Medical Identity Theft

updated slides available at www.pskl.us

Eric Smith
Bucknell University

Dr. Shana Dardan
Susquehanna University

Eric Smith and Dr. Shana Dardan

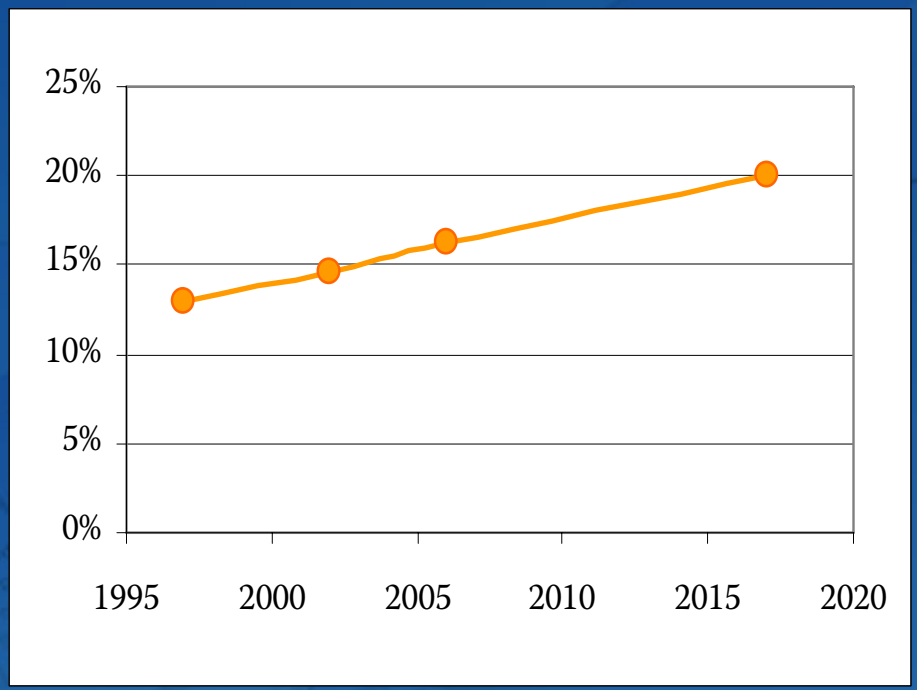
…Because of the difficulty in detection, the potential exists for this crime to be happening substantially more frequently than anyone has documented to date...

World Privacy Forum, Spring 2006

Eric Smith and Dr. Shana Dardan

Background of the Problem

US Health Care Costs as a Ratio of the GDP:



1997: 13.0%
2002: 14.6%
2006: 16.3%
2017: 20.0% [Forecast]

-Washington Post, 2008

Eric Smith and Dr. Shana Dardan

Who is paying for this?

- Businesses
- Governments
- Ultimately – the consumer

Craig Barrett, then-CEO of Intel noted in 2006 that health care costs were a driving factor in Intel's decision to pursue operations overseas.

Cutting Costs

- Digitize patient medical records
- Transmit them across a private network
- Patients' records can be shared easily among doctors and other health care providers

- "HIT Report at a Glance," U.S. Department of Health and Human Services Press Release, 7/21/04

Eric Smith and Dr. Shana Dardan

Cutting Costs

- Increased efficiency
- Better communication, especially between health care providers
- Reduction in medical errors
- Sutter Health: 88,000 medical errors prevented in first three years

- Conversations with Sutter Health, 2008

Costs of Medical Errors

~$17 to $29 billion per year

- "The Quality of Health Care Delivered to Adults in the United States," *New England Journal of Medicine*; June 2003

Costs of Medical Errors

98,000 deaths per year

- "To Err is Human: Building a Safer Health System;" Institute of Medicine, 2000, pg 26

The NHIN: National Health Information Network

"The very comprehensive and ubiquitous nature of the NHIN that makes it attractive also makes it a source of concern. If digitized medical records can move throughout a nationwide system easily and quickly, then that means that incorrect files, factual data, etc. will also move easily and quickly between every doctor and hospital."

- Dixon, 2006

Billions of Dollars and Computers: Fraud

"Certain kinds of fraud – such as falsification of medical records – probably would not be detected through current methodology… Some experts suggest that a statistically valid estimate of fraud might not be possible at all, given the covert nature and level of evidence necessary to meet the legal definition of fraud."

-Testimony given by Penny Thompson, Program Integrity Director, Health Care Financing Administration before the House Budget Committee Task Force on Health. (Federal News Service, July 12, 2000.)

Eric Smith and Dr. Shana Dardan

Health Care Fraud: Victims

Accounts for 3-10% of all health care costs
$120 to $500 billion per year

Demand for medical records? ID Theft:
-Lack of health insurance
-Fear of losing current or future employment

- Malcolm Sparrow , Harvard University

Medical Identity Theft

Eric Smith and Dr. Shana Dardan

Eric Smith and Dr. Shana Dardan

Real-Life Gattaca

In 2001, the Equal Employment Opportunity Commission sued Burlington Northern and Santa Fe Railway Company after the company genetically tested or sought to test employees' blood without their consent or knowledge. The testing was part of an examination for employees who had filed compensation claims for carpel tunnel syndrome; in response to the filing, the company wanted to know if those employees had a genetic predisposition to carpel tunnel syndrome.

The case was settled out of court in 2002 for $2.2 million.

Equal Employment Opportunity Commission vs. The Burlington Northern and Santa Fe Railway Company - Civil Action File No. 02-C-0456

Eric Smith and Dr. Shana Dardan

"Medical identity theft often leaves its victims without substantive recourse or clear pathways to follow for help. Recovery for victims of medical identity theft may be difficult or impossible because of the lack of enforceable rights, and because the dispersed and often hidden nature of medical records."

- World Privacy Forum, Spring 2006

Consumer Protections: Medical versus Financial

	FCRA	HIPAA
Correcting Errors	System in Place	No System
Viewing your Record	System in Place	No System
Legal Recourse	System in Place	No System

How hard would it be?

Hospital Penetration Tests:

- HIPAA-compliant facility
- Good physical and IT security
- 3.2 million patient records obtained in < 1 hour

Hospital Networks: Weak Spots

Discreet analysis at other large hospitals suggest that this is a widespread phenomena.

In this scenario, how does the "reasonable measures" clause compare with vulnerabilities discovered?

Eric Smith and Dr. Shana Dardan

Hospital networks: what's unique?

- Most areas open to the public 24/7
- Security staff are accustomed to random people
- Prevalence of guest/patient WiFi networks makes blending in easy

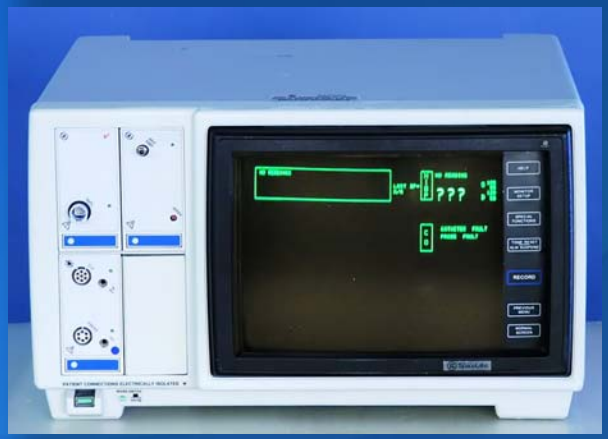
- Focus of our research: public areas in hospitals

Hospital Wireless Networks

- Typical Notebook PC / PDA Uses
- VoIP Handsets
- Equipment Monitoring
- Patient Vital Signs

Eric Smith and Dr. Shana Dardan

Medical Hardware



Many systems use embedded Windows or Linux.

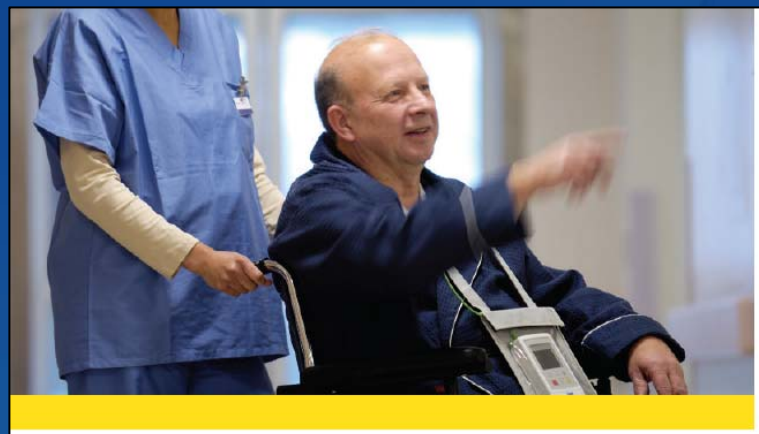
Providers are frequently unable to apply operating system patches due to software validation issues.

Few systems include anti-virus or anti-spyware packages.

Most systems are connected to the provider's production network.

Medical Identity Theft

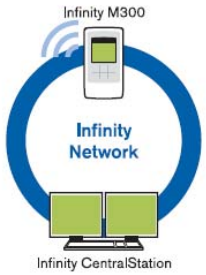
Eric Smith and Dr. Shana Dardan



Today's flexible WiFi technology

Reliable, industry-standard wireless technology
The Infinity Network forms the foundation of the Infinity M300 system. Fully compliant with IEEE 802.11 b/g standards, Infinity M300 and its Infinity Network share the same commercial access points* as wireless Infinity patient monitors.

Infinity M300 also supports Infinity OneNet, Dräger's awar winning shared infrastructure deployment that integrates pat monitoring systems into the ex hospital network, rather than re a separate network.



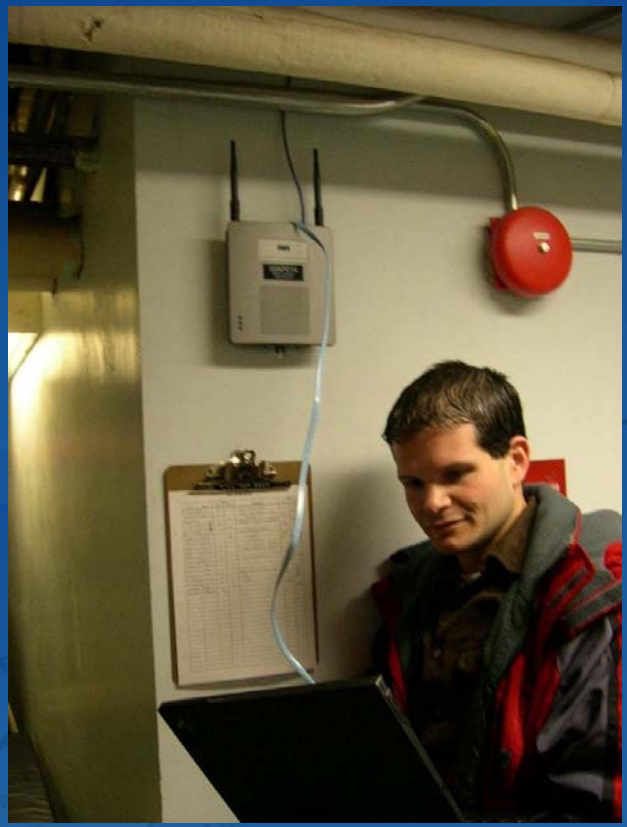
Reliable, industry-standard wireless technology

The Infinity Network forms the foundation of the Infinity M300 system. Fully compliant with IEEE 802.11 b/g standards, Infinity M300 and its Infinity Network share the same commercial access points* as wireless Infinity patient monitors.

Physical Attacks against a Wireless Network

Medical Identity Theft

Eric Smith and Dr. Shana Dardan



Eric Smith and Dr. Shana Dardan

Demo: Automating the Attack

Eric Smith and Dr. Shana Dardan

Questions?