



HCCA's 12TH ANNUAL COMPLIANCE INSTITUTE

APRIL 13–16, 2008 | NEW ORLEANS, LA | HILTON RIVERSIDE NEW ORLEANS

“Privacy & Security Hot Topics: HIPAA and Beyond”

*Randy Gainer, Partner, Davis Wright Tremaine, Seattle
Deann Baker, Compliance and Privacy Officer, Alaska
Native Tribal Health Consortium*



www.hcca-info.org | 888-580-8373



Proposed Agenda

- 1:00 – 1:10 Introductions
- 1:10 – 1:45 Healthcare regulations & general state laws
- 1:45 – 2:00 Break
- 2:00 – 2:40 Federal & State Activity Updates and the Payment Card Industry Data Security Standard
- 2:40 - 3:15 Enforcement Activity
- 3:15 – 4:00 Data Breach Notification Standards and Assessment of Best Practice – Case Study



Request that you:

- participate in the discussion
- be informal and flexible
- place cell phones and pagers on vibrate
- if you need to leave, please do so quietly

Sum - Privacy vs. Security Accountability

<u>Privacy Requirements</u>	<u>Security Requirements</u>
<ol style="list-style-type: none">1. Designate Privacy Official2. Criteria established for need to know & minimum necessary of <u>all forms/uses of PHI</u>3. P&P to protect uses and disclosures of all forms of PHI4. Accountability to patient for use and disclosure of PHI5. Documentation retained for 6 yrs from date of creation or last date in effect6. Training & education7. Sanctions8. BAA	<ol style="list-style-type: none">1. Identify Security Official2. Need to know & minimum controls for <u>access and uses of EPHI</u>3. P&P to ensure confidentiality, integrity & availability of EPHI4. Accountability of authorized users/access controls5. Documentation retained for 6 yrs from date of creation or last date in effect6. Training & education7. Sanctions8. BAA

HIPAA Privacy Rule

45 C.F.R. § 164.530(c) requires covered entities

- to have ensure appropriate administrative, technical, and physical safeguards to protect the privacy of PHI; and
- to reasonably safeguard PHI from intentional or unintentional disclosure in violation of HIPAA. This includes:
 - Use or disclosure of all forms of PHI (including EPHI & oral)
 - Understand incidental disclosures and how to limit those

Incidental Use and Disclosure

- Limited in nature
- Secondary use or disclosure
- Can't be reasonably prevented
- By-product of otherwise permissible use or disclosure
- Examples:
 - sign in sheets
 - white boards
 - calling out the name of the person
 - joint treatment areas
- Must address these incidental disclosures with procedures and education

Incidental Use and Disclosure

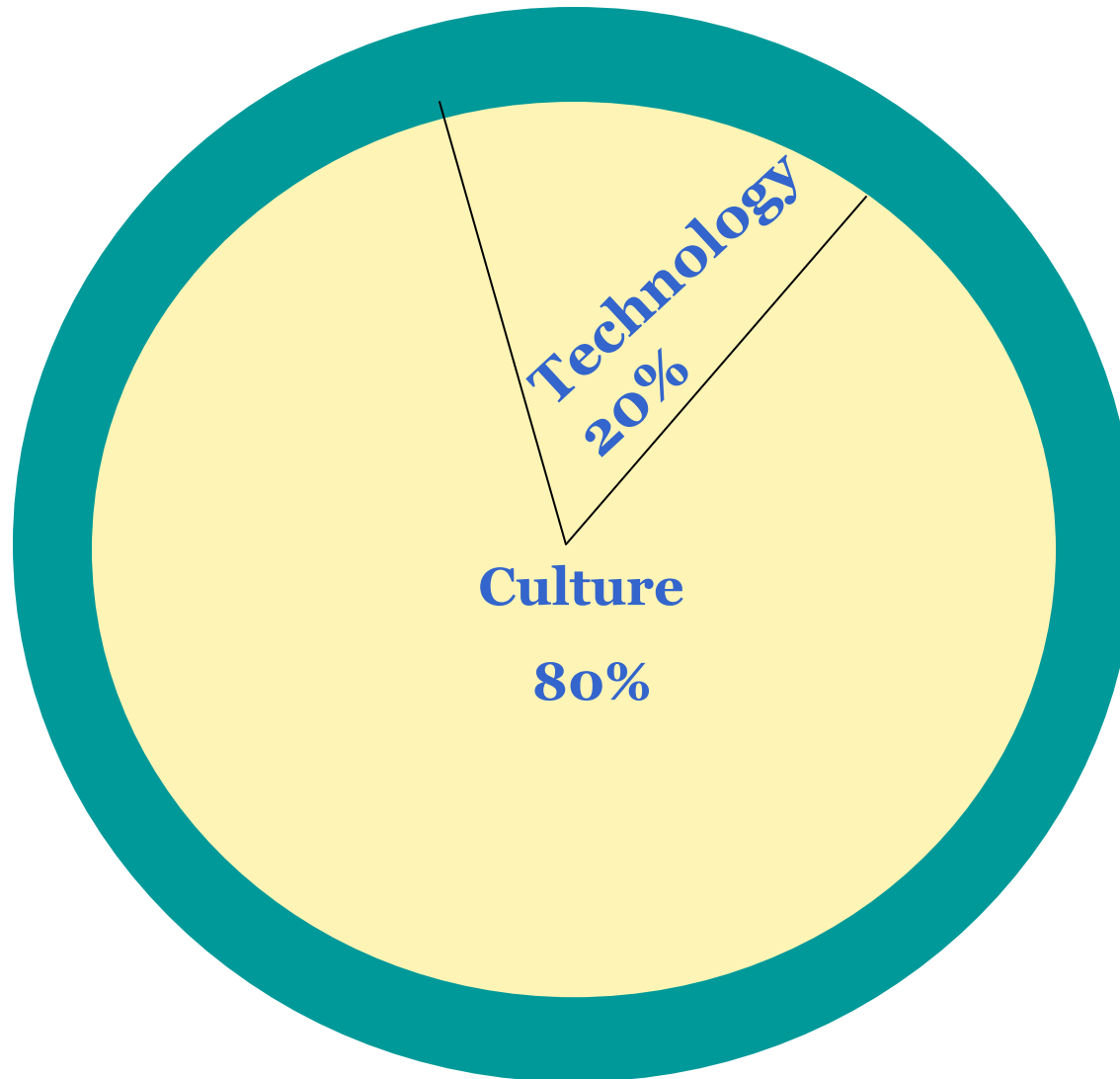
- Is permissible only to the extent that the CE has applied reasonable safeguards 45 CFR 164.530c
- An incidental disclosure that occurs due to a failure to apply reasonable safeguards or the minimum necessary standard could therefore violate the Privacy Rule
- WEDI White paper on oral disclosures:

http://www.details-worktools.com/media/scms/Oral_Communications_Myths_Facts.pdf



www.hcca-info.org | 888-580-8373

Privacy and Security – The Culture



HIPAA Security Rule

- 45 C.F.R. § 164.306 requires covered entities, among other things:
 - to protect against reasonably anticipated threats to the security of ePHI;
 - to protect against reasonably anticipated mis-uses or disclosures of ePHI;
 - to assure that their workforces comply with the Security Rule;
 - To obtain assurances of confidentiality and security from their contractors.

Ensure and Reasonableness

“Ensure”

- interpretation indicates an impossible task because we can't ensure privacy and security, we can only ensure the effort.

“Reasonableness”

- indicates a practical business approach as we have a responsibility to secure patient records and the responsibility is no different for any other industry

HIPAA Security Rule (cont'd)

- 45 C.F.R. §§ 164.308(a)(1)(ii)(A) & (B) require covered entities to engage in risk analysis and risk management to reduce risks to the security of ePHI to a reasonable level.
- 45 C.F.R. §§ 164.310(a)(2)(ii) & (d)(1) require covered entities to implement policies and procedures to safeguard their physical facilities, hardware, software, and electronic media to protect against theft. (Though 164.312(a)(2)(ii) is “addressable,” it will apply to hospitals.)

December 2006 HHS HIPAA Security “Guidance”

The “Guidance” is available at:

<http://www.cms.hhs.gov/SecurityStandard/Downloads/SecurityGuidanceforRemoteUseFinal.pdf>

- The “Guidance” states that CMS (which enforces the Security Rule) “may rely upon this guidance document in determining whether or not the actions of a covered entity are reasonable and appropriate . . . and it may be given deference in any administrative hearing pursuant to the HIPAA enforcement rule.”

HHS “Guidance” (cont’d)

- The “Security Guidance” states that covered entities should give “significant emphasis and attention” to:
 - Risk analysis and risk management strategies
 - Policies and procedures for safeguarding ePHI
 - Security awareness and training on the policies and procedures for safeguarding ePHI.

Medicare Conditions of Participation

- A Medicare rule, 42 C.F.R. § 482.24, requires hospitals to assure that:
 - Patient records are confidential;
 - Unauthorized persons cannot gain access to or alter patient records; and
 - Patient records are released only to authorized persons in accordance with law.

Consumer Protection Act

- Hospital privacy policies may assure patients that their information will be kept confidential.
- In other contexts, the FTC has brought unfair trade practice claims against companies that failed to implement adequate security after claiming they would protect consumers' data. E.g., Life Is Good, Inc., Consent Order, FTC File No. 072 3046 (January 2008).
- Plaintiffs in *Gibson v. Providence* claimed that the hospital violated the Oregon Unlawful Trade Practices Act by representing in its privacy policy that it would protect patient data and allegedly failing to do so.
- A similar claim could be brought under other consumer protection statutes. Potential remedies include actual damages, discretionary treble damages, attorneys' fees, and costs.

Negligence claims

- Plaintiffs in many data breach cases have claimed that companies that store consumer information have a duty to use reasonable care to protect the information.
- Litigants claim that the various statutes that address information security establish the elements of that duty.

State Data Breach Notice laws

- As of January 11, 2008, 40 states, Washington, D.C., and Puerto Rico have data breach notification laws.
 - Only Alabama, Alaska, Iowa, Kentucky, Mississippi, Missouri, South Carolina, South Dakota, Virginia, and West Virginia have not yet enacted data breach laws.
- As of the same date, 36 states and Washington, D.C. have adopted credit freeze laws.
- Effective January 1, 2008, California amended its data breach notice law to require notice if medical information and insurance account numbers are disclosed to unauthorized persons.

Other Pertinent State Laws

- A 2008 Nevada law requires encryption of personal information data when it is transmitted electronically.
- New Jersey has proposed a rule that would require all electronic personal to be encrypted.
- Several state laws requires businesses that collect or license personal information, or health care providers specifically, to implement reasonable safeguards to secure health care information.
 - Arkansas, California, Maryland, North Carolina, Rhode Island, Texas, Utah, and Washington have such laws
 - E.g., the Washington law, RCW 70.02.170, provides that patients may recover actual damages (though not consequential or incidental damages), attorneys' fees, and costs for failure to secure health care information.

Payment Card Industry Data Security Standard

- The Payment Card Industry (PCI) Data Security Standard applies to all “merchants” that store, process, or transmit cardholder data.
- If your organization accepts card payments, the Merchant Agreement with the bank that processes the payments likely requires you to comply with the PCI Standard.
- The Standard has been accepted by Visa, MasterCard, American Express, Discover, Diners Club, and JCB International.
- The PCI Standard requires organizations that process card payments to do 12 things:

PCI Standard (cont'd)

- Build and Maintain a Secure Network
 1. Install and maintain a firewall configuration to protect data
 2. Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Cardholder Data
 3. Protect Stored Data
 4. Encrypt transmission of cardholder data and sensitive information across public networks
- Maintain a Vulnerability Management Program
 5. Use and regularly update anti-virus software
 6. Develop and maintain secure systems and applications
- Implement Strong Access Control Measures
 7. Restrict access to data by business need-to-know
 8. Assign a unique ID to each person with computer access
 9. Restrict physical access to cardholder data

PCI Standard (cont'd)

- Regularly Monitor and Test Networks
 10. Track and monitor all access to network resources and cardholder data
 11. Regularly test security systems and processes
- Maintain an Information Security Policy
 12. Maintain a policy that addresses information security
- Visa and MasterCard require different level of proof of compliance with the Standard depending on the number of card transactions processed.
 - Level 1: 600,000 Visa transactions or over 6 million MasterCard transactions a year.
 - Level 2: 150,000 to 600,000 Visa transactions per year or 150,000 to 6 million MasterCard transactions per year
 - Level 3: between 20,000 and 150,000 Visa or MasterCard transactions per year
 - Level 4: all others

PCI Standard (cont'd)

- **Level 1:** must perform annual on-site security audit and quarterly network scans. The annual on-site security audit may be performed by a third party security assessor or by the entity's internal audit team if a corporate officer signs off. The quarterly network scan must be performed by an authorized third-party network security vendor.
- **Levels 2 & 3:** must complete an annual self-assessment and quarterly network scans. The quarterly network scan must be performed by an authorized third-party network security vendor.
- **Level 4:** Visa and MasterCard require, that Level 4 entities quarterly network scans performed by an authorized third-party network security vendor. Some banks also require Level 4 entities to conduct annual self-assessments.

Proposed Federal Data Breach Legislation

- Legislation was proposed in both houses in 2007
 - S. 239 (Feinstein), S. 495 (Leahy, Specter): would impose disclosure requirements, both bills approved in committee, both would preempt state data breach notice laws, neither bill made it to the Senate floor;
 - H.R. 836 (Lamar Smith): would not preempt state law, no action since referred to committee in March 2007;
 - H.R. 958 (Rush, Sterns): would preempt state data breach laws, stalled in committee; no action for almost one year;
 - H.R. 2124 (Davis) and S. 1558 (Coleman): identical bills requiring OMB to establish data breach policies for federal agencies, in committees in both houses;
 - S. 1202 (Sessions): introduced in April 2007; stalled in committee;
 - H.R. 1685 (Price), introduced in March 2007, and S. 1260 (Carper), introduced in May 2007, would preempt state laws, stuck in committee in both houses;
 - H.R. 4791 (Clay): introduced late 2007, requires OMB to establish data breach policies for federal agencies; in committee.

Proposed Federal Data Breach Legislation

Areas of contention:

- When a security breach would trigger notification requirements
 - S. 239: exempts businesses from having to notify if "a risk assessment concludes that there is no significant risk that the security breach has resulted in, or will result in, harm to the individuals whose sensitive personally identifiable information was subject to the security breach."
 - Less demanding than many state notice laws.
 - S. 495: must notify any U.S. resident whose "information has been, or is reasonably believed to have been accessed or acquired."
 - Identical to the majority of state laws.
- Whether federal law should preempt state laws.

Quantifying the risk that data will be wrongly disclosed

According to the Identity Theft Resource Center:

- 10 reported data breaches exposed 274,950 records from January 1-11, 2008.
- 443 reported data breaches exposed 127 million records in 2007.
- 315 reported data breaches exposed 20 million records in 2006.
- 158 data breaches exposed 65 million records in 2005.

The increase in the number of reported data breaches is likely due in part to the state laws that require notices of data breaches.

How protected information is compromised.

- Internal Risks:
 - General employees
 - Janitors copied information from paper charts left at a hospital's workstations; clerks at another hospital copied data
 - Employees working from home
 - IT employees
 - An IT director emailed a large number of patient records to his home computer.
 - Contractors
 - A hospital hired a transcriptionist to transcribe tapes. An Indian subcontractor's employee posted confidential transcribed medical information on the Internet.
 - Computer networks
 - Secure or insecure
 - Loss of data
 - Integrity of data

How protected information is compromised (cont'd).

- External risks:
 - Walk-in thieves
 - A laptop used for patient registration in an E.R. was stolen; a desktop computer with ePHI at a clinic was stolen after hours.
 - Thieves who steal laptops from employees' cars
 - Numerous laptops with confidential information have been reported stolen.
- Electronic penetration
 - In mid-2005, attackers accessed TJX computers and stole 94 million customer records over several months.
 - In May 2005, attackers accessed CardSystems Solutions' networks. They found a treasure trove of unencrypted credit card data.
 - In March 2004, a credit card database was stolen from BJ's Wholesale Club. Three million customers' card data were exposed. Hospital systems may be penetrated as well
- Medical Identity Theft
 - Billing issues
 - Health care risks to patients

Recent Breaches

- Jan. 4, 2008, Health Net (Mountain View, CA/CT):
 - 5,000 employees notified that their names and SSNs were on a laptop computer that was stolen from a company vendor.
- Dec. 17, 2007, West Penn Allegheny Health System:
 - The names, SSNs, phone numbers, addresses and patient care information of 42,000 home care and hospice patients were all on a laptop computer stolen from a nurse's home.
- Dec. 5, 2007, Memorial Blood Centers (Duluth, MN):
 - A laptop was stolen holding 268,000 donor names in combination with the donor's SSNs.
- Nov. 30, 2007, Prescription Advantage (MA):
 - Local authorities arrested a identity thief who had been using information taken from the program. Although the thief used information from only a small number of victims, state data breach laws required that 150,000 plan participants who could possibly be affected by the breach to be contacted.

See <http://www.privacyrights.org/ar/ChronDataBreaches.htm>



Breaches from the Internal Risk Area

Cox Communications sabotaged

- January 2008 Employee Gets Prison Time for causing Outage
- Employee sentenced to 5 years in prison, 200 hours community service and \$15,000 in restitution.
 - Five months in prison and five months of home confinement
 - serve two years of supervised release,
 - perform 200 hours of community service, and
 - pay more than US \$15,000 in restitution.
 - Cox provides computer and telecommunications services across the US.

Breaches from the Internal Risk Area continued

Employee was asked to resign from Cox

- employee remotely shut down parts of the company's network
 - Sabotage resulted in:
 - loss of services to customers in Texas, Las Vegas, New Orleans, and Baton Rouge.
 - In some cases, 911 emergency services were affected as well. \ The services were back up within hours of the attack.
- What could Cox have done differently?

Breaches from the Internal Risk Area

Stolen Lap Tops and Social Security Numbers

- Two laptop computers containing 337,000 Nashville voters Social Security numbers were stolen
 - Security guard failed to make his hourly rounds
 - another security guard discovered the break-in two days later
 - digital video recorder had been unplugged, erasing any chance of capturing images of the thief or thieves
 - council members continued to express outrage and frustration over the theft,
 - Theft may have exposed most of the countys voters to identity fraud

Breaches from the Internal Risk Area continued

Stolen Lap Tops & Social Security Numbers

- Steps to prevent another burglary include:
 1. requiring security guards to check windows regularly
 2. taking voters' Social Security numbers off all laptops and
 3. putting alarms on all digital video recorders
 4. security guards are now at the building around the clock
 5. Security guard terminated
 - no written procedure for securing laptops after business hours but will develop one
 - Sandy Cole, director of Metro Information Technology Services, said voters Social Security numbers shouldn't have been on the laptops. Cole said her department recommends sensitive data should not be stored on a mobile device.
 - Lap tops were not encrypted
 - <http://www.tennessean.com/apps/pbcs.dll/article?AID=200880103134>

Breaches from the External Risk Area

Laptop theft

- Research indicates that laptop theft is one of the three leading causes of data security breaches that require notification under California's and other states' notification laws. The research illustrates the risks associated with storing confidential information on unprotected laptops.

Enforcement Activities

PricewaterhouseCoopers hired for HIPAA reviews

- The CMS has hired consulting firm PricewaterhouseCoopers to perform a series of compliance reviews of hospitals regarding adherence to the security rule under the administrative-simplification section of the Health Insurance Portability and Accountability Act of 1996.
- April 20, 2005. Since then, the CMS has received more than 200 complaints about possible violations
- Pricewaterhouse could be assigned between 10 and 20 organizations against which security complaints have been lodged
- HHS' inspector general's office is looking into how the CMS handles its enforcement duties regarding the HIPAA security rule.

Enforcement Activities

- OIG Audits and Annual Work Plan
- CMS enforcement of the Security Rule
- OCR enforcement of the Privacy Rule

Methods to Avoid Security & Privacy Breaches

- Regence group of the Blue Cross and Blue Shield plans
 - Notify beneficiaries of the potential impact of lost ID cards.
- New York hospital
 - Issuing smart cards for users that include a PIN.
- Some facilities
 - Will only provide services if the patient produces a photo ID.
- Providence Health & Services
 - Hired a Chief Information Security Officer, who is revising information security policies, procedures, and training throughout PH&S's five-state organization.
- What are you doing?

Actions to prevent theft or loss of PHI

Hire a third party to conduct risk assessments:

- Contractors experienced with hospital security issues can spot vulnerabilities that employees fail to notice.
- Electronic security specialists should inspect and test systems, policies, and procedures used to protect ePHI.

Put together a multi-faceted Information Security committee together for ongoing assessment.

Security Committee

HIT Executive committee

- Also serve as Information Security Governance Body
- Made up of leadership from all divisions
- Role is to:
 - work on setting direction
 - Establish priorities
 - Align goals and priorities
 - Assess strategies for implementation and monitoring of systems
 - Assist with drafting policies and procedures
 - Provide education on policies and procedures
 - Evaluate security systems and report concerns (formal documented process)
 - Security incidents should be reported to

Actions to prevent theft or loss of PHI (cont'd)

Storing data and encryption:

- ePHI and other confidential data stored on laptops should be encrypted
- Many laptops are stolen and lost and therefore it is unreasonable to store unencrypted data on laptops
- User-friendly laptop encryption programs are available
- Alternatively, data needed offsite can be accessed via a VPN

Actions to prevent theft or loss of PHI (cont'd)

Employees and contractors:

- Should be carefully screened
 - Information that may be used for identity theft is valuable and easily converted to cash
 - Only those who can be trusted with access to such valuable information should be permitted access to it.
- Policies and procedures:
 - Should address exit strategies as well as “entrance” strategies
 - Entrance documents should include, but not be limited to, non-disclosure/confidentiality agreement

What could it cost your organization?

Recent reports of theft

- Providence Health & Services breach (2005)
 - 365,000 patients
 - \$6.9 million
- Emory breach
 - 38000 patients x \$10 per patient = \$380,000
 - 38000 patients x \$30 per patient = \$1,140,000
- Office of Veterans Affairs
 - Spent millions to hire a consultant to encrypt systems
- Potential state tort liability

Reputation and Financial Implications

The business perspective – Cost & effects of notification

- Notification statutes hold liable the very entities that thieves took advantage of
- Business is held accountable for a crime committed by against them
- Proactive expenses:
 - Cost for encryption mechanisms and Intrusion detection devices
 - Firewalls and other defense technology
- Reactive expenses:
 - Mailing notifications
 - Credit monitoring
 - Identify theft – medical or financial
- Larger Price to Pay with out adequate safeguards – loss of business
 - Many of those customers who receive notices blame organizations for not having sufficient controls and safeguards
 - Customer likely lose confidence in the organization
- What is the prices they pay if they don't notify?

Decision Making

Notification requirements

- HIPAA:
 - Accounting of disclosure
- Graham Leach Bliley
- State Laws
 - Data base notification
 - California data base - Numbers
- If not required to report – should you?

Best Practice Decision Making & Response

Six steps to respond to data breaches:

1. Notify senior management, board members, counsel and plan
2. Investigate
 - what information was obtained, lost, disclosed, or changed
 - determine how
3. Determine who else should notified – individuals, law enforcement, regulators, others?
4. Determine how to send the notifications
5. Respond to inquiries, litigation (determine who the contact will be)
6. Correct security flaws, remediate damages and document all mitigated efforts through a written corrective action plan

Actions to respond to data breaches (cont'd)

Step 1

Notify internal senior management, counsel, and develop:

- a communication plan to contact other internal officials
- written communications to and from counsel should be marked “attorney-client privileged.”
- a plan to identify, prioritize, assign and manage tasks
 - who will direct and manage the investigation as defined below
 - who, if necessary will contact law enforcement (if there was a theft),
 - who, if necessary, will coordinate media strategy, and
 - who will supervise the notification and inquiry process

Actions to respond to data breaches (cont'd)

Step 2

Investigate:

- Coordinate investigative steps consistent with initial plan:
 - What information was accessed or stolen?
 - Were “computerized data” and “personal information” obtained by an unauthorized person – internal/external?
 - If computer forensics, network security, or private investigators are needed, they should be hired by counsel to permit him or her to advise you. The consultants’ reports should be privileged.

Actions to respond to data breaches (cont'd)

Step 3

Determine whom to notify outside the organization:

- Notify law enforcement of any theft.
 - Discuss with law enforcement whether to delay notifying others.
- Create lists of any potentially affected individuals, with notice addresses.
- Notify CMS, JAHCO, State AG?
- Notify employees, media?

Actions to respond to data breaches (cont'd)

Step 4

Determine how to send notifications:

- If individuals are to be notified:
 - decide whether to outsource notice
 - decide whether to offer credit monitoring and other services (one year of credit monitoring is standard)
 - draft notice letters with potential litigation in mind
 - train operators for a call-in center; draft scripts and
 - post important info. and FAQs on your website
- Notices to regulators should concisely explain what occurred and what remediation steps have been and are being taken.

Actions to respond to data breaches (cont'd)

Step 5

Respond to inquiries and litigation:

- Respond to inquiries from individuals, employees, and the media honestly but with an understanding that everything you state may be used in court.
- Be prepared to defend against a class action, especially if any information is misused. Emotional distress alone should be insufficient for plaintiffs to avoid dismissal.

Actions to respond to data breaches (cont'd)

Step 6

Correct security flaws and remediate damages:

- Immediately correct all vulnerabilities, example:
 - institute secure transport and storage of backup tapes;
 - encrypt ePHI and personal information on laptops;
 - revise procedures to account for copies of patient data; and
 - assure that video surveillance of areas where data are stored is functioning properly.
- If your computer network was penetrated, prepare for additional attacks when the breach is disclosed.
- If individuals can show they suffered fraud related to the breach, compensate them.
 - Your claims specialist should review fraud claims.
 - Experts estimate that 1-4% of the population have experienced “identity theft.”
 - You should compensate only fraud that was probably caused by the breach at your hospital, not by another event.

CASE STUDY DISCUSSION

We want to hear from you!



www.hcca-info.org | 888-580-8373

Resources

Risk Analysis guidance

- <http://www.cms.hhs.gov/EducationMaterials/Downloads/BasicsofRiskAnalysisandRiskManagement.pdf>

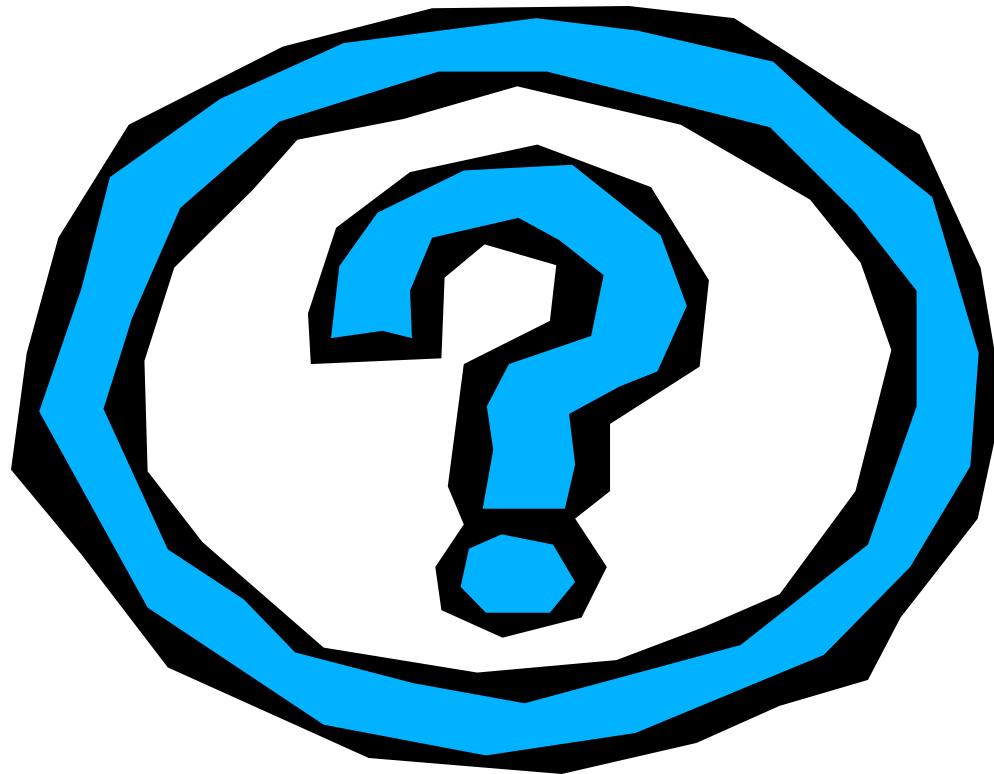
Administrative Safeguards

- <http://www.cms.hhs.gov/EducationMaterials/Downloads/SecurityStandardsAdministrativeSafeguards.pdf>

Document establishes the policy for the IS program at the CMS:

- <http://www.cms.hhs.gov/InformationSecurity/Downloads/PISP.pdf>
- Purpose of document:
 - This The formation of the CMS IS Program Policy is driven by many factors, the key one being **Risk**. This policy sets the ground rules under which CMS shall operate and safeguard its information and information systems to reduce the risk, and minimize the effect of security incidents.
 - This policy (CMS-CIO-POL-SEC02-02 November 15, 2007) supersedes the previous version that was signed by the CMS Chief Information Officer (CIO) on May 3, 2005.

QUESTIONS



Contact information

Randy Gainer

Phone: (206) 757-8047

Email: randygainer@dwt.com

Deann Baker

Phone: (907) 729-1992

Email: dmbaker@anthc.org

