GE Healthcare

Medical Device Product Security

Patient Safety…Patient Privacy…Patient Care

Presentation to the:
Information Security and Privacy Advisory Board
03-March-2011

Steven Abrahamson
Program Manager, Product Security
GEHC Science and Technology Office

GE imagination at work
Topics

GE Healthcare and the Healthcare Environment

Medical Device Security Environment and Challenges

Improving Security within the Medical Device Environment

Moving Forward
GE Healthcare

**Broad-based Technologies**
- Diagnostic imaging & surgery technologies
- Clinical products
- Medical diagnostics

**Information Technology**
- Integrated admin. & clinical
- Electronic medical records
- Picture Archiving System (PACS)

**Life Sciences**
- Biopharmaceutical solutions
- Protein & cell sciences
- Service

© Copyright GE Healthcare 2011
Our Purpose  At Work For A Healthier World
Our Strategy  Healthymagination

healthymagination

A new business strategy to address global healthcare needs

- **Reduce the cost** of health procedures and practices through GE technologies and services
- **Improve quality** and efficiency by simplifying ways of driving best standards of care
- **Increase access** to better health for more people through low-cost innovation, education, and financing

$6 billion commitment to make health sustainable
Where does cybersecurity fit?

A new business strategy to address global healthcare needs

- **Reduce the cost** of health procedures and practices through GE technologies and services
- **Improve quality** and efficiency by simplifying ways of driving best standards of care
- **Increase access** to better health for more people through low-cost innovation, education, and financing

$6 billion commitment to make health sustainable
Medical Device Security Environment

Growing Government and Customer interest…

HIPAA, HITECH, and other laws creating growing security focus among healthcare providers, and cybersecurity getting more attention in Congress – “Cyber is a new domain of vandalism, crime, espionage, and, yes, warfare, but we are not very well equipped to deal with any of those challenges…we need to act to improve our security.” Rep Mac Thornberry, Feb 11, 2011

FDA recognizes security relationship to patient safety…

FDA Guidance issued 2005 on manufacturer’s responsibility for addressing cybersecurity vulnerabilities as integral to ensuring the safety and effectiveness of the device within the requirements of the Quality System Reg.

But security features can introduce new risks…

“Our concern for products is: Are they safe and are they effective? We don’t weigh in on security per se, but on measures like encryption that might affect or could have an impact on product safety and effectiveness, we might look at…” – Karen Riley, FDA Spokesperson (Boston Globe, July 5, 2010)
Security Touch Points and Challenges

**Product Design** - making new products secure
- Long Product Life Cycles (20 yrs+)
- Emphasis on clinical functionality

**Product Installed Base Support** – enhancing our existing products
- Patch/Anti-Virus = design change
- Design changes require validation

**Service Technology** – remote service operations
- Focus on accessibility and uptime
- Reliance on remote monitoring

**Service** – supporting customer’s privacy and security obligations
- Large distributed workforce
- New operational rigor needed
Design Actions within the Quality System

Rigorous design controls for new designs and design changes

• Validation … “confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses, and that the particular requirements implemented through software can be consistently fulfilled.” – a comprehensive process of testing, analysis, documentation, and review

• Risk Management…looks at severity of harm and probability of occurrence…considers failure modes and expected user error…defines a threshold for action

Changes add risks: FDA study shows 79% of software defects that resulted in product recalls were introduced by changes

Validations are not days, but rather weeks or months of effort

No safe harbor for adverse events caused by security
Layered Security in Healthcare

Must consider security risks at...

Security at each layer must work together

Device manufactures do not have visibility to all security risks and mitigations
Working Toward Improved Security

Building the Security Team at GEHC:

- Customers
- Industry Groups
- GEHC IT
- GE Corp IT
- Service
- Legal
- Design Engineering
- Sales & Marketing
- Product Security Program
Integrating Security with Design

The medical device design continual improvement process (simplified):

Enhancing the Influence of Security:

User Needs – expand beyond clinical needs to security needs

Risk Assessment – use scanning tools to recognize security risks

Field Use / Complaints – track customer security concerns

External Requirements – Focused implementation program
Medical Device Security: Moving Forward

Product Security is not “one-size-fits-all” across the broad spectrum of networked devices

Security programs must be consistent with risks and patient safety needs

A collaborative approach needed to address security standards within the various layers: site, department, network, device

Safety and security – collaboration, not competition