

# 2009 HIPAA Security Rule Conference

*Framing the Two Days*

*Julie Boughn*

*CMS Chief Information Officer*

# Questions to Run On

- How do we collectively “raise our bar” for Security?
- How do we move past compliance to value-driven security?
- What are the key information security issues that we need to resolve to make progress on Interoperable Health IT?

# How to “BE” for the Two Days

- Curious – don’t let the way we’ve always done things be a barrier
- Humble – we can improve on what we’re already doing
- Think beyond compliance

# Opening Activity

- Turn to someone sitting near you who you don't know well.
  - Introduce yourself
  - Answer these questions:
    - Why did I come to this conference?
    - In order for to leave the conference thinking it was wildly successful, I will \_\_\_\_\_.

# Who wants our Data Anyway?

The screenshot shows a Windows Internet Explorer browser window with the address bar displaying [http://www.theregister.co.uk/2009/05/05/virginia\\_medical\\_records\\_extortion/](http://www.theregister.co.uk/2009/05/05/virginia_medical_records_extortion/). The page title is "Hackers demand \$10m ransom for Virginia medical data". The browser's taskbar at the bottom shows several open applications: Start, Inbox - Microsoft O..., Calendar - Microsof..., NISTOutline\_20090..., Hackers demand \$..., and NIST\_CMS\_2009HIP... The system tray on the right shows the time as 5:56 PM.

**The Register**  
Biting the hand that feeds IT

Hardware Software Music & Media Networks Security Public Sector Business Science Odds & Sods Search site

Crime Enterprise Security Anti-Virus Spam ID Spyware Infosec Newsletters Feeds

**Prevent Identity Theft**  
Always a step ahead of ID Thieves. Get Daily Surveillance & Protection  
[Stop.IdentityTheft.com](http://Stop.IdentityTheft.com)

**Credit Card Fraud**  
Spot Signs Of Fraud Before It Is Too Late. Get A Free Credit Report!  
[www.CreditReportCompare.com](http://www.CreditReportCompare.com)

**Two-Factor Authentication**  
Easy two-factor authentication via your mobile phone. Fast free trial.  
[www.smspsscode.com](http://www.smspsscode.com)

Ads by Google

Print story Post comment Track this topic

## Hackers demand \$10m ransom for Virginia medical data

### 8.3 million records held hostage

By **Dan Goodin in San Francisco** • [Get more from this author](#)  
Posted in [Security](#), 5th May 2009 19:02 GMT  
[Free whitepaper - A healthy prescription for secure and compliant file transfer](#)

Almost 8.3 million patient records have been stolen from a Virginia government website that tracks prescription drug abuse, according to hackers who are demanding a \$10 million ransom for their return.

"I have your shit!" the note, which was posted to Wikileaks read. "In \*my\* possession, right now, are 8,257,378 patient records and a total of 35,548,087 prescriptions. Also, I made an encrypted backup and deleted the original. Unfortunately for Virginia, their backups seem to have gone missing, too."

The message said if officials didn't respond within seven days the information would be

**TOP STORIES MOST READ MOST COMMENTED**


- [Hackers demand \\$10m ransom for Virginia medical data](#)
- [eBay driving world's tomb raiders out of business, says prof](#)
- [Botnet hijacking reveals 70GB of stolen data](#)
- [Sri Lankan Army site 'assassinated' by rebels](#)
- [US Congress wants hack teams for self-penetration](#)

**Free whitepaper**

## Does disaster recovery make

# Who wants our Data?


Yesterday, 01:20 AM #1

  
Member

Join Date: 2008

Posts: 5

---

 **Looking to buy Heathcare/Insurance data**

I am looking for someone that is selling possible database dumps from Healthcare or Insurance providers. Also, completed HCFA 1500 forms will work.

[QUOTE](#) [QUOTE](#)  [QREPLY](#)

# Why Do Security?

- Confidentiality
- Integrity
  - Health Care is a multi-trillion dollar business, representing more than 16% of our economy
  - Lives are at stake!
- Availability
  - Lives are at Stake

# CMS Statistics

- More than 90 Million Covered Lives
- \$1.3 Billion – *PER DAY!*
- 1.2 Billion Medicare FFS claims annually
- 1.2 Billion Medicare Prescription Drug Events
- 2.5 Billion Medicaid Claims Data Events
- ***15 million eligibility inquiries per week***



# FISMA in a Nutshell

- The act requires program officials, and the head of each agency, to conduct annual reviews of information security programs, with the intent of keeping risks at or below specified acceptable levels in a cost-effective, timely, and efficient manner. The National Institute of Standards and Technology ( NIST ) outlines nine steps toward compliance with FISMA:
  1. Categorize the information to be protected
  2. Select minimum baseline controls
  3. Refine controls using a risk assessment procedure
  4. Document the controls in the system security plan
  5. Implement security controls in appropriate information systems
  6. Assess the effectiveness of the security controls once they have been implemented
  7. Determine agency-level risk to the mission or business case
  8. Authorize the information system for processing
  9. Monitor the security controls on a continuous basis

# Do Federal Agencies Care about FISMA?

http://republicans.oversight.house.gov/media/PDFs/Reports/FY2007FISMAReportCard.pdf - Windows Internet Explorer

http://republicans.oversight.house.gov/media/PDFs/Reports/FY2007FISMAReportCard.pdf

File Edit Go To Favorites Help

Hackers demand \$10m ransom... http://republicans.oversi... x

75%

Find

2 / 2

2007 2006

**FEDERAL COMPUTER SECURITY REPORT CARD** May 2008

**GOVERNMENTWIDE GRADE 2007: C (2006: C-)**

	2007	2006		2007	2006
			NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	C	D-
DEPARTMENT OF JUSTICE	A+	A-			
AGENCY FOR INTERNATIONAL DEVELOPMENT	A+*	A+	DEPARTMENT OF STATE	C*	F
ENVIRONMENTAL PROTECTION AGENCY	A+	A-	DEPARTMENT OF EDUCATION	C-	F
NATIONAL SCIENCE FOUNDATION	A+*	A+	DEPARTMENT OF COMMERCE	D+	F
SOCIAL SECURITY ADMINISTRATION	A+*	A	DEPARTMENT OF TRANSPORTATION	D	B
HOUSING AND URBAN DEVELOPMENT	A	A+	DEPARTMENT OF LABOR	D	B-
OFFICE OF PERSONNEL MANAGEMENT	A-	A+	DEPARTMENT OF DEFENSE	D-	F
GENERAL SERVICES ADMINISTRATION	B+	A	DEPARTMENT OF THE INTERIOR	F	F
DEPARTMENT OF ENERGY	B+	C-	DEPARTMENT OF TREASURY	F	F
DEPARTMENT OF HOMELAND SECURITY	B+	D	NUCLEAR REGULATORY COMMISSION	F	F
DEPARTMENT OF HEALTH AND HUMAN SERVICES	B	B	DEPARTMENT OF VETERANS AFFAIRS	F	N/A
SMALL BUSINESS ADMINISTRATION	B	B+	DEPARTMENT OF AGRICULTURE	F	F

\*Based on Financial Statement reporting and audit results showing "no significant deficiencies" we have confidence these grades accurately reflect agencies' ability to secure data.

Done

Unknown Zone

Start | Inboxes - Microsoft O... | Calendar - Microsof... | NISTOutline\_20090... | http://republicans... | NIST\_CMS\_2009HIP... | 6:58 PM

**Interoperable  
Health Information Technology  
DEMANDS  
Accessibility**

**FISMA's risk-based approach is not incompatible with accessibility.**

# CMS Information Security Program

- Policies and Standards
- Certification & Accreditation
- Security Technical Architecture
- Training & Awareness

# http://www.cms.hhs.gov/InformationSecurity/

The screenshot shows a Windows Internet Explorer browser window displaying the CMS Information Security Overview page. The browser's address bar shows the URL <http://www.cms.hhs.gov/InformationSecurity/>. The page header features the HHS.gov logo and the tagline "Improving the health, safety and well-being of America". Below this is the CMS logo and the text "Centers for Medicare & Medicaid Services". A navigation menu includes links for Home, Medicare, Medicaid, CHIP, About CMS, Regulations & Guidance, Research, Statistics, Data & Systems, Outreach & Education, and Tools. A secondary menu lists "People with Medicare & Medicaid", "Questions", "Careers", "Newsroom", "Contact CMS", "Acronyms", "Help", "Email", and "Print". The breadcrumb trail reads: [CMS Home](#) > [Research, Statistics, Data and Systems](#) > [Information Security](#) > Overview.

The main content area is titled "Information Security" and "Overview". On the left, a sidebar lists various sub-topics under "Information Security": Overview, Certification & Accreditation, Laws & Regulations, Policies, Standards, Procedures, EUA, Certification, CBT Instructions, Guidelines & Tools, Templates, Other References, and Info Security Library. The main text area contains the following sections:

- Overview**: CMS Information Security (IS) "Virtual Handbook". The links to the left are the collection of all CMS policies, standards, procedures, and guidelines which implement the CMS Information Security Program.
- "Holding Ourselves to a Higher Standard"**: As CMS is a trusted custodian of individual health care data, we must protect its most valuable assets, its information and its information systems. At CMS, we believe that putting the government's credibility at risk is not acceptable.
- Computer Based Training (CBT)** is mandatory for most users of CMS Information Systems when an individual is initially issued their CMS User Id and then in conjunction with annual certification of their CMS User Id. Select the "CBT Instructions" menu item on the left or the "Information Security CBT" link below.
- Access to CMS Systems** - for more information about CMS User Ids in the EUA system, the annual User Id certification process, EUA Passport or EUA Workflow, select the "EUA" link to the left or below. Select the "IACS" link below for User Ids related to Medicare Parts C and D.
- Identity Theft** - find out everything that you need to know about how to protect yourself or recovery from Identity Theft by visiting the Federal Trade Commission's web site by selecting the "Identity Theft" link below.
- Information System Security Officers (ISSO)** are the primary points of contact within each CMS Office/Center regarding information security issues and they are the component's liaison with the CMS Chief Information Security Officer (CISO). CMS contractors should contact their Project Officer in order to identify which ISSO supports their system. Select the "ISSO" link below.

The browser's taskbar at the bottom shows several open applications: Start, Microsoft Outlook (Inbox - Microsoft...), Microsoft Calendar (Calendar - Microso...), a document titled "NISTOutline\_20090...", the current page "Overview Informa...", another document "NIST\_CMS\_2009HI...", and a document "051909 CMS NIST ...". The system tray shows the date "5/22/2009", the time "7:27 PM", and the page zoom level "100%".

# Thought Question

- Can protected health information be both accessible and secure?
  - Decisions regarding the balance are made every day, but within the framework of the information security program policies & standards

# ENDING IN ACTION

- With the same partner you talked to at the beginning of my session, spend the next 3-4 minutes responding to these questions:
  - Is FISMA an unreasonable bar for any organization that values information security?
  - What are the information security barriers that will hold us back from achieving the vision of a nationwide, interoperable EHR for most Americans by 2014?