

CHOP Annual Health Informatics Symposium 30 April, 2010 – Philadelphia, PA

## HIPAA 2.0

# The next generation of HIPAA: Effects of ARRA- and FDA-related security issues

(Living in a High Tech - HITECH World)

**Elliot B. Sloane, PhD, CCE, FHIMSS**

Drexel University Health Systems Engineering Director

Founder, Center for Healthcare Information Research and Policy

Co-Chair, IHE International

Board of Directors, Delaware Valley HIMSS

Board of Directors, ANSI Healthcare Technology Standards Panel

Sponsor, IEEE 11073 Medical Informatics Standards

Past Chair, HIMSS Security and Privacy Steering Committee



# Elliot Sloane's Bio Brief

- 35+ years in the medical technology and IT/HIT fields, as a technology/engineering expert and consumer/safety advocate
  - Biomedical and Clinical Engineering core
  - Information Systems and Sciences graduate
- 25 years as a CIO, COO, CTO, CRO in the medical technology industry (ECRI Institute & MEDIQ, Inc)
- 10+ years in business schools, MIS, CS, and, finally, ***Health Systems Engineering*** at Drexel University
  - Founder and board member/chair with multiple non-profits
  - Consultant to US gov't and World Health Organization
    - Specializations: medical devices, privacy, security, patient safety (and related technical standards and policies)

# A brief US historical legislative context

- Interoperable electronic health records evolved out of a two-decade journey:
  - Hillary Clinton and Senator Harris Wofford helped broker “HIPAA 1.0,” the core of which was “administrative simplification” in the mid-90’s
    - The arrival of Electronic Data Interchange (EDI) to healthcare, with national standardized billing coding
    - Allowed insurance portability from employer to employer
  - The Security/Privacy aspects that you and I commonly call “HIPAA,” though, were simultaneously instituted to protect consumers’ health data privacy once insurance and employer portability was mandated

# G.W. Bush Administration launched this century's new EHR climate!

- 2004 Bush Presidential Executive Order mandates:
  - Personal health record for EVERY US citizen by 2014
  - New Office of the National Coordinator of Health IT within the Department of Health and Human Services
  - National “HIT Strategic Plan” by 2005 to develop necessary HIT standards, architecture
- 2006 Bush Presidential Executive Order
  - ALL federal health IT purchases MUST use federally-approved HIT standards exclusively if/when such standards exist!

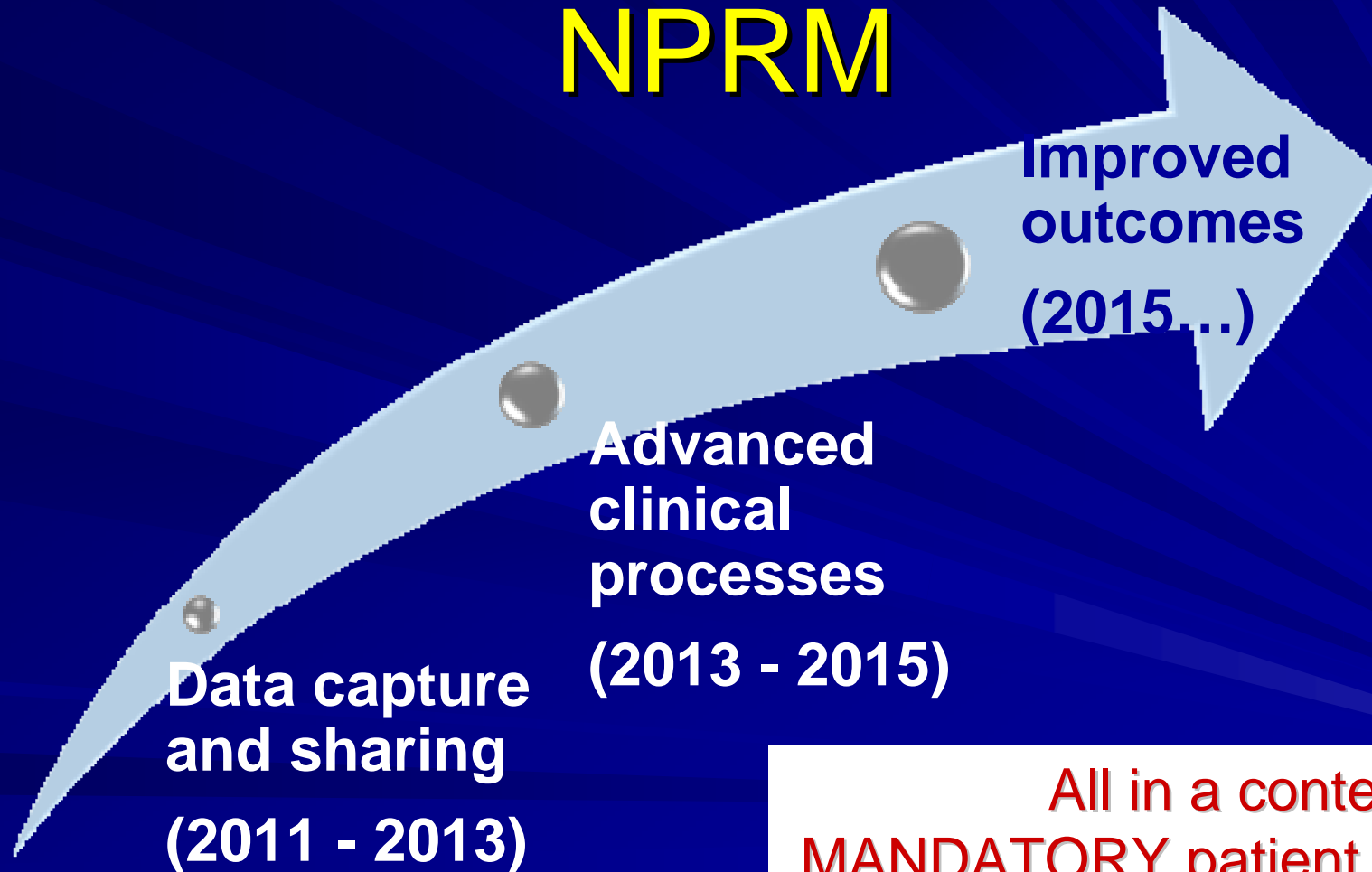
# Obama Administration has adopted, endorsed, and FUNDED those mandates!

- Nearly half of the pages of the American Recovery and Reinvestment Act of 2009 were devoted to Electronic Health Records
  - HHS ONCHIT was made permanent, with an initial \$2 Billion budget
  - \$30 Billion earmarked for CMS incentive payments to physician's and hospitals for standardized/certified EHRs through 2015
  - STRONG new personal health data privacy and access rights and penalties (leading to HIPAA 2.0)

# From Feb'09 ARRA to today...

- Exhaustive work/rework of 2004-2010 standards work
  - Focused on “operationalizing” the mandates
  - Promulgation of final regulations for EHRs, “meaningful use” exchange of patient’s clinical data, and CMS incentive payments
- August, 2009, personal health data “Breach” Notification Interim Final Rule (IFR) posted by NIST, specifying encryption and data destruction requirements
- Interim Final Rule (IFR) posted 30 December 2009 by ONC specifying HIT/EHR data exchange standards AND the specific privacy and security requirements
- 30 December, 2009 also posted the Notice of Proposed Rule Making (NPRM) by CMS for incentive payments under the “Meaningful Use” ARRA regulation
- Mid March, 2010, NPRMs regarding certification programs for software systems by NIST

# Meaningful Use, as articulated in the 12/30/2009 IFR and NPRM



All in a context of  
**MANDATORY** patient data  
privacy and security

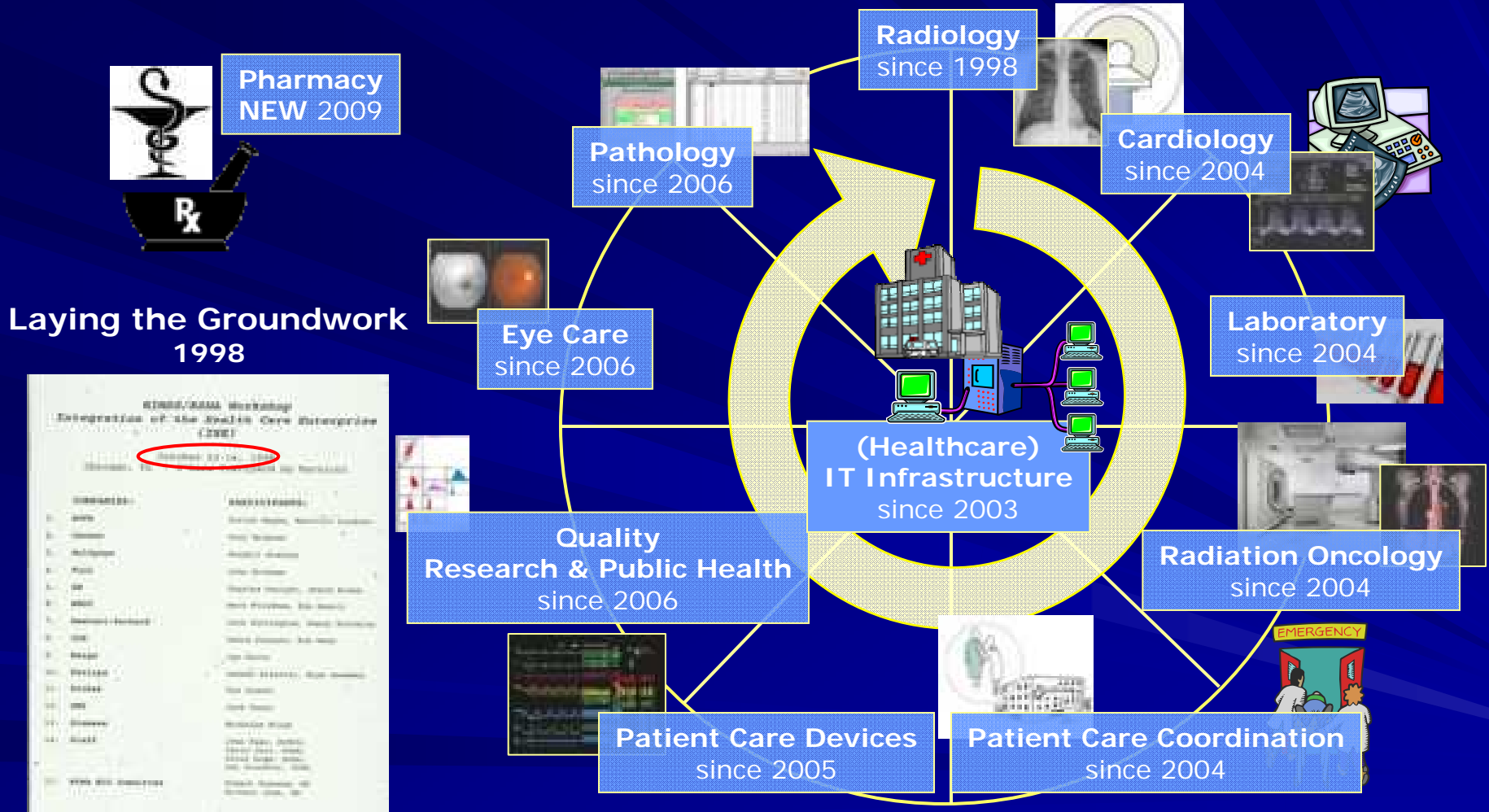
At the same time, an overarching electronic patient data sharing architecture labeled “**IHE**” has been developed and deployed around the world since the late 90’s.

- This architecture is “**IHE**,” which stands for **Integrating the Healthcare Enterprise**
  - IHE underlies all of our US Federal Health Architecture (FHA) used by DoD and VA (**FHA Connect**)
  - IHE also underlies all of our Nationwide Health Information Network (**NHIN Direct**) sponsored by ONC

IHE is not yet mandated for CMS Meaningful Use incentives; the initial CMS reimbursement requirements are much, much simpler.

# IHE: Integrating the Healthcare Enterprise

Based on 11 Years of Steady Evolution 1998 – 2010

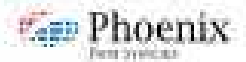


Leadership



Partnership of 2013  
© 2014 American Information and Management Systems Society

Implementer



Supporter



Organizational Participants



# HIPAA 2.0 Topic Preview

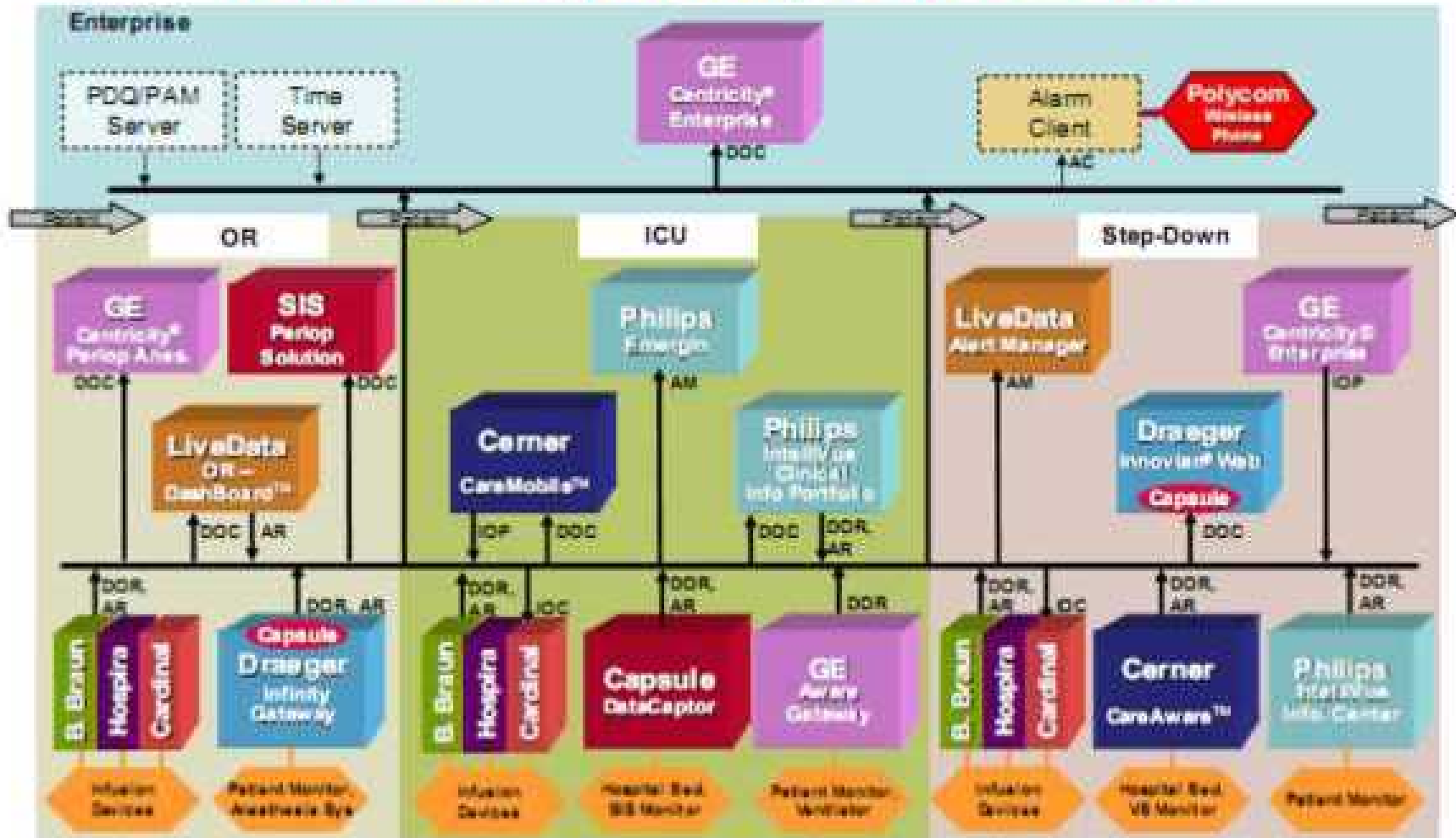
- The High Tech world
- The HITECH world
- CIAS – the “extended security” world of medical devices
- Conclusion

# Topics

- The High Tech world
  - Data wants to be free!
  - One example: the diffusion of mobile medical devices into the home, directly connected to electronic health records for physician/nurse oversight
- The HITECH world
- CIAS – the “extended security” world of medical devices
- Conclusion

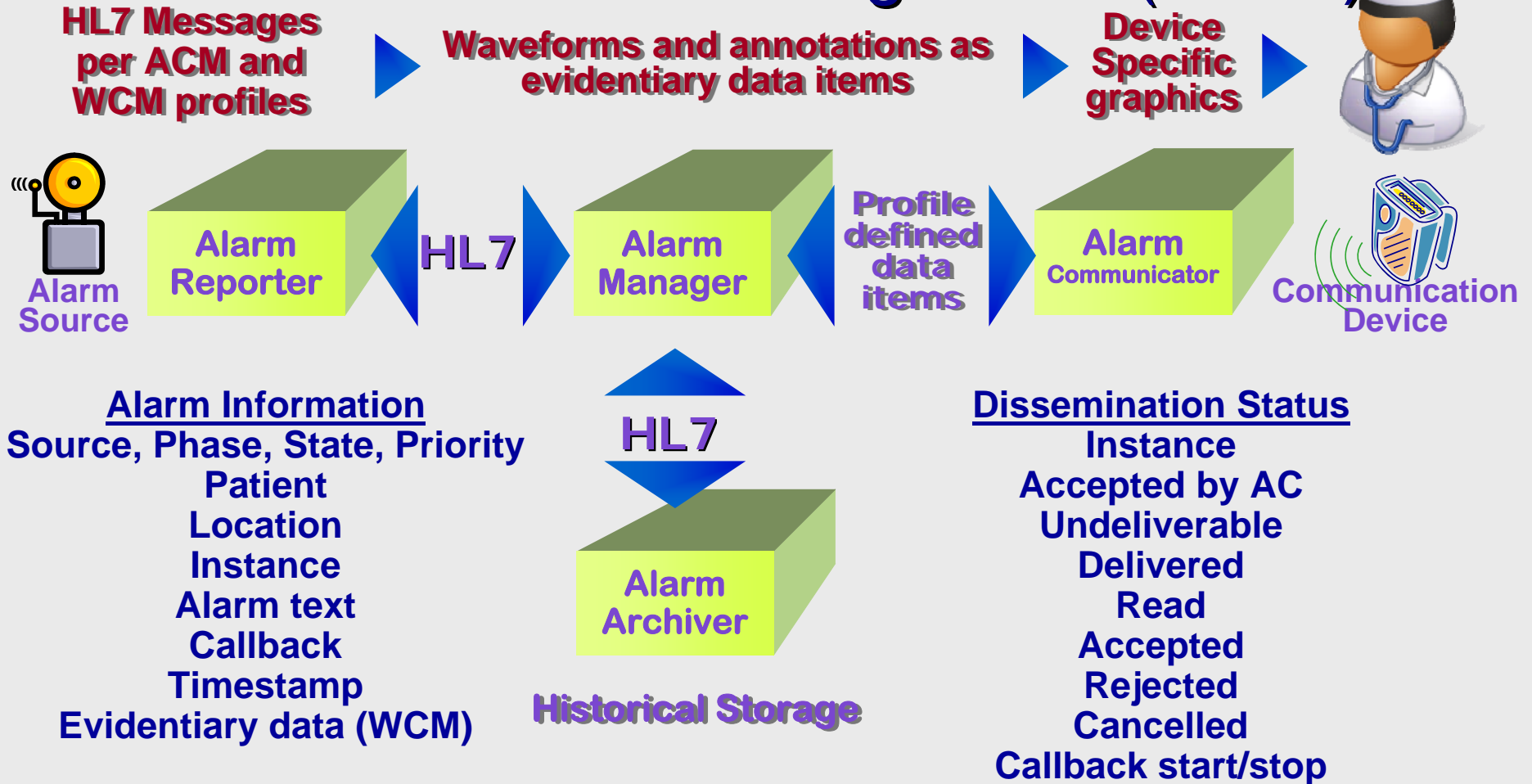
After over 5 years of hard work, medical device standards are seeing terrific uptake!

**HIMSS** **IHE** Patient Care Devices  
**HIMSS Interoperability Showcase 2009** **ACCE**



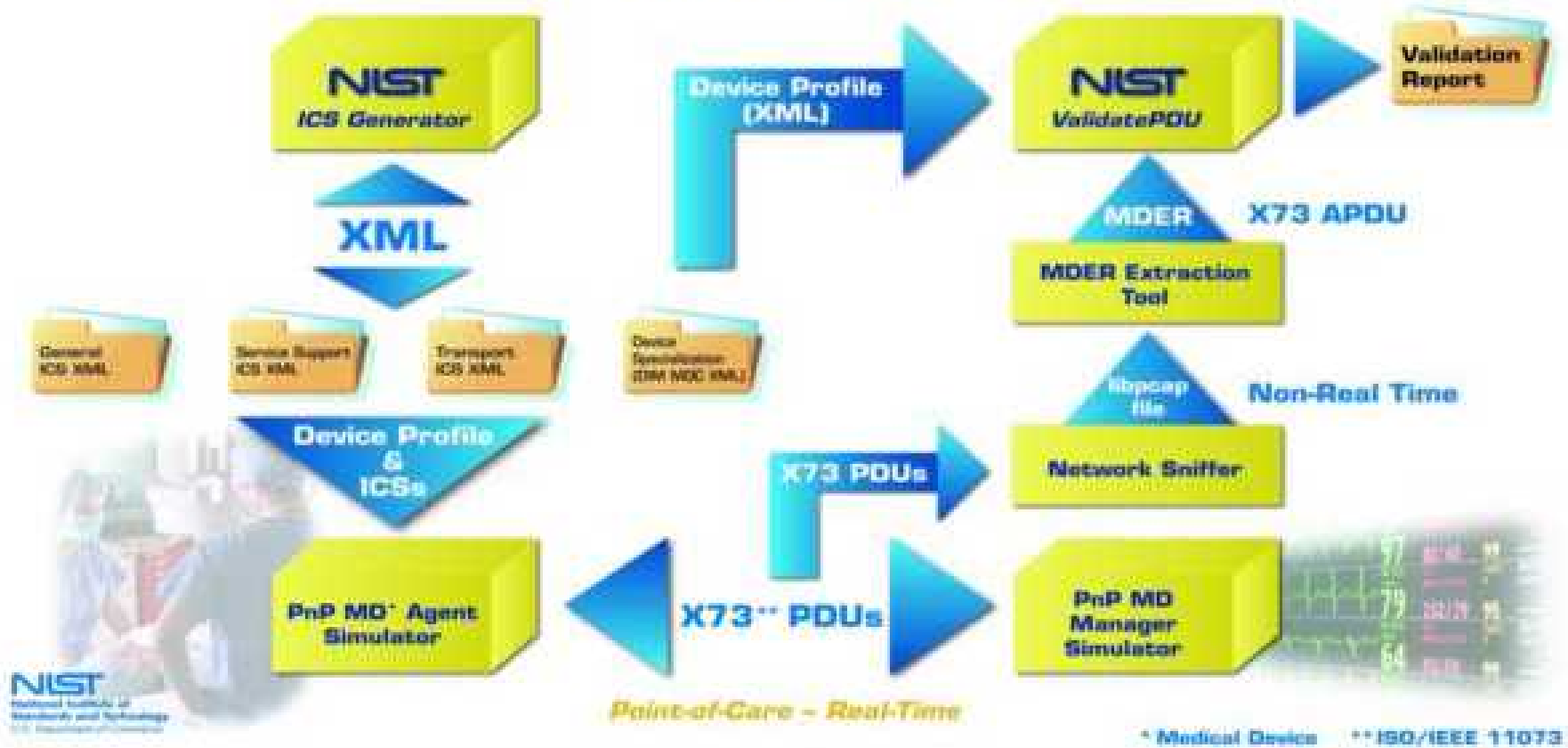
DOR = Device Observation Reporter / DOC = Device Observation Consumer  
 AR = Alarm Reporter / AM = Alarm Manager; IOP = Infusion Order Programmer / IOC = Infusion Order Consumer

# Includes Life-Critical Alarm Communication Management (ACM) and Waveform Communication Management (WCM)



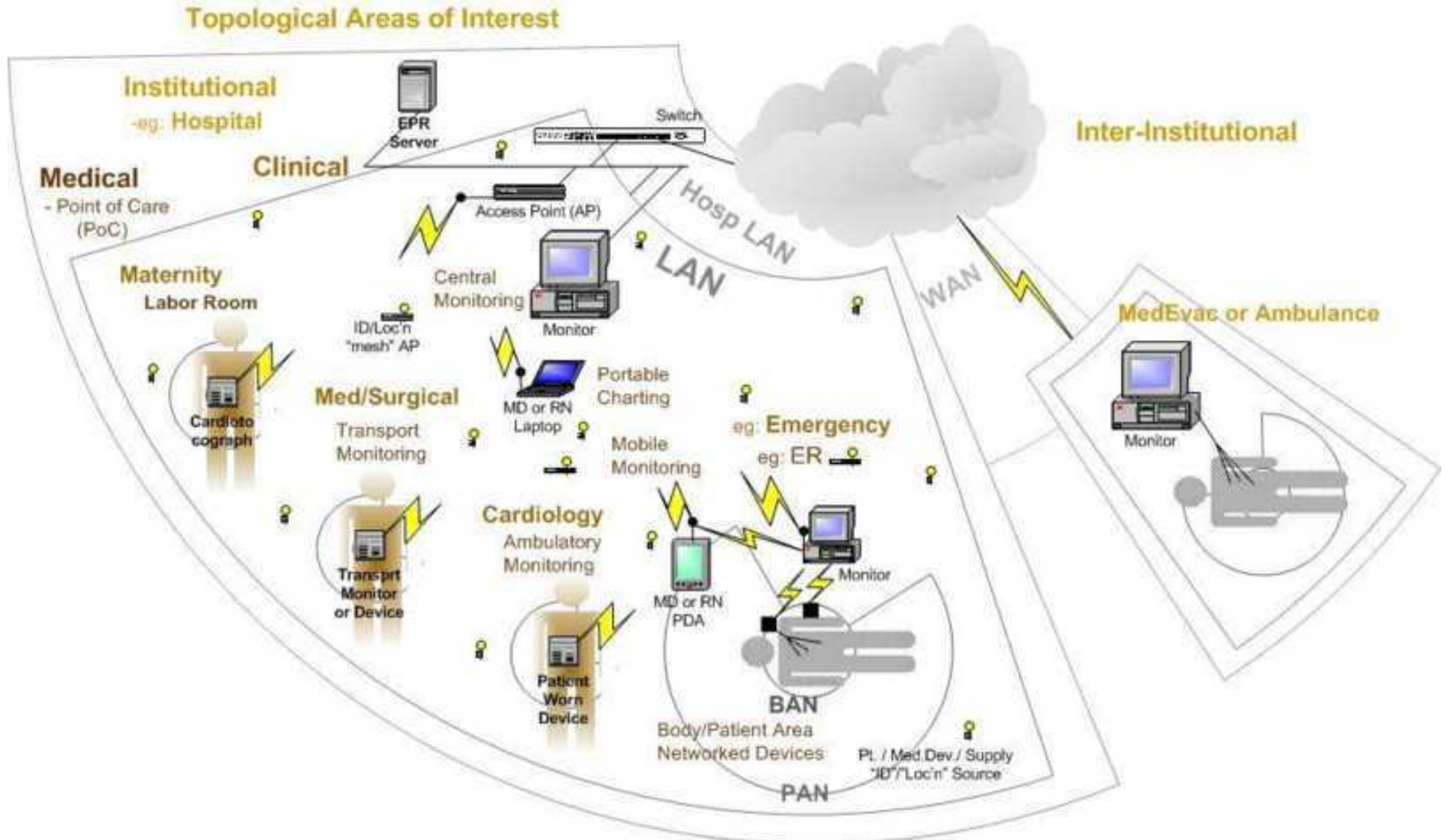
***The devices, data, and alarms interoperate with each other AND the EHR systems.***

## Medical Device Communication Test Process Point of Care, Plug-n-Play, Real-Time Profile



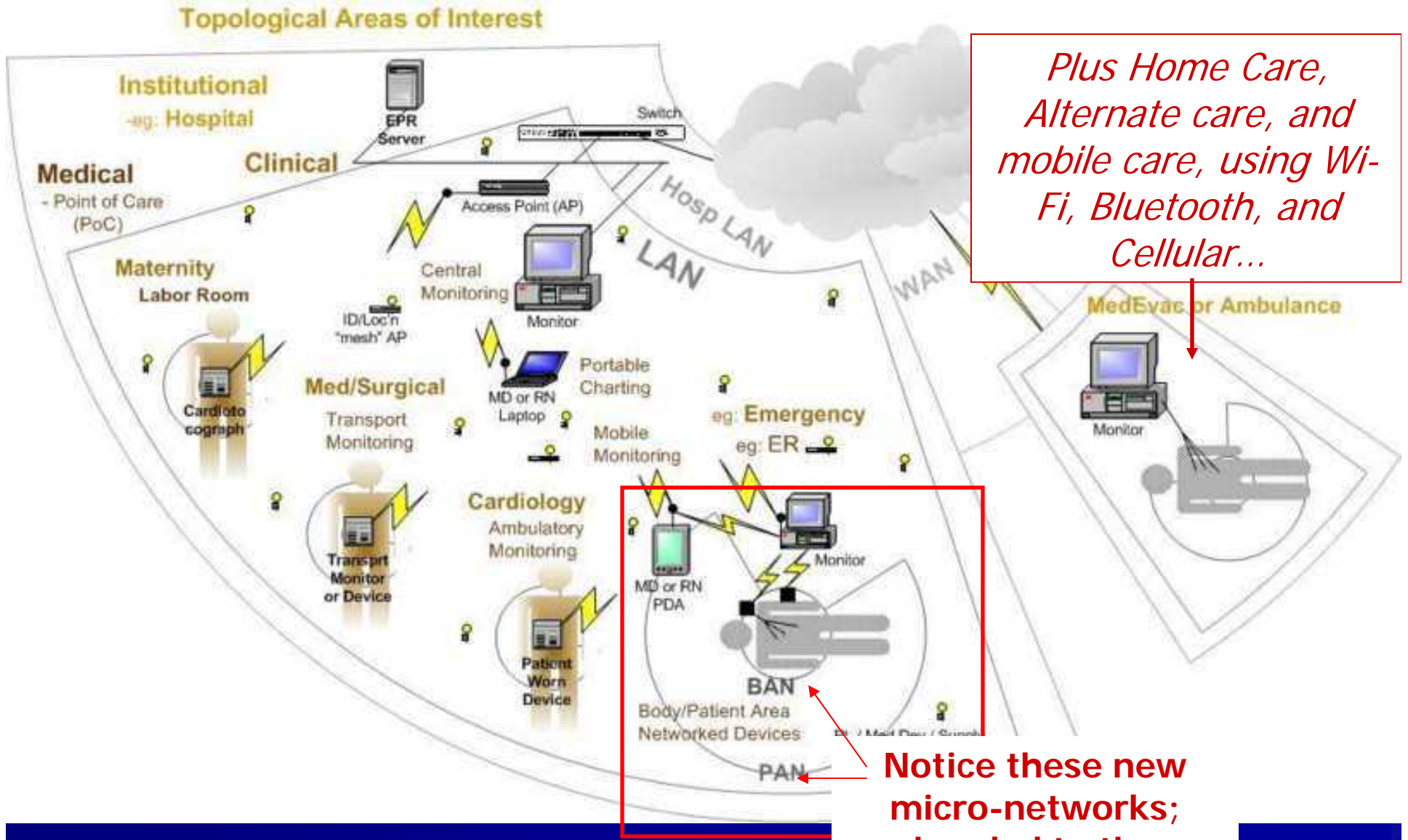
**This is a national priority, being driven by NIST!**

# "High Tech" healthcare wired/wireless environment



Courtesy Jan Wittenber, Philips/IEEE 11073

# "High Tech" healthcare wired/wireless environment



*Plus Home Care, Alternate care, and mobile care, using Wi-Fi, Bluetooth, and Cellular...*

**Notice these new micro-networks; headed to the nano/cellular level!**

# High Tech to HITECH

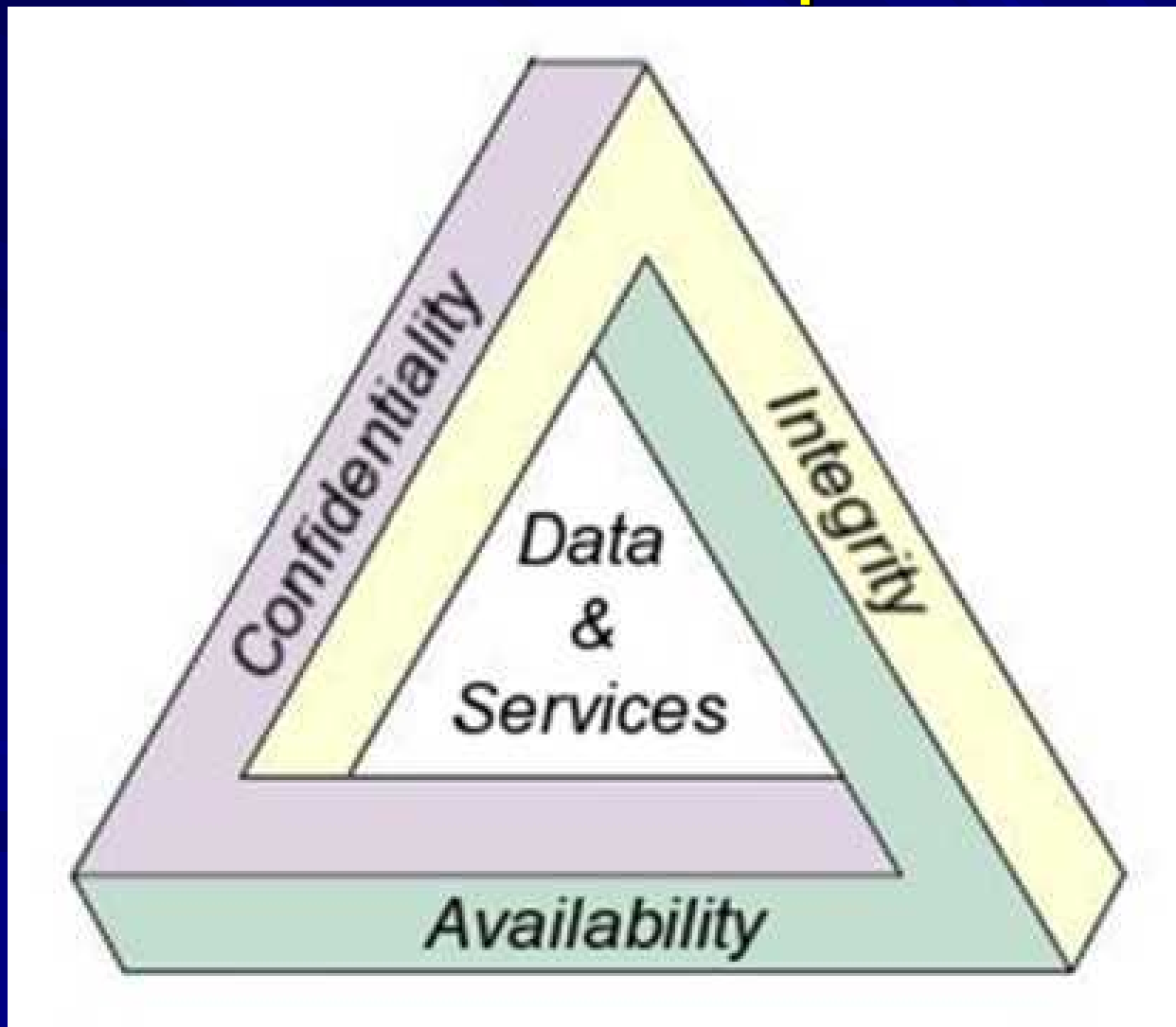
- From the High Tech world to
- **The HITECH world**
- CIAS – the “extended security” world of medical devices
- Review

HIPAA is aging; circa '96, rooted in '94  
**HITECH** is the “Son of HIPAA”



***Health Information Technology  
for Economic and Clinical Health  
Act of January '09***

# This CIA Triad is the Basis of HIPAA 1.0 Compliance



# HIPAA's Final Security Rules, 2003

## “*General Requirements*” for compliance ‘05

“Ensure the *confidentiality, integrity, and availability of all electronic protected health information* the covered entity *creates, receives, maintains, or transmits.*”

- **Integrity** means the property that data or information have not been altered or destroyed in an unauthorized manner
- **Availability** means the property that data or information is accessible and useable upon demand by an authorized person
- **Confidentiality** means the property that data or information is not made available or disclosed to unauthorized persons or processes \*

\* 68 FR 8376  
Feb 20, 2003

# HIPAA's Final Security Rule

## *"Applicability"*

Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this part apply to the following entities:

- (1) A health plan
- (2) A health care clearinghouse
- (3) **A health care provider who transmits any health information in electronic form \***

\* 68 FR 8375  
Feb 20, 2003

# HIPAA's Final Security Rule “*Applicability*”

“A covered entity must comply with the applicable *standards, implementation specifications, and requirements* of this subpart with respect to ***electronic Protected Health Information***” \* ~ a.k.a. ***ePHI***

\* 68 FR 8376  
Feb 20, 2003

# The HITECH Act of 2009

- “Ensuring that new entities that were not contemplated when the Federal privacy rules were written, as well as those entities that do work on behalf of providers and insurers, are subject to the same privacy and security rules as providers and health insurers.”

<http://waysandmeans.house.gov/media/pdf/110/hit2.pdf>

- i.e., EMR/EHR/PHR providers, HIEs and RIOs, data repositories, out-source/off-shore data-entry firms patient registries, home care companies, etc.

# HIPAA's Final Security Rule “Applicability”

## Definition:

*Electronic Protected Health Information (ePHI)* means *individually identifiable health information (IIHI)* ... that is:

- (i) *Transmitted by electronic media;*
- (ii) *Maintained in electronic media \**

\* 68 FR 8374  
Feb 20, 2003

# HITECH “*Applicability*” to medical devices?

*Those devices that might store and/or transmit:*

1. Name,
2. Dates (e.g., birthdate, admission, discharge, death, treatment),
3. Treatment type (s)
4. Medical record or Patient ID No.,
5. Billing Account No.,
6. Device identifiers,
7. Biometric identifiers,
8. Full face (or comparable personalized images such as tattoos) photographic images or videos
9. Prescription ID, and
10. Any other unique identifying number, characteristic or code (e.g., patient bar code, prescription bar code, various RFID tags, etc.)

# HITECH Applicability to

## Device-HCIT combination systems?

*Those systems that store and/or transmit:*

1. Name,
2. Dates (e.g., birthdate, admission, discharge, death, treatment),
3. Treatment type (s)
4. Medical record or Patient ID No.,
5. Billing Account No.,
6. Device identifiers,
7. Biometric identifiers,
8. Full face (or comparable personalized images such as tattoos) photographic images or videos
9. Prescription ID, and
10. Any other unique identifying number, characteristic or code (e.g., patient bar code, prescription bar code, various RFID tags, etc.)



# New, substantial HITECH penalties...

- “Willful neglect” bears the highest penalty: \$50,000 *per violation*, up to \$1.5 million per year, with no maximum total penalty for multiple violations.
- A violation is the disclosure of PHI by any sort of breach.

# New, substantial HITECH disclosure obligations:

- Covered entities must:
  - Provide detailed report of ALL PHI disclosures to any party upon request, and
  - Notify party directly if PHI is disclosed by breach of security.
- These are both new; HIPAA only required tracking/reporting of unusual disclosures, not breaches, and no active breach disclosure was mandated.

## But wait: there's more

- Within 3 years, HITECH requires federal and state regulations that clarify how individuals and state AGs may sue violators to recoup damages caused by PHI breaches!

# The HITECH + High Tech punch?

- Very significant new risk exposures for medical devices and medical device-HCIT systems
  - Our communities will need to work hard and fast to develop good practice standards, guidelines, and audit processes for compliance for devices, networks, and data storage.
  - I am working with HIMSS to reactivate the Medical Device Security Task Force that Steve Grimes and ACCE helped create in 2004 (and you are WELCOME to join!)

# Will HITECH have more “bite” than HIPAA?? You decide....



amednews.com  
— American Medical News —

HOME | LATEST ISSUE | PAST ISSUES | TOPICS | MULTIMEDIA | MOBILE | Published 1

<http://www.ama-assn.org/amednews/2010/02/01/bisc0201.htm>

Government  
Profession  
Business  
Opinion  
Health

## Connecticut sues Health Net over data security breach

The insurer becomes the first plan sued under a new law allowing attorneys general to enforce HIPAA privacy laws.

By EMILY BERRY, amednews staff. Posted Feb. 1, 2010.

PRINT | E-MAIL | RESPOND | REPRINTS | SHARE



Connecticut Attorney General Richard Blumenthal has filed a lawsuit against California-based Health Net, alleging the company violated federal laws protecting medical records when a portable data drive disappeared.

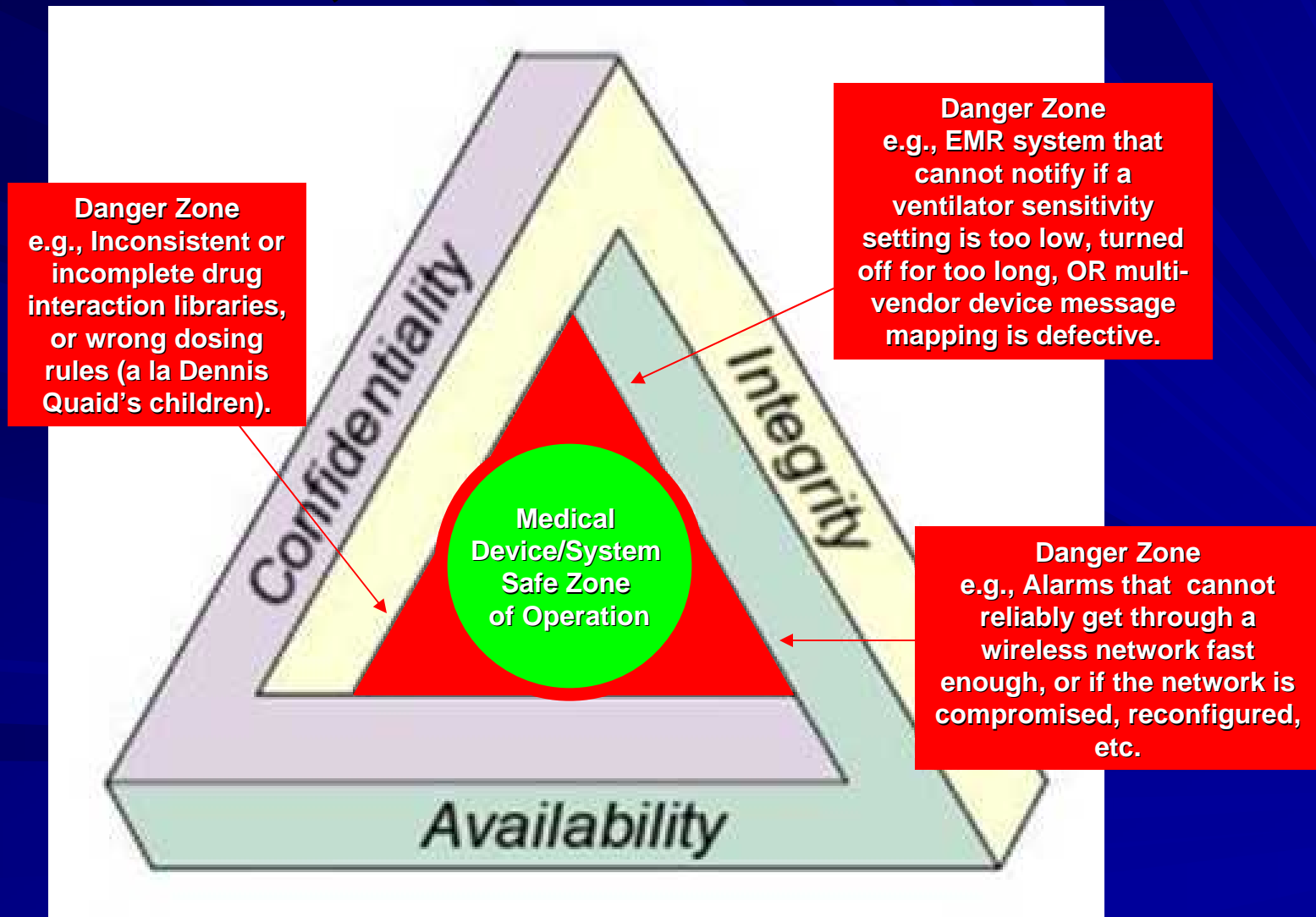
According to Blumenthal's office, the Jan. 13 lawsuit is the first action by an attorney general acting under the Health Information Technology for Economic and Clinical Health, or HITECH Act (part of the 2009 federal stimulus package) to enforce privacy laws under the Health Insurance Portability and Accountability Act.

HEA  
Heal  
desp  
Man;  
insur  
Medi  
to de  
Reac  
inter

# Oh, yes, I mentioned CIAS

- Though not directly related to HITECH, I believe we need to add a very critical element to the historic CIA model:
  - **Confidentiality**
  - **Integrity**
  - **Availability**
  - **Safety**

# This CIA Triad is NOT enough for healthcare; Need SAFETY zones!



# FYI “HIT Patient Safety” is now on ONC and FDA’s radar screen!

February 25, 2010  
HIT Safety Hearing

## Meeting Materials

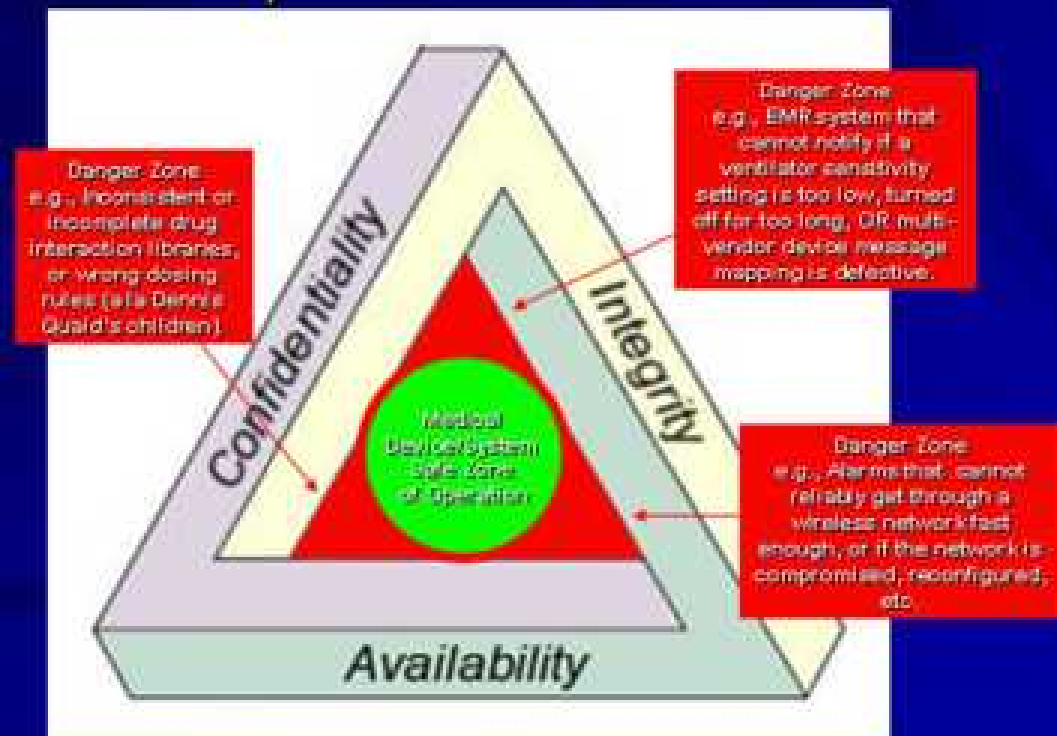
- [Agenda \[PDF - 350 KB\]](#)
- [Questions for Presenters \[PDF - 318 KB\]](#)
- [Biographical Sketches of Presenters \[PDF - 420 KB\]](#)
- Identifying the Issues
  - [Ross Koppel, University of Pennsylvania \[PDF - 487 KB\]](#)
  - [Gil Kupeman, Columbia University \[PDF - 494 KB\]](#)
  - [Alan Morris, Intermountain Healthcare \[PDF - 1.05 MB\]](#)
- Stakeholders
  - [Dave deBronkart, ePatient Dave \[PDF - 679 KB\]](#)
  - [Justin Starren, Marshfield Clinic \[PDF - 434 KB\]](#)
  - [Jeanie Scott, Veterans Health Administration \[PDF - 140 KB\]](#)
  - [Michael Stearns, e-MDs \[PDF - 624 KB\]](#)
  - [Shelley Looby, Cerner \[PDF - 481 KB\]](#)
  - [Carl Dvorak, Epic \[PDF - 444 KB\]](#)
- Possible Approaches
  - [Jeff Shuren, Food and Drug Administration/HHS \[PDF - 273 KB\]](#)
  - [William Mupier, Agency for Healthcare Research & Quality \[PDF - 314 KB\]](#)
  - [James Walker, Geisinger \[PDF - 592 KB\]](#)
  - [Edward Shortliffe, American Medical Informatics Association \[PDF - 145 KB\]](#)

[http://healthit.hhs.gov/portal/server.pt?open=512&objID=1473&&PageID=17117&mode=2&in\\_hi\\_userid=11673&cached=true](http://healthit.hhs.gov/portal/server.pt?open=512&objID=1473&&PageID=17117&mode=2&in_hi_userid=11673&cached=true)

**Consider attending Session 171 on Wed; we have added an FDA speaker!**

# My suspicion: CIAS will become the framework for “HIPAA 2.0”

- Confidentiality
- Integrity
- Availability
- Safety



# Topics

- The High Tech world
- The HITECH world
- CIAS – the “extended security” world of medical devices
- Conclusion

# Conclusions

- What to do, and what's next?

# There's more planning/learning to do.

- The ONC IFR from 30 December 2009 requires robust “electronic destruction of data,” which few systems, devices, or organizations presently use
  - What are your plans for fixed AND mobile devices?
- Your hospital/physician practice MIGHT elect to have your customized EHR system certified “in place”
  - Are your encryption, access audit log, and breach identification/notification systems “NIST-ready?”
- The Drug Enforcement Agency just released a new controlled substances e-Prescribing IFR that requires “2-part strong authentication,” and detailed data logging/auditing/reporting
  - Do you have resources available to support this?

# Additional large questions:

- How will *your* enterprise manage data you acquire from numerous other providers via the Health Information Exchange network?
  - How much will you retain/protect?
- HITECH provides broad consumer rights to their own clinical data, and there is strong interest in providing very granular controls to consumer's data
  - How will you accommodate those requirements if/when embodied in “HIPAA 2.0” later this year?

# Main resource site:

- Type in “HealthIT.hhs.gov” in your browser, where all of the IFRs, NPRMs, grant opportunities etc, are visible for review and download

# Grab, download, and read the FREE information that is online:

- All IHE profiles are free, and can be downloaded at [www.IHE.net](http://www.IHE.net)
- A rich library of interesting IHE-oriented clinical use cases and integration specifications can be downloaded at [www.HITSP.org](http://www.HITSP.org)

*Both sites also have free educational webinars that can be downloaded!*

# Consider joining HIMSS and their local HIMSS Chapters

- HIMSS has web-based resources and webinars for its members to keep everyone up to date
- If you want to take an active role in helping the government sets and enforces HIT policy, join the HIMSS state and/or federal advocacy programs
  - HIMSS'10 Advocacy Summit in DC June 16-17

# **LEAD!**

**We may never have a chance like this  
again...**

**OUR TIME IS NOW.**

**As General George Patton said:**

**“Lead, follow, or get out of the way!”**

**For further information:**

**Elliot B. Sloane, PhD, CCE, FHIMSS**

[www.ebsloane.org](http://www.ebsloane.org)

[ebsloane@drexel.edu](mailto:ebsloane@drexel.edu), and

ebsloane@ any of:

gmail.com, ieee.org, drexel.edu, ebsloane.org,  
yahoo.com, hotmail.com, etc.

or just Google™ me!!

**Thanks for sharing this time with me!**

**The floor is open for Q&A!!!**