving fundraising communications

Proposed HITECH Act modifications

3. Updates HIPAA Privacy Rule on Breach Notification

HHS to issue final rule on breach notification

- "HHS is **withdrawing the breach notification final rule from OMB review** to allow for further consideration, given the Department's experience to date in administering the regulations. This is a complex issue and the Administration is committed to ensuring that individuals' health information is secured to the extent possible to avoid unauthorized uses and disclosures, and that individuals are appropriately notified when incidents do occur."
- **Intent to publish a final rule in the Federal Register in the coming months**
- Until such time as a new final rule is issued, the **Interim Final Rule** that became effective on September 23, 2009, **remains in effect**

Speculation for withdrawal of final rule

- Opposition from Congress and privacy advocates to the **"harm standard"** contained in the now-withdrawn regulations. Under the standard, covered entity that discovered unauthorized access to, or acquisition, use or disclosure of, PHI was not required to provide notice of security breach unless the unauthorized conduct "pose[d] a significant risk of financial, reputational or other harm" to the subject of the information
- In the event the "harm standard" is removed, there could be impact for providers and covered entities in increased reporting of incidents and out-of-pocket expense and potential damage to business reputation

Impact to Providers

- Providers must determine whether a security incident should be analyzed with or without the "harm standard" before HHS publishes a final rule in the "coming months"
- Until clarification is issued, providers will make a judgment call to either ignore the harm standard and "over-notify" or apply the standard to justify a decision not to provide notice and run a risk of enforcement action

Q&A

- Are your organizations subject to HITECH and Meaningful Use requirements?
- How would you describe your journey to achieve compliance?
- What actions have been taken to manage third party risks/business associates handling ePHI?

Security and Privacy Requirements for Meaningful Use

Security & privacy for Meaningful Use compliance

Security and privacy is part of the core set of Meaningful Use objectives, specifically to "implement systems to protect privacy & security of patient data in the EHR"; **EHs and EPs must conduct or review a security risk analysis, implement security updates as necessary, and correct identified security deficiencies**

Key Takeaways

- Prescriptive requirements include transport layer security, message integrity, and auditing & logging capabilities as part of **EHR Technology certification**
- Breach notification process and response considered an active requirement for EHs and EPs

Key Challenges

- Standards-based security risk analysis methodology, process, and enablement
- Compliance initiatives in addition to Meaningful Use must be addressed, including HIPAA Privacy & Security and ICD-10 implementation
- Maturity of EHR Technology, specifically security and privacy functionality in line with criteria
- Security & privacy to support interoperability – e.g. establishing trust in HIE deployment

Implications

- Adoption of a security risk analysis process and scope to demonstrate completion of Stage 1 measure
- EPs may have to carry the burden of managing systems and application security as EHR is deployed
- Improvement in enterprise security management, privacy and compliance, and governance
- Investment in data protection solutions to limit regulatory and reputational risk as a result of a security breach

Security & privacy for Meaningful Use compliance

Health Outcome # 5	**Ensure adequate privacy and security protections for personal health information** Care goals: ▪ Ensure **privacy and security** protections for confidential information through operating policies, procedures, and technologies and compliance w/applicable law ▪ Provide transparency of data sharing to patient
Objective	Protect electronic health information created or maintained by the **certified EHR technology** through the implementation of **appropriate technical capabilities**
Measure	Conduct or review a **security risk analysis** per 45 CFR164.308 (a)(1) and **implement security updates** as necessary and **correct identified security deficiencies** as part of its risk management process

Questions for health care providers for Stage 1 measure

1	**Have you implemented the certified EHR?**
2	**If yes, have you conducted a security risk analysis?**
3	**If yes, have you applied the security updates or corrected the deficiencies based on the risk analysis?**

Security risk analysis

Health care providers and covered entities must conduct a security risk analysis as per 45 Code of Federal Regulations (CFR) 164.308 (a)(1) – based on the HIPAA Security Rule.

Security Risk Analysis per 45 CFR 164.308 (a)(1):	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the [organization].

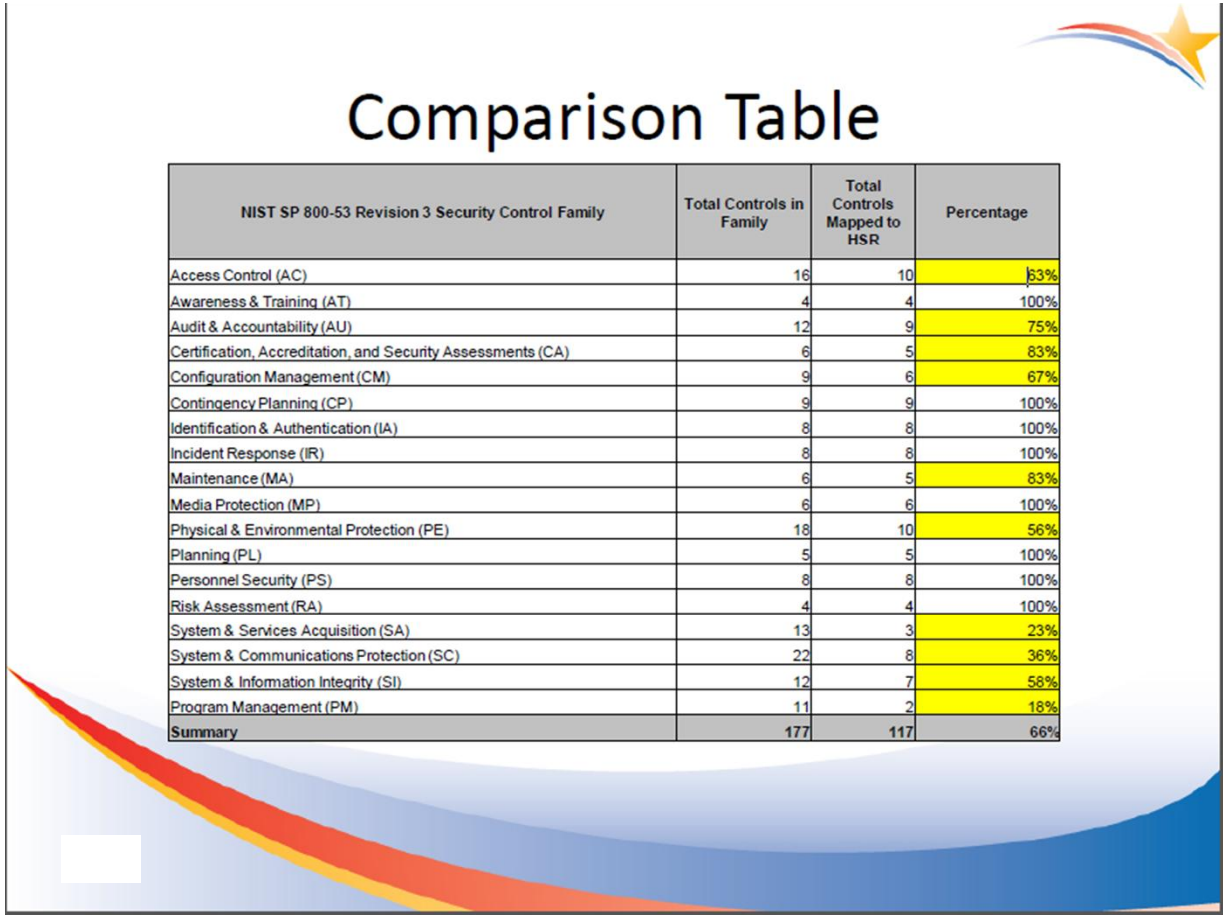
Numerous methods of performing risk analysis exist and there is no single method that guarantees compliance with the Security Rule. Regardless of the method employed, security risk analysis should be comprised of the following elements

Key Elements	• Scope • Data Collection • Identify & Document Potential Threats & Vulnerabilities • Assess Current Security Measures • Determine Likelihood of Impact of Threat Occurrence • Determine level of risk • Finalize documentation • Periodic review and updates to risk assessment
Risk analysis Methods & templates	• NIST 800-30 • Healthcare Information and Management Systems Society (HIMSS) • Health Information Trust Alliance (HITRUST)

What do we know about security & privacy for stage 2

- The HIT Policy Committee Security & Privacy Tiger Team recently (November 2011) conducted an analysis between the HIPAA Security Rule and well known security frameworks (e.g. NIST 800-53, HITRUST, etc..)
- Gaps exist between the HIPAA Security Rule and other commonly used security frameworks (see next slide)
- The "framework" approach used in other contexts (FISMA, ISO, etc.) seems to allow for more frequent updating to keep up with innovation
- The Tiger Team has made recommendations to the HIT Policy Committee to do a more thorough gap analysis

What do we know about security & privacy for stage 2



Comparison Table

NIST SP 800-53 Revision 3 Security Control Family	Total Controls in Family	Total Controls Mapped to HSR	Percentage
Access Control (AC)	16	10	63%
Awareness & Training (AT)	4	4	100%
Audit & Accountability (AU)	12	9	75%
Certification, Accreditation, and Security Assessments (CA)	6	5	83%
Configuration Management (CM)	9	6	67%
Contingency Planning (CP)	9	9	100%
Identification & Authentication (IA)	8	8	100%
Incident Response (IR)	8	8	100%
Maintenance (MA)	6	5	83%
Media Protection (MP)	6	6	100%
Physical & Environmental Protection (PE)	18	10	56%
Planning (PL)	5	5	100%
Personnel Security (PS)	8	8	100%
Risk Assessment (RA)	4	4	100%
System & Services Acquisition (SA)	13	3	23%
System & Communications Protection (SC)	22	8	36%
System & Information Integrity (SI)	12	7	58%
Program Management (PM)	11	2	18%
Summary	**177**	**117**	**66%**

Q&A

- How frequently does your organization perform an information security risk assessment?
- How would you characterize the risk assessment - e.g. application vs. process based, stakeholders involved, risk management process, alignment with privacy, reporting?
- How does Internal Audit support your information security risk assessments?
- Does your organization leverage a “framework” approach to information security and privacy?


Electronic Health Record (EHR)
System Certification

Certification versus Meaningful Use

While certification will now be an almost mandatory result of the Meaningful Use incentives program, it is not the end goal.

Certification will focus on identifying a set of core functional requirements that align with HITECH payment incentives. Coordination will be required to ensure that certification timelines don't interfere with providers' ability to achieve Meaningful Use.

Certification

- Objective measure of an EHR's technical capabilities
- Establishes meaningful baseline for functionality
- Will leverage competitive forces on vendors based on compliance
- Drives vendors toward consistency
- 50% to 75% of EHR market offerings are certified products already – without this legislation

Meaningful Use

- Qualitative measure of EHR adoption
- Highly dependent upon implementation, training, support, leadership and governance
- Difficult to achieve regardless of certification status
- Drives providers toward significant change

Stage 1 – privacy and security certification criteria

Rule	Interim final certification criterion	Final certification criterion	Comments
§170.302(o) - Access control	Interim Final Rule Text: Access control. Assign a unique name and/or number for identifying and tracking user identity and establish controls that permit only authorized users to access electronic health information.	Final Rule Text: §170.302(o) Unchanged	
§170.302(p) - Emergency access	Interim Final Rule Text: Emergency access. Permit authorized users (who are authorized for emergency situations) to access electronic health information during an emergency.	Final Rule Text: §170.302(p) Unchanged	
§170.302(q) - Automatic log-off	Interim Final Rule Text: Automatic log-off. Terminate an electronic session after a re-determined time of inactivity.	Final Rule Text: §170.302(q) Unchanged	
§170.302(r) - Audit log	Interim Final Rule Text: (1) Record actions. Record actions related to electronic health information in accordance with the standard specified in §170.210(b). (2) Alerts. Provide alerts based on user-defined events. (3) Display and print. Electronically display and print all or a specified set of recorded information upon request or at a set period of time.	Final Rule Text: §170.302(r) (1) Record actions. Record actions related to electronic health information in accordance with the standard specified in §170.210(b). (2) Generate audit log. Enable a user to generate an audit log for a specific time period and to sort entries in the audit log according to any of the elements specified in the standard at 170.210(b).	Removed ‘alerts’ from final rule.

Stage 1 – privacy and security certification criteria

Rule	Interim final certification criterion	Final certification criterion	Comments
§170.302(s) - Integrity	Interim Final Rule Text: (1)In transit. Verify that electronic health information has not been altered in transit in accordance with the standard specified in §170.210(c). (2) Detection. Detect the alteration and deletion of electronic health information and audit logs, in accordance with the standard specified in §170.210(c).	Final Rule Text: §170.302(s) (1) Create a message digest in accordance with the standard specified in 170.210(c). (2) Verify in accordance with the standard specified in 170.210(c) upon receipt of electronically exchanged health information that such information has not been altered. (3) Detection. Detect the alteration of audit logs.	Added create language in final rule.
§170.302(t) - Authentication	Interim Final Rule Text: (1)Local. Verify that a person or entity seeking access to electronic health information is the one claimed and is authorized to access such information. (2)Cross network. Verify that a person or entity seeking access to electronic health information across a network is the one claimed and is authorized to access such information in accordance with the standard specified in §170.210(d).	Final Rule Text: §170.302(t) Authentication. Verify that a person or entity seeking access to electronic health information is the one claimed and is authorized to access such information.	Removed 'Cross Network' in final rule.

Stage 1 – privacy and security certification criteria

Rule	Interim final certification criterion	Final certification criterion	Comments
§170.302(u) - Encryption	Interim Final Rule Text: (1) General. Encrypt and decrypt electronic health information according to user-defined preferences in accordance with the standard specified in §170.210(a)(1). (2) Exchange. Encrypt and decrypt electronic health information when exchanged in accordance with the standard specified in §170.210(a)(2).	Final Rule Text: §170.302(u) General encryption. Encrypt and decrypt electronic health information in accordance with the standard specified in §170.210(a)(1), unless the Secretary determines that the use of such algorithm would pose a significant security risk for Certified EHR Technology. §170.302(v) Encryption when exchanging electronic health information. Encrypt and decrypt electronic health information when exchanged in accordance with the standard specified in §170.210(a)(2).	Added consideration for 'risk' in final rule.

Certified EHR vendors

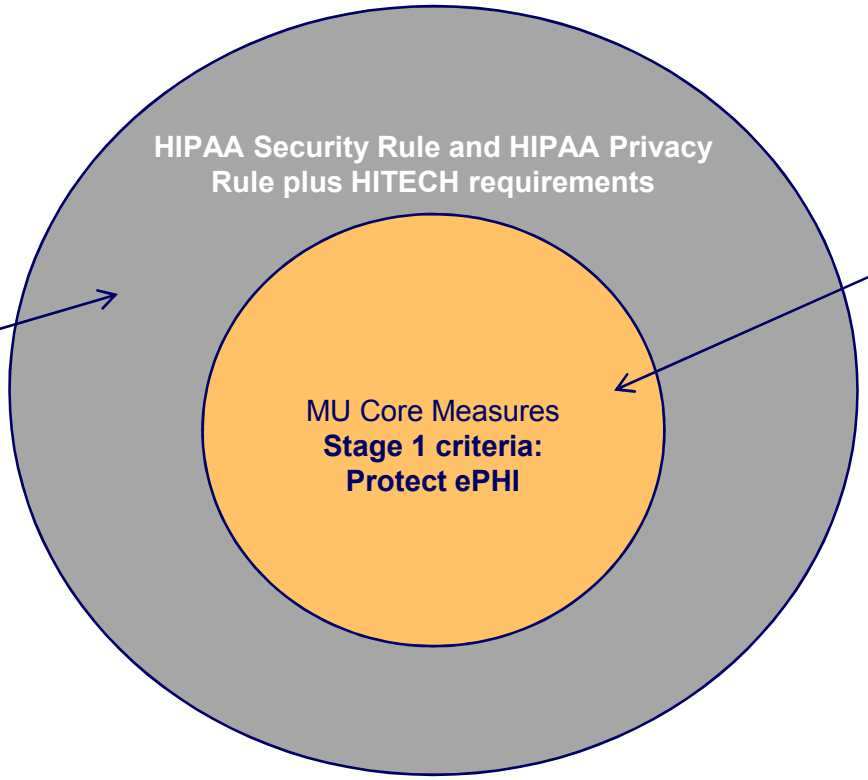
- **The Certified HIT Product List (CHPL)** provides the authoritative, comprehensive listing of Complete EHRs and EHR Modules that have been tested and certified under the Temporary Certification Program maintained by the Office of the National Coordinator for Health IT (ONC). Each Complete EHR and EHR Module listed below has been certified by an ONC-Authorized Testing and Certification Body (ONC-ATCB) and reported to ONC. Only the product versions that are included on the CHPL are certified under the ONC Temporary Certification Program.

- List of certified EHR Technology: http://onc-chpl.force.com/ehrcert

- List of FAQ for certification: http://questions.cms.hhs.gov/app/answers/list/p/21,26,1058

HIPAA Security/Privacy plus MU

Focus is on protecting ePHI and PHI within the organization via Administrative, Physical and Technical Safeguards



Primary focus is on EHR's ability to protect ePHI created/maintained by the EHR via "appropriate technical capabilities"

You Have to do BOTH

Many healthcare providers will require risk assessment frameworks, control frameworks and technology solutions to address HIPAA Security, Privacy, HITECH and MU


Security Risk Analysis
Approach and Methodology

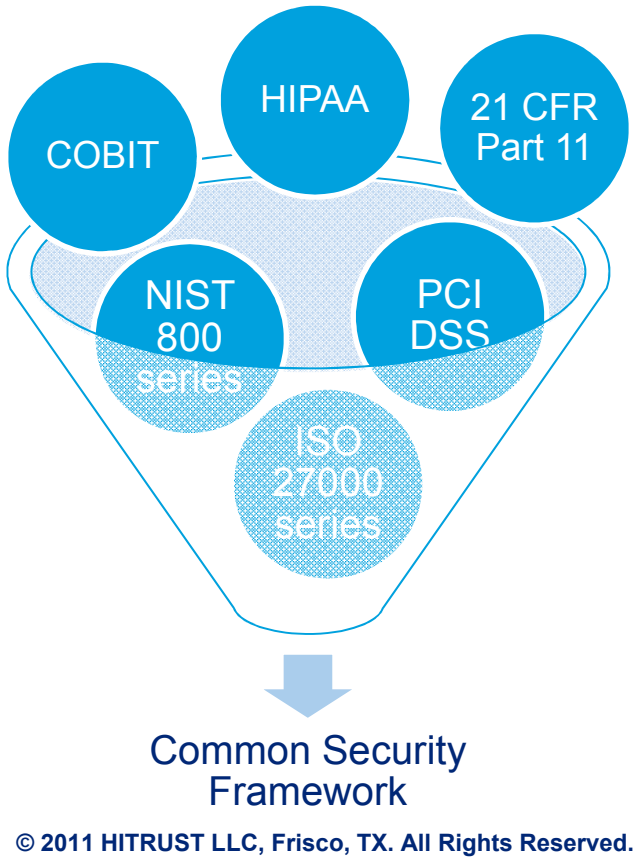
Adoption of a common security framework - HITRUST

The Health Information Trust Alliance (HITRUST)

- Private, independent company (**near non-profit status**)
- Standardizing a higher level of security to build greater trust in the electronic flow of information through the health care system
- Collaborating with health care, business, technology, and information security leaders
- Certifiable framework that any and all organizations in the health care industry can implement and be certified against

Common Security Framework (CSF)

- First IT security framework for health information
- Set of standards for security governance and control practices
- Based on leading information security standards as well as regulatory requirements
    - e.g., HIPAA security rule, ISO 27002, and NIST 800-53r3



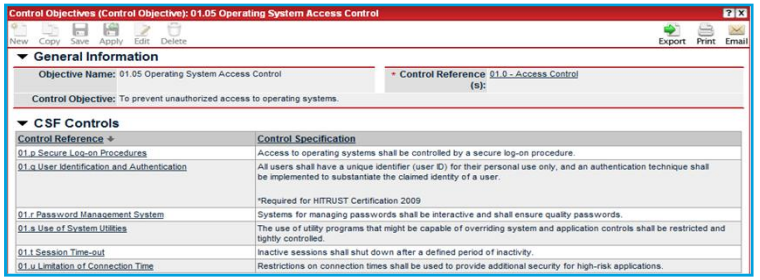
HITRUST CSF overview

Common Security Framework (CSF) components

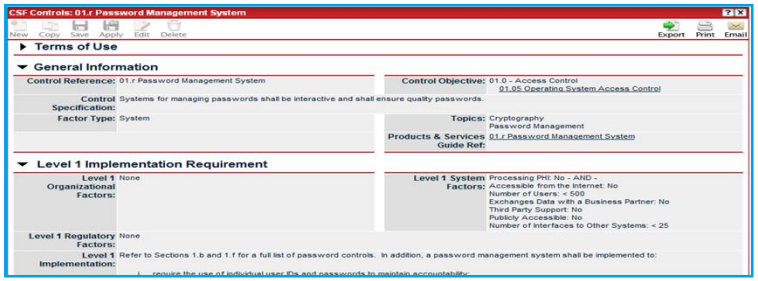
- **Security controls**
  - 13 control categories
  - 43 control objectives
  - 136 control specifications
- **Three levels** of requirements based on organization's scale & operations
- **Implementation & audit guidance**
- Maps controls to **authoritative sources**
- Process for approving **alternate controls** (compensating and mitigating) for systems that are not in compliance
- **Security Configuration Packs** will recommend configuration and maintenance of security in critical applications (e.g., electronic health medical record systems and medical devices)
- **Products and Services Guide** link to solutions based on CSF

Control category

Control objective



Control specification

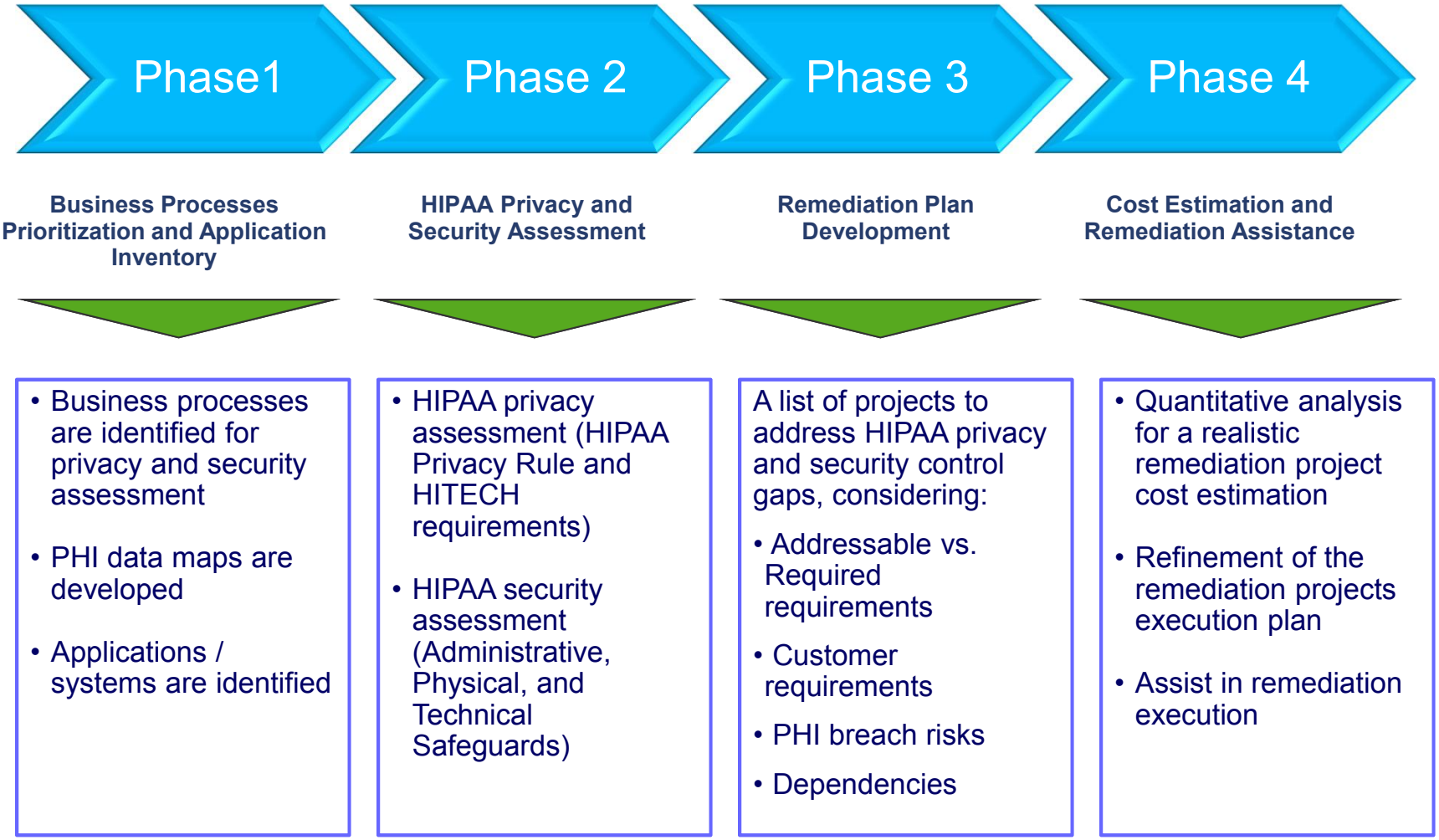


Authoritative sources

Source: http://hitrustalliance.net/csf/

Perspectives and insights: high level approach

The following describes Deloitte's approach for executing a security risk analysis for HITECH/HIPAA.



Business processes prioritization and application inventory

Steps

Business processes containing ePHI are analyzed and risk- prioritized for the privacy and security assessment:

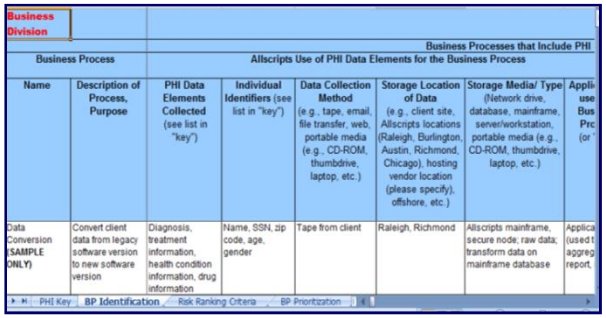
1. Send the Business Process Identification and Risk Ranking spreadsheet to key business contacts to identify processes where ePHI is collected, stored, processed, and transferred.

2. Review the Business Process Identification and Risk Ranking spreadsheet with the key business contacts to determine high risk processes where ePHI is involved.
3. Create data flow maps to describe high risk business processes involving ePHI.

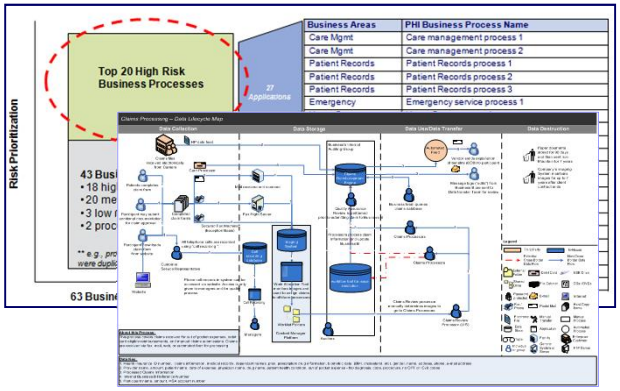
4. Identify and assess the security of applications that are managed by the client or the client is responsible for the security and maintenance of in support of identified business processes.

Tools/Accelerators

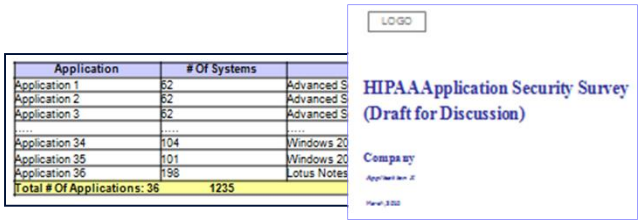
Business Process Identification and Risk Ranking



Business Process Inventory



Application Inventory



HIPAA privacy and security assessment

Steps

Interviews and workshops with key personnel from business, clinical, and IT and functional areas are conducted:

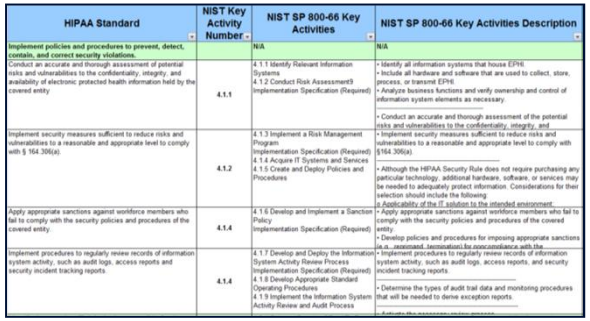
1. Identify the privacy and security control gaps against the HIPAA Privacy Rule and Security Rule requirements (using NIST SP800-66) and HITECH requirements.

2. Work with key client personnel to assess the risk, likelihood and impact of the identified gaps.

3. Assist client with briefing executive management on HIPAA Privacy and Security risks found during the assessment.

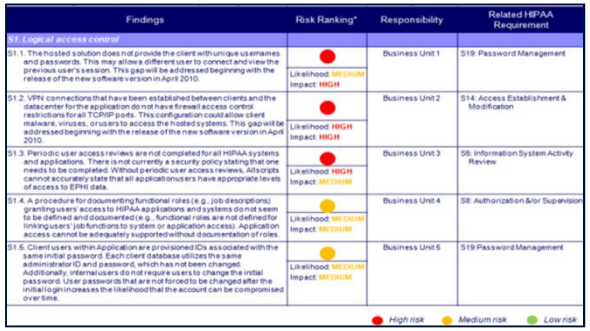
Tools/Accelerators

HIPAA Privacy and Security Assessment



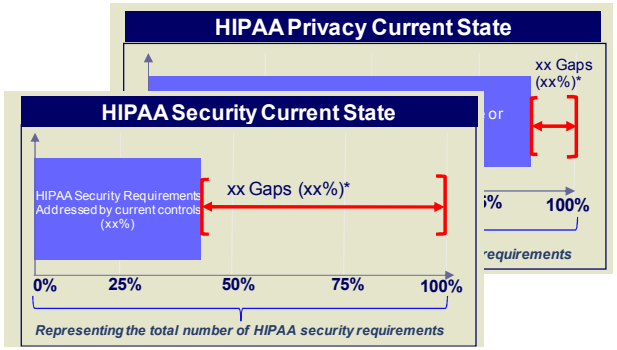
HIPAA Standard	NIST Key Activity Number	NIST SP 800-66 Key Activities	NIST SP 800-66 Key Activities Description
Implement policies and procedures to prevent, detect, contain, and correct security violations.		N/A	N/A
Conduct an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity	4.1.1	4.1.1 Identify Relevant Information Systems 4.1.2 Conduct Risk Assessment§ Implementation Specification (Required)	• Identify all information systems that house EPHI. • Include all hardware and software that are used to collect, store, process, or transmit EPHI. • Analyze business functions and verify ownership and control of information system elements as necessary. • Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and
Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).	4.1.2	4.1.3 Implement a Risk Management Program Implementation Specification (Required) 4.1.4 Acquire IT Systems and Services 4.1.5 Create and Deploy Policies and Procedures	• Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a). • Although the HIPAA Security Rule does not require purchasing any particular technology, additional hardware, software, or services may be needed to adequately protect information. Considerations for their selection should include the following: a Applicability of the IT solution to the intended environment
Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.	4.1.4	4.1.6 Develop and Implement a Sanction Policy Implementation Specification (Required)	• Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity. • Develop policies and procedures for imposing appropriate sanctions (e.g., reprimand, termination) for noncompliance with the
Implement procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports.	4.1.4	4.1.7 Develop and Deploy the Information System Activity Review Process Implementation Specification (Required) 4.1.8 Develop Appropriate Standard Operating Procedures 4.1.9 Implement the Information System Activity Review and Audit Process	• Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. • Determine the types of audit trail data and monitoring procedures that will be needed to derive exception reports.

Detailed HIPAA Privacy and Security Control Gap Details



Findings	Risk Ranking*	Responsibility	Related HIPAA Requirement
s1.1 Logical access control			
S1.1. The hosted solution does not provide the client with unique usernames and passwords. This may allow a different user to connect and view the previous user's session. This gap will be addressed beginning with the release of the new software version in April 2010.	Likelihood: MEDIUM Impact: HIGH	Business Unit 1	S19: Password Management
S1.2. VPN connections that have been established between clients and the datacenter for the application do not have firewall access control restrictions for all TCP/IP ports. This configuration could allow client malware, viruses, or users to access the hosted systems. This gap will be addressed beginning with the release of the new software version in April 2010.	Likelihood: HIGH Impact: HIGH	Business Unit 2	S14: Access Establishment & Modification
S1.3. Periodic user access reviews are not completed for all HIPAA systems and applications. There is not currently a security policy stating that one needs to be completed. Without periodic user access reviews, ARscripts cannot accurately state that all applications users have appropriate levels of access to EPHI data.	Likelihood: HIGH Impact: MEDIUM	Business Unit 3	S6: Information System Activity Review
S1.4. A procedure for documenting functional roles (e.g., job descriptions) granting users' access to HIPAA applications and systems do not seem to be defined and documented (e.g., functional roles are not defined for linking users' job functions to system or application access). Application access cannot be adequately supported without documentation of roles.	Likelihood: MEDIUM Impact: MEDIUM	Business Unit 4	S8: Authorization &/or Supervision
S1.5. Client users within Application are provisioned IDs associated with the same initial password. Each client database utilizes the same administrator ID and password, which has not been changed. Additionally, internal users do not require users to change the initial password. User passwords that are not forced to be changed after the initial login increases the likelihood that the account can be compromised over time.	Likelihood: MEDIUM Impact: MEDIUM	Business Unit 5	S19:Password Management
	High risk	Medium risk	Low risk

HIPAA Privacy and Security Control Gap Summary



Remediation plan development

Steps

Identified gaps are aggregated into remediation projects:

1. Aggregate the gaps into remediation projects in synergy with the responsible parties and with consideration of other projects that are occurring in the organization.

2. Perform a cost/benefit analysis following a qualitative approach to help determine the first level prioritization of the remediation projects.
3. Based on workshops with the key business contacts, determine the estimated duration, deliverables, resources and the dependencies of the remediation projects.

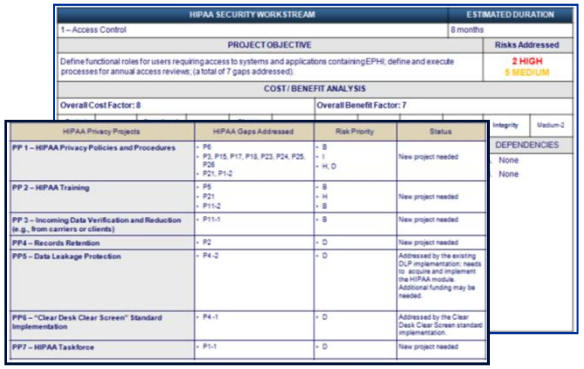
4. Provide recommended priority and timelines of proposed projects.

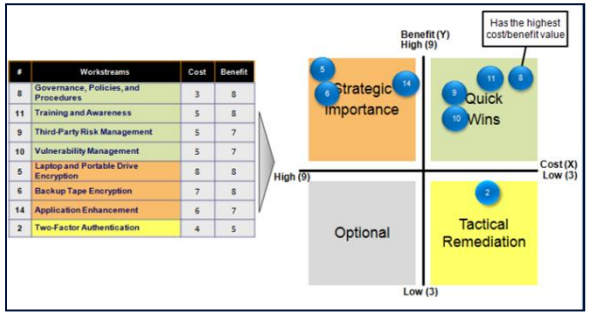
Recommended Workstream Groupings

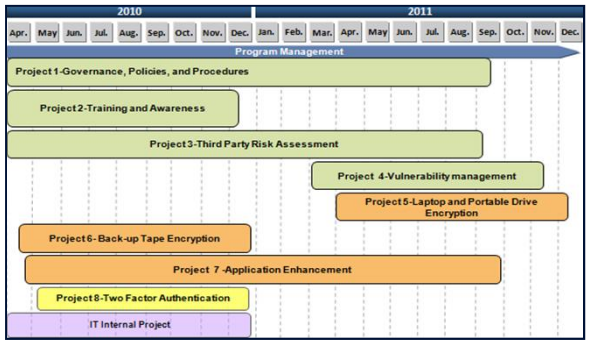
Cost/Benefit Analysis

Recommended Project Implementation Roadmap

Tools/Accelerators







Cost estimation and remediation assistance

Steps

Detailed cost estimation for the remediation workstreams is performed:

1. Perform a quantitative analysis for a realistic estimation of the remediation projects costs and an in-depth prioritization of the remediation projects.

2. Refinement of the remediation projects execution plan. Identify those remediation projects that are optional, should be executed or must be executed.

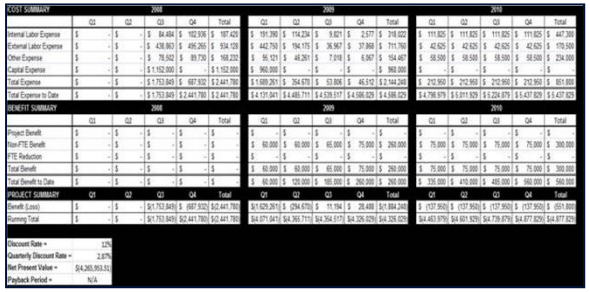
3. Socialize the cost/benefit analysis and actual estimated cost with executive management.

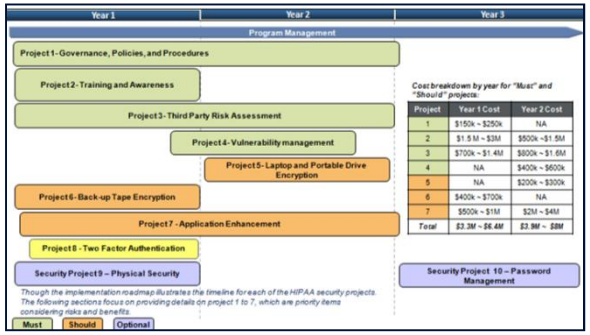
Detailed Cost Estimation

Refined Project Implementation Roadmap

Prioritized Remediation Projects

Tools/Accelerators





Audit considerations

Preparing for an HHS OCR HIPAA Security and Privacy Audit

- HIPAA Privacy Rule
  - Are policies and procedures up-to-date?
  - Have all policies and procedures been implemented?
  - Do policies and procedures actually work?
  - Have all appropriate stakeholders been adequately trained on the HIPAA Privacy Rule?
  - Is evidence of training documented?
  - Do you have a clear, written sanctions policy?
  - Has sanctions policy been applied consistently?

See http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.htm for official guidance from HHS OCR

Audit considerations

Preparing for an HHS OCR HIPAA Security and Privacy Audit

- HIPAA Security Rule
  - Not a checklist of controls approach
  - Do you have a risk management framework in place?
  - Can you provide evidence that the risk management framework is leveraged as a normal course of business?
  - Can you trace the HIPAA Security Rule to your actual policies and procedures?
- Top areas of HHS OCR Auditor focus[1]:
  - Reasonable audit of access logs
  - Security incident detection/response
  - Secure wireless network
  - User-ids and passwords
  - Encryption of mobile devices
  - Up-to-date software (e.g. OS, anti-virus, etc..)
  - Role-based access

[1]Source: IAPP "The Upcoming OCR HIPAA Audit Program..", July 28, 2011


Emerging Trends

The mobility imperative

The increased adoption of devices has created an imperative for mobility that healthcare organizations cannot ignore. Members, patients, caregivers and employees demand the use of these devices in the field.

"Over half of consumers (52%) say they **would use a smart phone or PDA to monitor their health** if they were able to access their medical records and download information about their medical condition and treatments"[1]

"Use of **social networking sites** for healthcare purposes… was **primarily for sharing personal health care experiences** or for **seeking information** on pharmaceutical products"[1]

"The number of smart phones sold in the United States rose more than 60%, from 26 million in 2008 to **42 million in 2010**. Another 25 million consumers are expected to purchase smart phones by 2012."[2]

"More than 1.3 million healthcare professionals, including 50 percent of U.S. physicians, **use Epocrates** to help improve patient care and practice efficiencies with its drug reference, educational and clinical apps"[3]

Sources:
1 – "2011 Survey of Health Care Consumers in the United States: Key Findings, Strategic Implications." Deloitte Center for Health Solutions, 2011.
2 – "Mobile banking: A catalyst for improving bank performance." Deloitte Consulting, 2010.
3 – http://www.epocrates.com/company/
4 - http://manhattanresearch.com/News-and-Events/Press-Releases/physician-iphone-ipad-adoption

Some examples of current mobile device usage

Third party medical apps

- Use of medical calculators and medical libraries (e.g., Epocrates)
- Multiple other apps targeted at different clinical specialties

Video interaction

- Physician-to-physician and physician-to-patient interaction
- Video consultation is very useful for visual symptoms (patient's stroke, etc.)
- Video follow-up with patients increases consistency of taking medications

Real-time patient readings

- Outfitting cardiologists with smartphones to view and provide a reading on EKG in real-time for patients with cardiac diagnosis
- Outfitting clinicians with smartphones to receive real-time waveform patterns, bedside alarms, and other patient data directly from bedside devices, EHRs, etc..

AirStrip Technologies

Security and risk management

Complex organizations will have many mobility use cases and associated security and privacy risks. A monolithic 'one size fits all' approach while tempting from an operational perspective, is unlikely to be successful. A principle based, adaptable, programmatic strategy is critical.

Core Principles	Key Considerations
Define the key business drivers and objectives for mobility	• Identify the mobility opportunities for the organization • Analyze the opportunities to understand the potential value they can deliver • Value becomes the basis for the necessary risk v. reward analysis
Understand the specific mobility use cases	• Articulate the specifics for each use case – the actors, actions, conditions, data types, etc. • Not all use cases are created equal – prioritize based on value and realize that your use cases will evolve (and will need to be reassessed)
Identify the material risks related to each use case	• Define your mobile ecosystem and the integration points with your technology environment • Define risk prioritization criteria, evaluate the risks associated with each use case and prioritize for mitigation • When considering risks, look at your entire mobile ecosystem; evaluate key categories of mobile risk -- operational, legal and regulatory, technology and data protection and, infrastructure and device • When considering mitigations look across your entire environment (it's not just about securing the device)
Implement security controls through policy and technology	• Certain risks may be mitigated by technical controls, others through policy – both will be necessary • Consider a device, data or application centric approach – complex entities will likely want to consider a combination of all three • Don't underestimate the importance of UX – design for consumer expectations, not corporate user tolerance
Enable, not disable adoption of new innovations	• NFC, location based services, special purpose add on hardware, new virtualization solutions, shifts in the vendor landscape, etc. will all continue to change the game • Recognize that mobility is changing at a torrid pace and what works today may not work in 18 months • Develop a program that is principle and process based so you can adapt

Networked Biomedical Devices: Security and Privacy Challenges

- Risks and Challenges

Healthcare providers using "networked" medical devices that collect, store and process patient health data identified the following challenges:

Healthcare Provider Challenges

Inadequate Anti-Virus Management
- Poor to no alert/notification process from vendors on security vulnerabilities impacting their products
- Vendors slow to respond with patches/fixes for worms/viruses that are discovered

Inadequate Encryption
- Most vendors are unable to encrypt patient health data that their products collect
- Even if an encryption solution exist, it might not meet FIP 140-2 encryption requirements

Limited Security Restrictions
- Products have very limited capability to address access privilege changes

Limited Monitoring and Auditing
- Products have very limited capability to record and time-stamp data adds/moves/deletes
- Audit logs are not easily importable into external security audit tools

Ownership of Remediation
- Healthcare providers believe that the medical device vendor is responsible for appropriately developing security controls in their products
- Vendors have not met all HIPAA security requirements

Risks

- *ePHI breaches leading to:*
  - *Penalties*
  - *Regulatory investigations*
  - *Brand issues*
- *Patient Safety*
- *Non-compliance with regulatory requirements*

Networked Biomedical Devices: Security and Privacy Challenges

- FDA "Guidance for Industry: Cyber Security for Networked Medical Devices containing Off the Shelf (OTS) Software"[1]

The Center for Devices and Radiological Health, FDA, has issued a guidance document for manufacturers.

SCOPE	EXAMPLES
• Use OTS software • Can connect to networks, such as a private intranet or the public Internet • Need updates or patches because their OTS software is found vulnerable to viruses, worms, and other threats.	• systems that obtain, archive, and communicate pictures on networks within healthcare facilities, such as computed tomography (CT), • magnetic resonance (MR), ultrasound (US), nuclear medicine (NM), and endoscopy • systems that monitor patient activity, such as electrocardiographic (ECG) systems • systems that communicate with clinical laboratory analyzers, such as laboratory information systems

Based on FDA's CFR Part 820 Quality System Regulation and covers:

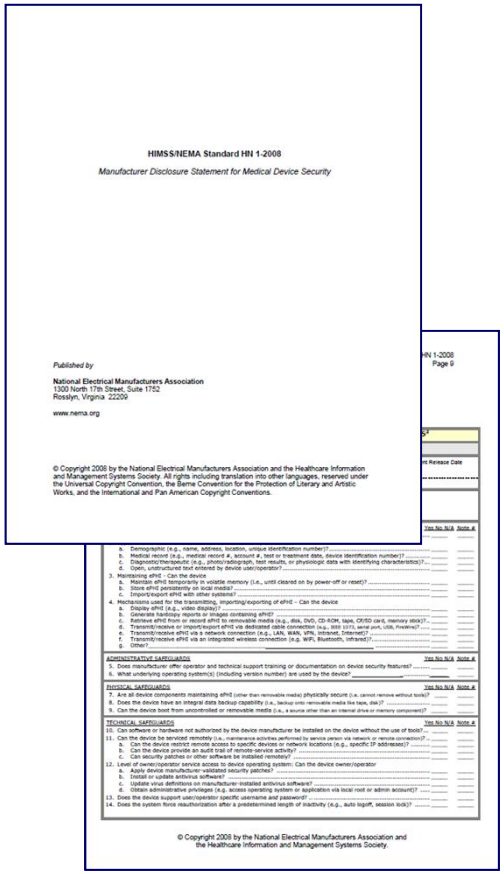
- *Safety and Effectiveness*
- *Data quality (detection and correction)*
- *Virus and malicious code detection*
- *Patch Management*
- *Data Protection*

[1] http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm

Customer Security and Privacy Challenges

- Industry Response

HIMSS/NEMA Standard HN 1-2008 - Manufacturer Disclosure Statement for Medical Device Security



Goal:

- Manufacturer Disclosure Statement for Medical Device Security (MDS2 form)
- Intent to supply healthcare providers with important information to assist them in assessing the vulnerability and risks associated with protecting ePHI transmitted or maintained by medical devices.

Benefit:

- Allows manufacturers to quickly respond to a potentially large volume of information requests from providers regarding the security related features of the medical devices they manufacture
- Facilitates the providers' review of the large volume of security-related information supplied by the manufacturers.
- Supplies information important to providers who must comply with HIPAA privacy and security rules
- Outside the US, useful for providers wanting to address regional regulations such as EU 95/46 (Europe), Act on the Protection of Personal Information (Act No. 57 of 2003, Japan), and PIPEDA (Canada).

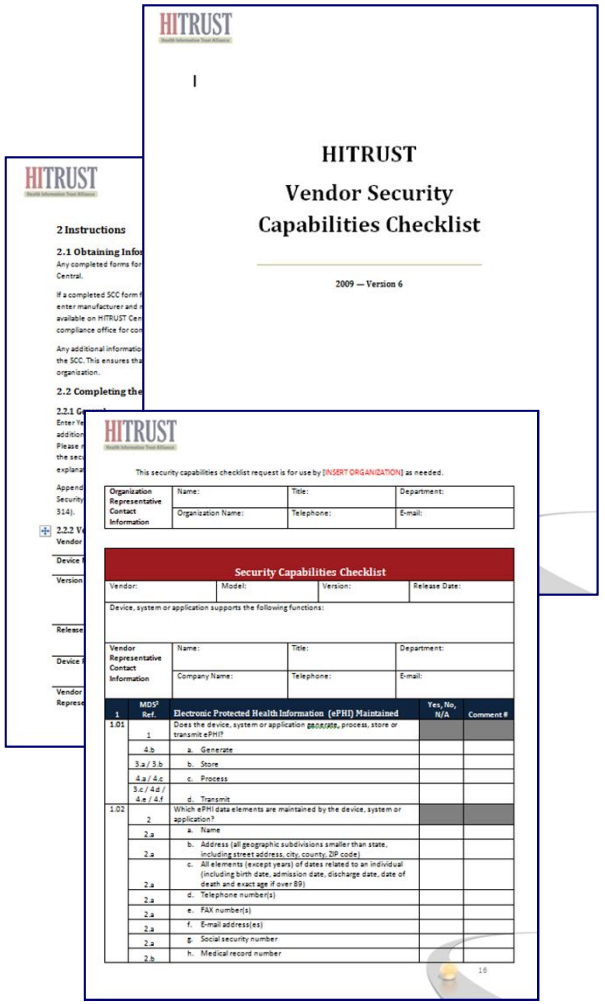
Customer Security and Privacy Challenges

- Industry Response

HITRUST Vendor Security Capabilities Checklist (SCC)

Goal:

- Provide a framework for the implementation of reasonable and appropriate security controls
- Relates to the HITRUST Common Security Framework (CSF)
- Establishes a list of security controls considered as the minimum set of security functionality needed for devices, systems and applications



Implementation:

- Responsibility of implementing the device's security capability is the responsibility of the acquiring organization
- Device manufacturers must ensure that their products can meet CSF requirements (where applicable)

External References/:

- HIPAA - Federal Register 45 CFR Part 164 Sections 308, 310, 312, 314 and 316
- Health Insurance Reform: Security Standards
- ISO/IEC 27799:2008

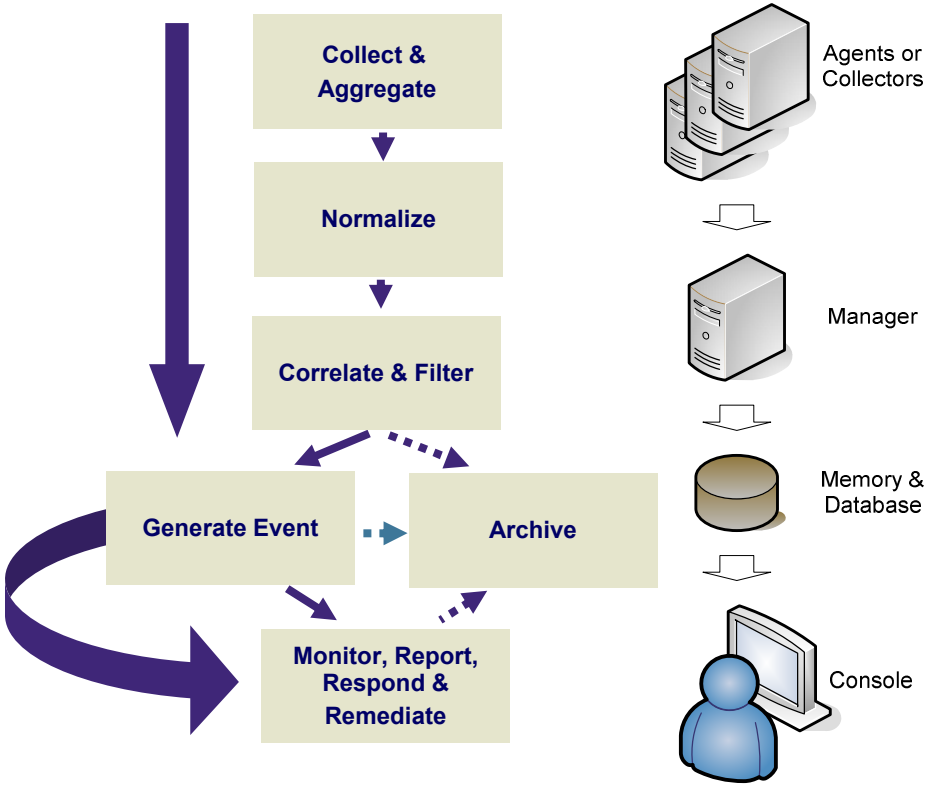
Security Incident & Event Management (SIEM) overview

Compelled by the daunting task of sorting through millions of security logs and events generated by network and system devices, many organizations have adopted Security Information & Event Management (SIEM) solutions. SIEM solutions automate the process of looking through logs. They normalize and store event data, correlate it, help produce reports, issue alerts, and assist in forensic analysis.

SIEM solution assists in

- Defining what a **Security Event** is…
  - Policy Violation → based on any enterprise-defined security policies (e.g., ISO, CoBiT, Internal policies)
  - Suspicious Activity → based on alarms & alerts by intrusion detection sensors as well as correlated data gathered from various systems (e.g., servers, routers, firewalls)
  - Vulnerability Identification → based ongoing vulnerability assessments

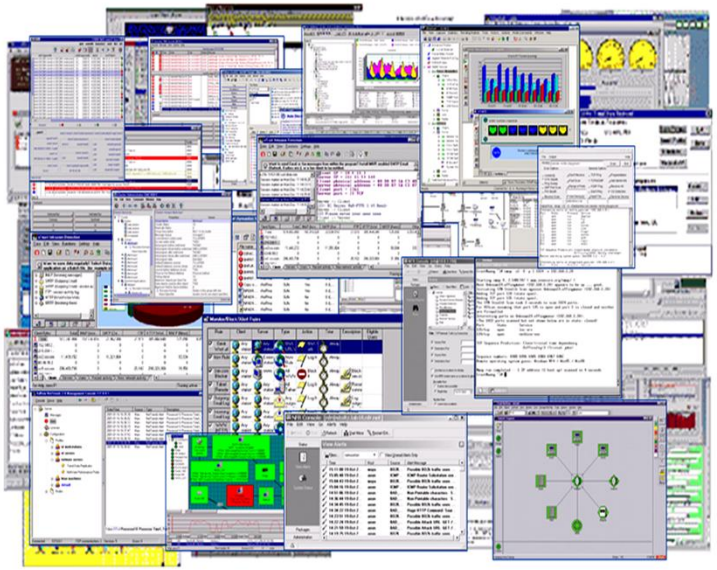
- **Management** of these events through…
  - Centralized / Aggregated Logging Mechanisms
  - Correlation Engines & Tools
  - Event Response & Remediation
  - Reporting & Metrics



SIEM business drivers

External and internal business drivers are demanding more transparency into system and application access activities. Effectively managing IT risk and compliance monitoring requirements by focusing on what matters most is the need of the hour.

Challenges



Too much technology creates too much disparate security information.

SIEM

Business Drivers

1) **Compliance and Reporting**

   Need for the ability to monitor and report access activities to key financial data and consumer personal information (e.g., PCI, HIPAA, SOX)

2) **Incident Investigation**

   Need for the ability to collect and analyze security and correlate them to identify the root cause of an incident

3) **Event Correlation**

   Need for the ability to collect and correlate event data, vulnerability data, and configuration data

4) **Security Effectiveness**

   Need for the ability to analyze the effectiveness of the security and privacy safeguards. This includes consolidation of disparate event / incident monitoring capabilities to improve operational efficiency

A successful SIEM solution can improve the efficiency and effectiveness of company's logging, monitoring, and reporting capabilities, and thus help address the overall enterprise IT compliance & risk management objective.

More Information

For more information on Deloitte Security & Privacy Services visit:

http://www.deloitte.com/us/securityandprivacysolutions