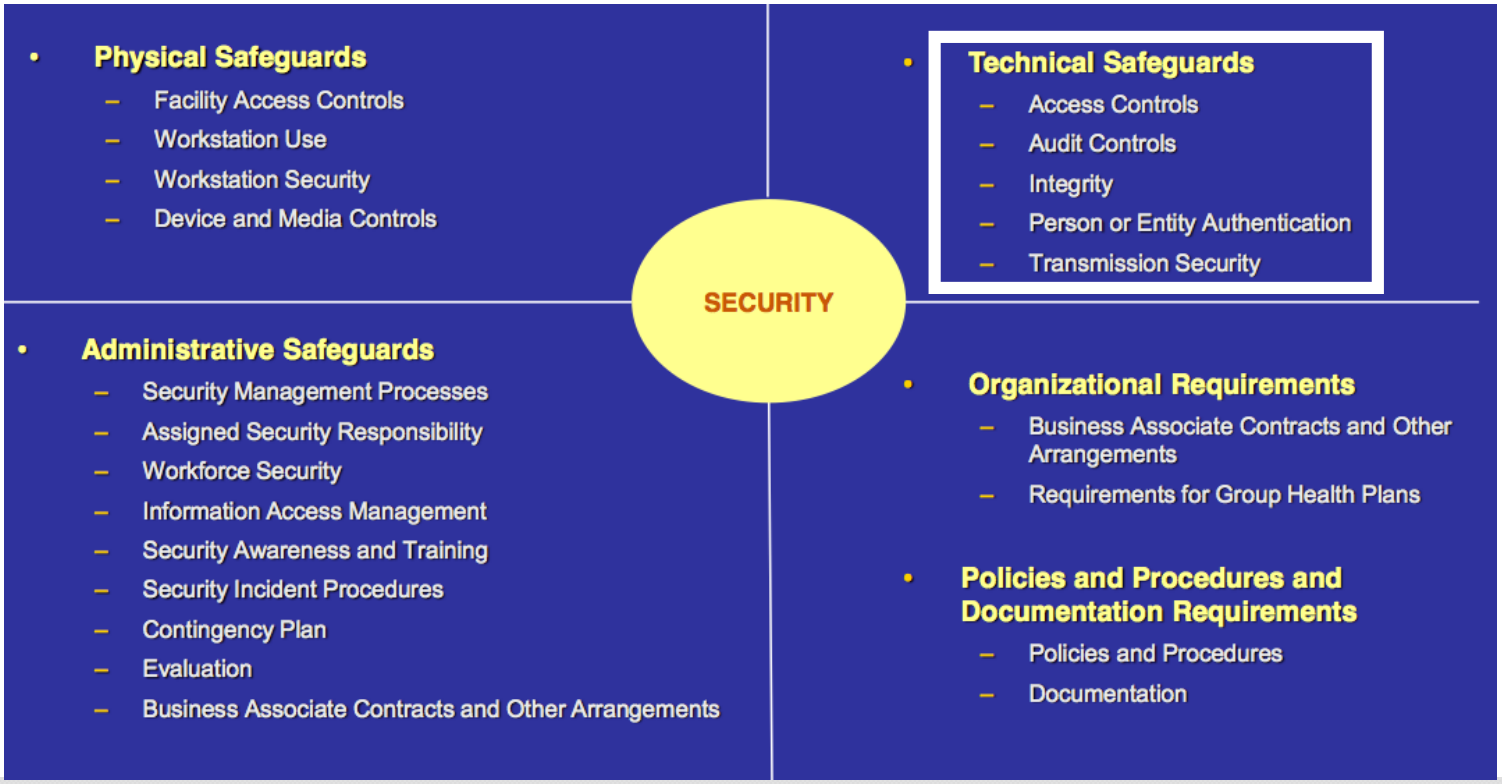
HIPAA/HITECH: Conditional Access Management for Business Performance

Mark Seward, Director Security and Compliance Solutions Marketing

Agenda

- HIPAA – compliance problems (a review for most)
- EHR access issues / access qualifiers
- Current solution issues
- Access use cases
- Looking beyond HIPAA – or, while we're collecting data…
- Fraud
- Measuring performance
- Improving outcomes

HIPAA at a Glance According to PWC



HIPAA / ARRA (HITECT) Changes

- With the passing of ARRA (HITECH provisions), HIPAA divided into two distinct compliance areas – data privacy and security
- Recent changes to HIPAA have moved responsibilities for governance of data privacy issues to the Office of Civil Rights (OCR) with security governance aspects remaining with Centers for Medicare & Medicaid Services (CMS)
- Agencies incentivized to perform audits – get to keep the fines collected in their own account

HITECH/HIPAA Compliance Timeline

Effective Date	Compliance Provision
On or Before September 15, 2009	New security breach notification obligations effective
February 17, 2010	• Business associates are directly subject to HIPAA • Limited Data Set standard for "minimum necessary," except as necessary to the purpose of the disclosure • Marketing communications further restricted • Business associate agreements required for "courier" entities • Employees of covered entities may have independent criminal liability
On or After January 1, 2011	Accounting for treatment, payment, or healthcare operation (TPO) disclosures from EHR systems acquired *after* January 1, 2009; HHS may extend deadline by two years
On or Before February 17, 2011	• New prohibitions on disclosure of PHI in exchange for remuneration • Mandatory civil monetary penalties for violations involving "willful neglect"
On or before February 17, 2012	Complainants will share in collected civil monetary penalties
On or After January 1, 2014	Accounting required for TPO disclosures from EHR systems acquired *before* January 1, 2009; HHS may extend deadline by two years

National Data Breach Laws for Healthcare

- Breaches of PII defined:
  - A data breach involving unsecured protected health information of more than 500 people must be reported promptly to the HHS, major media outlets and each individual affected by the breach.
  - Breaches affecting fewer than 500 people must be reported annually to the HHS secretary and the individuals.
  - On-line form to be filled out for Office of Civil Rights (OCR) in Health and Human Services (HHS) – fill out the form send in the money

The Carrot

The HITECH Act provides approximately $31.2 billion for healthcare infrastructure and adoption of electronic health records (EHR).

The Congressional Budget Office assumes that the Act will save federal healthcare programs an estimated $12 billion from higher EHR use, resulting in a net cost to the federal government of $19.2 billion.

The Stick -- Data Breach Penalties

Civil Money Penalties. OCR may impose a penalty on a covered entity for a failure to comply with a requirement of the Privacy Rule. Penalties will vary significantly depending on factors such as the date of the violation, whether the covered entity knew or should have known of the failure to comply, or whether the covered entity's failure to comply was due to willful neglect. Penalties may not exceed a calendar year cap for multiple violations of the

	For violations occurring prior to 2/18/2009	For violations occurring on or after 2/18/2009
Penalty Amount	Up to $100 per violation	$100 to $50,000 or more per violation
Calendar Year Cap	$25,000	$1,500,000

The Stick – Interesting Note

Any civil monetary penalty or monetary settlement collected with respect to an offense punishable under this subtitle or [the civil monetary penalty provision of HIPAA] insofar as such section relates to privacy or security shall be transferred to the Office of Civil Rights for [HHS] to be used for purposes of enforcing the provisions of this subtitle and [the HIPAA privacy rules]

Agency is incentivized to audit and find problems as the agency is self funded through enforcement actions.

The compliance problem -- HIPAA

- The business vision of providing healthcare (saving lives – providing services) means having open access to systems and data
  - Current access systems are 1 or 0 – don't support the healthcare business vision
  - …And care delayed is care denied
- High Risk Scenarios
  - Employee as patient (user and patient same name) – access control
  - Family member viewing – access control/management
  - Neighbor viewing – access control/management
  - VIP snooping (everyone is a VIP) – access control/management
  - Medical identity theft (FTC Red Flag) -- – general security, encryption and access control

HIPAA -- Patient Record Access: The ideal

- Monitor and report on EHR access based on three factors:
  - Temporal – The time element of access
    - Is the person viewing the record supposed to be on shift
  - Situational – Positive caregiver / patient assignment
    - Affirmative assignment of the caregiver / patient relationship
  - Appropriate – Caregiver / patient relationship
    - Can a relationship be established between caregiver – the 'old 6 degrees of separation'
- Monitor and report where EHRs go
  - Fax / Email / USB / other peripherals
  - Integrations with HIEs, 3rd-parties (contracted MRI, pharma retailers, other)

The compliance problem – HIPAA – Technical Solutions

- In general – access management systems provide strict access (1 or 0) to data
- FairWarning (access SIEM) – accepts access data from traditional Healthcare application vendors to monitor and audit access
  - Will create alerts and reports
  - Has SIEM partners that can receive its alerts
  - Will watch for first-name last-name similarities
  - Doesn't accept deep contextual information
  - Custom applications not be supported with out-of-the-box content
  - Doesn't help with the 'business associate' access record auditing
- Solutions not ready for comprehensive data access report supplied to patient at check-out
- No other non-vendor specific correlation solution for Healthcare HIPAA issues

What combination of data for what type of access

Temporal

- Is the person viewing the records 'on-shift'
  - Logon / Log-off (network)
  - Logon / Log-off (application)
  - Electronic time management data
  - EHR access records

Situational

- Assignment of patient / caregiver relationship
  - Charting data
  - Patient assignment data
  - EHR access records

Appropriate

- Is there an inappropriate relationship between patient and caregiver?
  - Patient intake data
  - Caregiver HR records
  - Compare patient current record attributes with caregiver HR data (i.e. residence and employment history data)
  - EHR access records
- Flag potential HIPAA issues for review by in-house privacy officer(s)

The data collection problem

- What data do I collect (obvious)?
  - Logon / Log-off (network)
  - Logon / Log-off (application)
  - Database access records
  - EHRs
- What data do I collect (not so obvious)?
  - HR employee records
  - Electronic time management data
  - Charting data
  - Electronic physical access records
  - eFax records
  - Electronic acknowledgements from 3rd-parties (business associates)
- What data do I collect (really not so obvious)?
  - RFID
  - Pharmaceutical dispensary system records
  - Requirement repair records
  - Other – (use your imagination)
- Data formats
  - HL7
  - Syslog (TCP stream)
  - Database connectors
  - Files
  - Others

Healthcare's 'rear-view mirror' HIPAA metrics

- Are we getting better or worse – KPIs
  - Patient EMR breaches over time
  - Patient EMR breaches by patient
  - Patient EMR breaches by caregiver
  - Patient EMR breaches by application (where is this occurring)
  - Patient EMR breaches by type (temporal, situational, appropriateness)
- Results lead to access policy changes – re-education
- What's next – "continuous monitoring"

What else keeps the healthcare C-suite up at night?

- Things that have a negative (or positive effect) on:
  - Top line revenue
  - Expenses
  - Reputation / compliance / other

Collection of log data beyond HIPAA

While we are collecting log data - other use cases the data can be used for?

- Billing errors
  - "Pat Palmer, founder of Medical Billing Advocates of America, estimates that she finds multiple errors in 8 out of every 10 hospital bills she reviews."
- Healthcare fraud (internal)
  - accounts for an estimated 3% of all health care spending, or $68 billion – low end estimate
- Service improvements
  - Service process and action tracking

Revenue Capture / Billing Errors

"Pat Palmer, founder of Medical Billing Advocates of America, estimates that she finds multiple errors in 8 out of every 10 hospital bills she reviews."

•Billing errors - Detect and monitor HL7 stream and system configurations for errors that might result in :

- Repeat billing: twice for the same procedure, supplies or medications.
- Length of stay: admission and discharge charge for arrival but not for discharge day
- Correct type of room charge: shared room vs. private
- "Average" time needed to perform an operation vs. anesthesiologist's records
- Up coding (most common): doctor changes an order for medication and/or service from an expensive version to one that costs less, like generic medications. Billed at the higher rate
- Keystroke mistake: results in overcharges or undercharges
- Canceled service: medication / procedure prearranged and then canceled later

Revenue Capture / Billing Errors

- Monitor systems using HL7 for proper system configuration and for configuration changes
- Compare patient information on the charting application to list of available generic medications
- Compare typical/average bill amount for services to what was rendered to a patient – in or out of percentage tolerance
- Monitor and flag double charges – does a same day charge already exist in a system
- Monitor that cancelled services are removed from the billing systems
- Monitor equipment RFID for equipment left in the patient's room
- Monitor and flag arrival date, number of 'stay days' and discharge date across billing systems

Insider Fraud

- "According to the National Council of State Boards of Nursing, approximately 15% of healthcare professionals struggle with drug dependence at some point in their career."
- How Splunk can Help
  - Monitor and report access to automated pharma systems compare drug selection and quantity with HL7 charting data
  - Monitor and report access to automated pharma system compare to 'on-shift' information from Kronos
  - Monitor the process of supplies distributed from Dock-to-Doc. Changes in quantity supplies -- same person receives and accesses DB to mark spoilage

Hospital metrics – Monitoring & Improving Performance

- If there are a series of sequential steps to a treatment -- then – the amount of time a treatment takes can be measured and monitored as a transaction with the patient.
  - Monitor performance by shift
    - Medication to be administered at midnight
      - What time was the medication retrieved
      - What time was it administered
      - What time was it charted
  - Other ‘transactions’?

Revenue Capture / Billing Errors

- “Pat Palmer, founder of Medical Billing Advocates of America, estimates that she finds multiple errors in 8 out of every 10 hospital bills she reviews.”
- Billing errors - Detect and monitor HL7 stream and system configurations for errors that might result in :
  - Repeat billing: twice for the same procedure, supplies or medications.
  - Length of stay: admission and discharge charge for arrival but not for discharge day
  - Correct type of room charge: shared room vs. private
  - ”Average" time needed to perform an operation vs. anesthesiologist's records.
  - Up coding (most common): doctor changes an order for medication and/or service from an expensive version to one that costs less, like generic medications. Billed at the higher rate
  - Keystroke mistake: results in overcharges or undercharges
  - Canceled service: medication / procedure prearranged and then canceled later

Improving outcomes

- Project starting with Northern CA VA
  - Review recorded ICU data – look for patterns of factors in/out of tolerances in situations where a bad outcome occurred for the patient
    - Respiration
    - Blood Pressure
    - Heart rate
    - EKG
  - Compare to patient information (weight, age, ethnicity, other factors)
  - Determine predictive analytics for bad outcomes more tailored to the patient

What should we really audit for?

- Risk to top line revenue
  - Reputation
  - Compliance
  - Fraud
- Operational (pun intended) risk
  - Personnel Performance
  - Medical Errors
  - Business associate risk

What is HL7?

- Health Level Seven (HL7), is an all-volunteer, not-for-profit organization involved in development of international healthcare standards.
- “HL7” is also used to refer to some of the specific standards created by the organization.
- HL7 and its members provide a framework (and related standards) for the exchange, integration, sharing and retrieval of electronic health information.
- Although v3.x using XML is currently available, v2.x of the standards, which support clinical practice and the management, delivery, and evaluation of health services, are the most commonly used in the world.

Example Use Cases

- Prescription inventory →validation
- Medical locker/cabinet → prescription → patient/doctor
- For any patient visit, show me a chronological ordering of HL7 message for that visit
- For a medical record number, find all of the associated visits/orders/prescriptions
- For placer order number (unique ID for order placed by hospital) find all discontinued message (D/Cs)
- For any patient, show me their doctors/prescriptions/allergies?
- Are there any messages where the zip code was not provided?
- Which apps are sending in bad/incomplete/invalid messages?

DEMO


splunk>