



Innovation 2010:  
On the Threshold of Meaningful Use

## Healthcare Goes Digital: Healthcare Regulations via the Lens of PCI DSS



Joy Marie Forsythe  
Security Researcher  
jforsythe@fortify.com

[www.govhealthitconference.com](http://www.govhealthitconference.com)



Innovation 2010:  
On the Threshold of Meaningful Use

### Healthcare Goes Digital

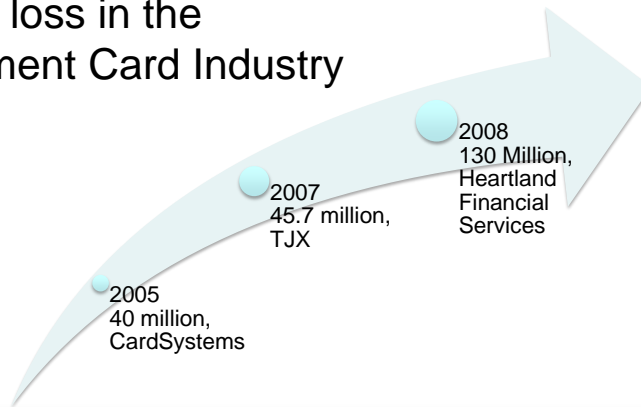
- Government incentives
- Improve care
- Increase efficiency

*Haven't we been here before?*



[www.govhealthitconference.com](http://www.govhealthitconference.com)

## Data loss in the Payment Card Industry



[www.govhealthitconference.com](http://www.govhealthitconference.com)

## PCI DSS Overview

- Industry security standard to prevent credit card fraud
- Published in 2005, updated in 2006 and 2008



[www.govhealthitconference.com](http://www.govhealthitconference.com)



Innovation 2010:  
On the Threshold of Meaningful Use

## PCI DSS Response

- Compliance is no guarantee of security
- Most systems turn out not to be compliant

But...

*"Regulation--SOX, HIPAA, GLBA, the credit-card industry's PCI, the various disclosure laws, the European Data Protection Act, whatever--has been the best stick the industry has found to beat companies over the head with. And it works. Regulation forces companies to take security more seriously, and sells more products and services." - Bruce Schneier*

[www.govhealthitconference.com](http://www.govhealthitconference.com)



Innovation 2010:  
On the Threshold of Meaningful Use

	Credit Card Merchants	Health IT Systems
Assets	Credit card information, customer personal information	Patient medical information, patient personal information
Motives	Financial	Privacy, improving care, research, financial
Roles	Merchant and processor	Doctors, nurses, pharmacists, patients, insurance companies
Context	Proprietary IT systems	COTS, proprietary systems, open-source, combinations

[www.govhealthitconference.com](http://www.govhealthitconference.com)

## Health IT Assets - Challenges

- Patient medical information is immutable and irreplaceable



But...

- Overly stringent control can lead to serious harm

## Health IT Assets - Approach

- Must identify different class of sensitive data
- Increased scrutiny of treatment of sensitive data



Innovation 2010:  
On the Threshold of Meaningful Use

## Health IT Motives

- Financial mitigation
  - More stringent about large transactions
- Non-financial mitigation
  - What data is more potentially harmful?
  - What data is lack of access to more potentially harmful?
  - How to aggregate data?

[www.govhealthitconference.com](http://www.govhealthitconference.com)



Innovation 2010:  
On the Threshold of Meaningful Use

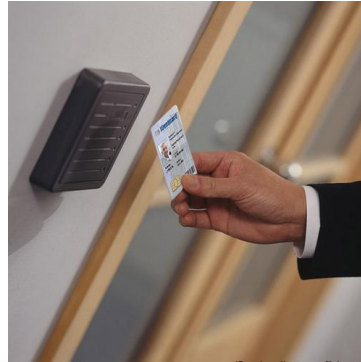
## Health IT Roles - Challenges

- More levels of access
  - Doctors, pharmacists, and patients will see different types of information
  - Each role could have many tasks
- Patients are a special case

[www.govhealthitconference.com](http://www.govhealthitconference.com)

## Health IT Roles – Approach

- Increased emphasis on access control
- Greater importance on auditing



IDcardimages, flickr.com

[www.govhealthitconference.com](http://www.govhealthitconference.com)

## Health IT Context - Challenges

- Health IT systems are rarely homogenous
  - COTS
  - Different systems must interact securely
- Multiple physical sites
  - Data in the cloud

[www.govhealthitconference.com](http://www.govhealthitconference.com)



Innovation 2010:  
On the Threshold of Meaningful Use

## Health IT Context – Approach

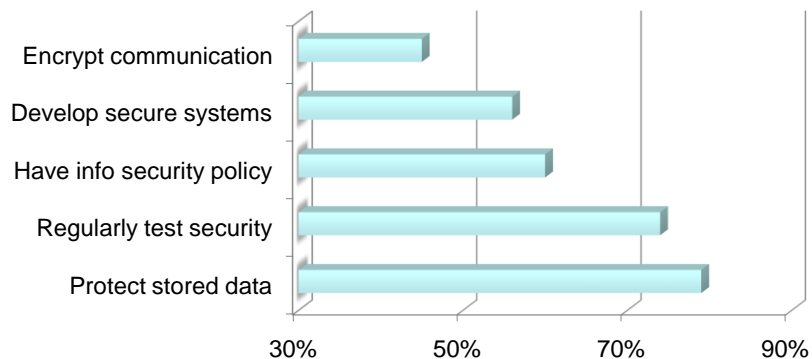
- Assess security of any COTS before purchase
- Test security of the system as a whole, not just components
- Remove infrastructure dependencies to facilitate moving components to the cloud

[www.govhealthitconference.com](http://www.govhealthitconference.com)



Innovation 2010:  
On the Threshold of Meaningful Use

## Areas of Failure in PCI DSS Assessments



VeriSign Global Security Consulting Services, "Lessons Learned: Top Reasons for PCI Audit Failure and How to Avoid Them"

[www.govhealthitconference.com](http://www.govhealthitconference.com)



Innovation 2010:  
On the Threshold of Meaningful Use

#### PCI Lessons Learned #1

### Encrypt sensitive data and communication properly

- Many breaches of other types would have been mitigated if data was properly encrypted
- 79% of failed PCI DSS assessments involved a failure to protect stored data, 45% involved a failure to encrypt the transmission of sensitive information

[www.govhealthitconference.com](http://www.govhealthitconference.com)



Innovation 2010:  
On the Threshold of Meaningful Use

#### PCI Lessons Learned #1 cont.

### Failure to encrypt data a known issue for Health IT Systems

- Sept 2006: VA laptop containing the unencrypted medical and personal information of 1600 veterans stolen



Encryption addressed in HHS initial set of standards

[www.govhealthitconference.com](http://www.govhealthitconference.com)

June 15-16, 2010  
GOVERNMENT  
**HEALTH IT**  
conference & exhibition  
sponsored in part by HIMSS

Innovation 2010:  
On the Threshold of Meaningful Use

Obvious Problem **Why is this still a problem?** Obvious Solution

[www.govhealthitconference.com](http://www.govhealthitconference.com)

June 15-16, 2010  
GOVERNMENT  
**HEALTH IT**  
conference & exhibition  
sponsored in part by HIMSS

Innovation 2010:  
On the Threshold of Meaningful Use

PCI Lessons Learned #2

Verify the security of the system, not just the security features

- Security vulnerabilities will not be uncovered before an exploit without regular testing
- Options
  - Test deployed systems, manually or automatically
  - Review source code, manually or automatically

[www.govhealthitconference.com](http://www.govhealthitconference.com)



Innovation 2010:  
On the Threshold of Meaningful Use

## Root cause of security problems

- Gartner – 75% of breaches due to security flaws in software
- NIST – 92% of vulnerabilities are in software
- Yet, 90% of security spending is on perimeter protection

## Even the Best Developers Write Insecure Code

- Custom, COTS, Open Source, Third Party
- False Safety in Firewalls/Perimeter Defense

[www.govhealthitconference.com](http://www.govhealthitconference.com)



Innovation 2010:  
On the Threshold of Meaningful Use

## PCI Lessons Learned #2 cont.

- PCI DSS evolution
  - V1.1: Best practice, either
    - Code review or vulnerability assessment
    - WAF
  - Mandatory as of June 2008, 75% of failed assessments involve a lack of regular security testing
  - Still room to improve...



HHS security standards do not go beyond security features

[www.govhealthitconference.com](http://www.govhealthitconference.com)



Innovation 2010:  
On the Threshold of Meaningful Use

### PCI Lessons Learned #3

## Education and training are key to preventing future vulnerabilities

- Only 25% of PCI DSS assessments passed on the first try, most failed in multiple areas
- Most vulnerabilities due to similar mistakes
  - Human: easily guessed passwords, failure to physically secure data
  - Developer: input validation, configuration
  - Administrator: access control, auditing

[www.govhealthitconference.com](http://www.govhealthitconference.com)



Innovation 2010:  
On the Threshold of Meaningful Use

- PCI DSS
  - Requires organizations to maintain an information security policy
    - Process for identifying threats and vulnerabilities
  - Led some organizations to adopt a Secure Development Lifecycle

Current HHS regulations lack this level of detail,  
but increased attention to security is a start...

[www.govhealthitconference.com](http://www.govhealthitconference.com)



Innovation 2010:  
On the Threshold of Meaningful Use

## Health IT systems present challenges not considered in PCI DSS

- Increased focus on data security and access control
- Need to assess security of components and entire system

[www.govhealthitconference.com](http://www.govhealthitconference.com)



Innovation 2010:  
On the Threshold of Meaningful Use

## However, the lessons learned from the PCI industry are not unique

- Protect data
- Focus on secure systems, not security features
- Education and training can prevent future vulnerabilities

[www.govhealthitconference.com](http://www.govhealthitconference.com)



Innovation 2010:  
On the Threshold of Meaningful Use

## Fortify Software: Software Security Assurance

- Fortify 360
  - Vulnerability Detection: static code analysis, program trace analysis, real-time analysis
  - Remediation
  - Governance
  - Compliance
- Fortify OnDemand
- Services and Training

[www.govhealthitconference.com](http://www.govhealthitconference.com)



Innovation 2010:  
On the Threshold of Meaningful Use

## Insurance company

- Motivation:
  - PCI Compliance
  - Preventing breaches
- Results
  - Passed PCI audit where other business units did not
  - Reduced costs through improved developer efficiency

[www.govhealthitconference.com](http://www.govhealthitconference.com)



Innovation 2010:  
On the Threshold of Meaningful Use

## Healthcare Systems Provider

- Motivation
  - Customer required implementation of security best practices
- Results
  - Reduces business risk
  - Meets contractual obligations
  - Reduces time to market for new applications

[www.govhealthitconference.com](http://www.govhealthitconference.com)



Innovation 2010:  
On the Threshold of Meaningful Use

## Questions?

Drop by Booth #25 on show floor  
for more information

[www.govhealthitconference.com](http://www.govhealthitconference.com)