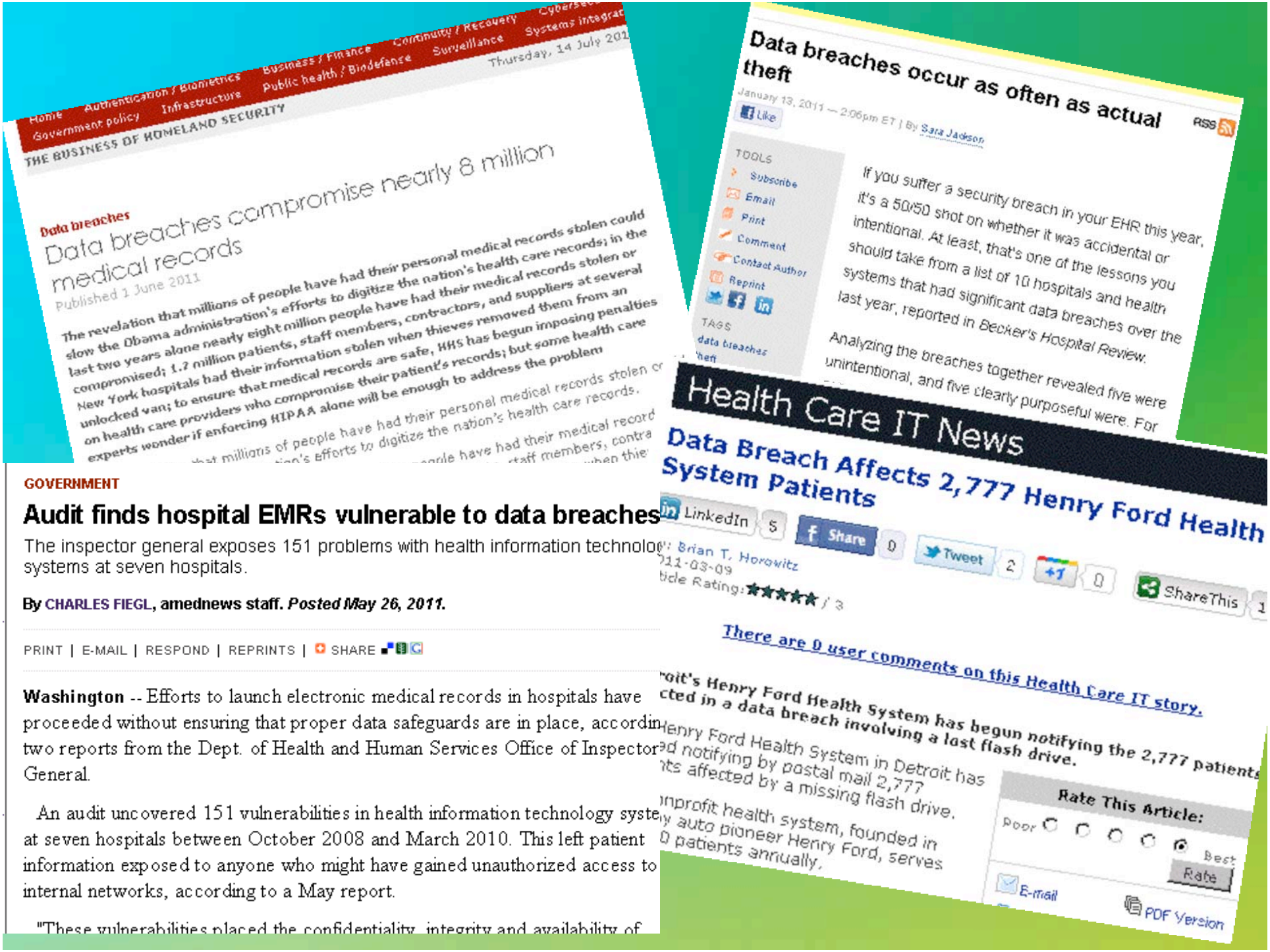
Redwood MedNet 2011 Security and Health Information Exchange Panel

Michele D. Guel
Senior Security Architect/Advisor/Evangelist
Global Employee Services IT

"My passion is to develop and build the next generation of cyber security professionals through innovative, relevant and collaborative training. Tribal knowledge doesn't work. Information and expertise must be shared and codified if we, as an industry, are to outpace the well-connected and highly-skilled cyber underground"

Background

- 23 year professional in the Information Security Field
- 11 years at NASA Ames, 15 years at Cisco
- Avid participant, speaker, teacher, influencer and evangelist in the cyber security industry for over 20 years
- All aspects of security (privacy, host, infrastructure, applications)
- Spent last 4 years securing employee workforce data & applications at Cisco
- Its is all about "building it in and not bolting it on"



THE BUSINESS OF HOMELAND SECURITY

Data breaches

Data breaches compromise nearly 8 million medical records

Published 1 June 2011

The revelation that millions of people have had their personal medical records stolen could slow the Obama administration's efforts to digitize the nation's health care records; in the last two years alone nearly eight million people have had their medical records stolen or compromised; 1.2 million patients, staff members, contractors, and suppliers at several New York hospitals had their information stolen when thieves removed them from an unlocked van; to ensure that medical records are safe, HHS has begun imposing penalties on health care providers who compromise their patient's records; but some health care experts wonder if enforcing HIPAA alone will be enough to address the problem

Data breaches occur as often as actual theft

January 13, 2011 — 2:06pm ET | By Sara Jackson

TOOLS
Subscribe
Email
Print
Comment
Contact Author
Reprint

TAGS
data breaches
theft

If you suffer a security breach in your EHR this year, it's a 50/50 shot on whether it was accidental or intentional. At least, that's one of the lessons you should take from a list of 10 hospitals and health systems that had significant data breaches over the last year, reported in Becker's Hospital Review.

Analyzing the breaches together revealed five were unintentional, and five clearly purposeful were. For

Health Care IT News

Data Breach Affects 2,777 Henry Ford Health System Patients

LinkedIn 5 Share 0 Tweet 2 +1 0 ShareThis 1

By Brian T. Horowitz
2011-03-09
Article Rating: ★★★★★ / 3

There are 0 user comments on this Health Care IT story.

Detroit's Henry Ford Health System has begun notifying the 2,777 patients affected in a data breach involving a lost flash drive.

The Henry Ford Health System in Detroit has begun notifying by postal mail 2,777 patients affected by a missing flash drive.

The nonprofit health system, founded in 1915 by auto pioneer Henry Ford, serves 1.2 million patients annually.

Rate This Article:
Poor Best
Rate

E-mail PDF Version

GOVERNMENT

Audit finds hospital EMRs vulnerable to data breaches

The inspector general exposes 151 problems with health information technology systems at seven hospitals.

By CHARLES FIEGL, amednews staff. *Posted May 26, 2011.*

PRINT | E-MAIL | RESPOND | REPRINTS | SHARE

Washington -- Efforts to launch electronic medical records in hospitals have proceeded without ensuring that proper data safeguards are in place, according two reports from the Dept. of Health and Human Services Office of Inspector General.

An audit uncovered 151 vulnerabilities in health information technology systems at seven hospitals between October 2008 and March 2010. This left patient information exposed to anyone who might have gained unauthorized access to internal networks, according to a May report.

"These vulnerabilities placed the confidentiality, integrity and availability of

My Views…

- The technical, privacy and security challenges with EHR and HIE are no different from Personal HR data (Safe Harbor) and PCI compliance. Is there really more at stake?
- The Health IT industry is relatively young and will face many of the same challenge as above.
- AARA may result in people joining “the party” before they are ready (i.e. knowledgeable about risks and secure).
- Compliance and Privacy does not mean security… Layers and levels
- End to end architecture & security must be a focus – endpoints are a risk.
- Security must be “built in” and not “bolted on”
- Strong partnerships with technical teams (architecture, networking & security) is needed from the beginning.
- Medical professionals & IT people working in medical environments must be more aware of the threats and changing landscape

Multiple Paths to Compromise…

Vulnerable applications allow attacks through defense-n-depth technologies

Insufficient defense-n-depth allows attacks despite well secured applications.

It's inevitable…

Many Places Where Things Are Going Wrong...

- Infrastructure Gaps
- Configuration Errors
- Architecture Misses
- Coding Errors
- Data Governance Issues
- Broken Processes
- Incidental Data Exposure
- Insecure Transmission
- Insecure Storage Points
- Users & Decision Makers

If we are not looking, does that mean it's not broken?

Security must be part of the DNA

That means:
Built in, not Bolted on…

Security DNA Building Blocks

- Ownership
- Knowledge
- Partnerships
- Visibility
- Informed Decisions

- Strong, Multi-factor Authentication
- Identity Management System
- File Encryption Technology
- Encryption Technology
- Data Centric Controls
- Network Firewalls
- Application Firewall
- Malware Defense
- SIMS
- IDS/IPS
- OS and Application Hardening
- Runtime/execution restrictions
- Application Vulnerability Testing

- Standards
- Policies
- Imperatives
- Templates
- Training
- Awareness
- Governance


Is the Health Informatics industry willing to do what it takes?

Thank you.