

HealthSec

2005 CONFERENCE & EXPO

Session H7 Securing a Public Health Surveillance System



Securing a Public Health Surveillance System

Session H7

John R. McLamb, MSIA

Adjunct Assistant Professor

Director of Informatics

Department of Emergency Medicine

University of North Carolina at Chapel Hill

HIMSS NPR Task Force Chair

Wednesday, Sept. 28

2:00 PM – 3:00 PM

HealthSec
2005 CONFERENCE & EXPO



© 2005 University of North Carolina at Chapel Hill

Key Points

- Regulatory and compliance requirements (HIPAA and PHIN)
- Security Lessons Learned for voluntary participation in a public health system
- Security Architecture
- “Best Practices” for information assurance for a public health and hospital collaboration

Key Points

- Regulatory and compliance requirements (HIPAA and PHIN)
- Security Lessons Learned for voluntary participation in a public health system
- Security Architecture
- “Best Practices” for information assurance for a public health and hospital collaboration

Agenda

- Brief overview of North Carolina's Public Health Surveillance System (NC BEIPS)
- Security Drivers
 - HIPAA
 - State Law & Hospital Issues
 - PHIN
- Security Architecture

What is NC BEIPS?

North Carolina Bioterrorism and Emerging Infection Prevention System

- Early Event Detection using secondary data sources
 - Emergency department data from the North Carolina Emergency Department Database
 - Other data sources in development (pre-hospital, poison center, veterinary laboratory, wildlife)
- Tabular, graphical and map-based results, both aggregate and line listing using in-house web portal and CDC's Early Aberration Reporting System (EARS)
- Automated alerting option

ED Data Collection Background

- 1999-2002: NCEDD in pilot phase
- 2002-2004: Rapid expansion (voluntary participation)
- 2005-Present: Launch of statewide mandate for ED data collection, NCHES (North Carolina Hospital Emergency Surveillance System)
 - NCEDD continues data management and analysis
 - NCHA oversees data collection

How NC BEIPS Began

CDC Funded “Proof of Concept” Project

Objectives:

- Collect and standardized ED Data from disparate and heterogeneous hospital systems
- Transmit data securely via the Internet
- Test value of the data for public health utility
- Provide feedback to the CDC on the DEEDS 1.0 Standard

ED Data Collection Steps

Current NCEDD Process

- Encrypted FTP of select ED data elements from participating hospitals
 - **No additional data entry required**
 - **Receive data in format easiest for hospital to provide**
- Standardize and aggregate the data to CDC's Data Elements for Emergency Department Systems (DEEDS) standard

NCHES process

- Hospitals standardize their own data and follow a standard HL7-based file format
- Submit via HTTPS to data provider
- Data provider aggregates and sends one file to NCEDD every 12 hours

Database Status

As of April 15, 2005, data from 28 hospitals (24 NCEDD/4 NCHESS)

- **4000 visit records per day on average (including both new and updated records)**
- **Total Number of Visits: 1,833,337**
- **Total Number of Patients: 978,270**
- **Total Number of Final Diagnosis Codes: 4,871,691**
- **Total Number of Cause of Injury Codes: 532,916**

Data Elements

- Patient & Visit IDs
- DOB, Sex
- City, County, State, 5-digit ZIP
- Arrival Date/Time
- Chief Complaint and Triage Note (when available)
- Triage Acuity Rating
- Transport Mode to ED
- Insurance Coverage
- ED Facility
- ED Disposition
- BP, Initial ED Temperature
- ICD-9 Final Diagnosis and Injury (E) codes
- Procedure Codes

Data Users

- NC Division of Public Health epidemiologists
- Hospital-based public health epidemiologists (PHEs)
 - **In-hospital liaison to local health departments in NC's 11 largest hospitals**
 - **Perform in-hospital surveillance for community-acquired infections and for defined syndromes which may be indicative of a terrorist attack**
- Public Health Regional Surveillance Team (PHRST) members

NCEDD Web Portal & EARS

- 24/7/365 SSL access
- Updates every morning
- Functionality offering report customization
- Role-based access

Security Drivers

- Budget
- HIPAA
- Hospital Participation Politics
- State Legislation
- PHIN

Security Driver: Budget

How does NCEDD move from “pilot” to “production” and provide IT security best practices with limited budget and human resources?

Major Problems Faced:

- Inadequate physical security
- Inadequate Network Security
- No staff skills in IT Security and no budget to hire someone

Problems resolved:

- Contracted with a party data center
- Contracted for a managed firewall
- Hired a security consultant to help technical team with security issues

Security Driver: HIPAA and Public Health

“Without individual authorization, a covered entity may disclose PHI to a public health authority that is legally authorized to collect or receive the information for the purposes of preventing or controlling disease, injury, or disability”

45 CFR § 164.512(b)

Security Driver: HIPAA and Public Health

De-identified data (e.g., aggregate statistical data or data stripped of individual identifiers) require no individual privacy protections and are not covered by the Privacy Rule.

45 CFR § 164.512(b)

Security Driver: HIPAA and Public Health

De-identifying can be conducted through

- statistical de-identification — a properly qualified statistician using accepted analytic techniques concludes the risk is substantially limited that the information might be used, alone or in combination with other reasonably available information, to identify the subject of the information
- safe-harbor method — de-identifies information by removing 18 identifiers and the covered entity does not have actual knowledge that the remaining information can be used alone or in combination with other data to identify the subject (see next slide)

18 Individual Identifiers

- names;
- all geographic subdivisions smaller than a state, including county, city, street address, precinct, zip code,*and their equivalent geocodes;
- all elements of dates (except year) directly related to an individual; all ages >89 and all elements of dates(including year) indicative of such age (except for an aggregate into a single category of age >90);
- telephone numbers;
- fax numbers;
- electronic mail addresses;
- Social Security numbers;
- medical record numbers;
- health-plan beneficiary numbers;
- account numbers;
- certificate and license numbers;
- vehicle identifiers and serial numbers, including license plate numbers;
- medical device identifiers and serial numbers;
- Internet universal resource locators (URLs);
- Internet protocol (IP) addresses;
- biometric identifiers including fingerprints and voice prints;
- full-face photographic images and any comparable images; and
- any other unique identifying number, characteristic, or code, except that covered identities may, under certain circumstances, assign a code or other means of record identification that allows de-identified information to be re-identified.

HIPAA PRIVACY and DISCLOSURES IN EMERGENCY SITUATIONS

- Providers and health plans covered by the HIPAA Privacy Rule can share patient information in all the following ways:
 - Treatment
 - Notification
 - Imminent Danger
 - Facility Directory

HIPAA PRIVACY and DISCLOSURES IN EMERGENCY SITUATIONS

TREATMENT

Health care providers can share patient information as necessary to provide treatment.

Treatment includes

- sharing information with other providers (including hospitals and clinics),
- referring patients for treatment (including linking patients with available providers in areas where the patients have relocated), and coordinating patient care with others (such as emergency relief workers or others that can help in finding patients appropriate health services).
- Providers can also share patient information to the extent necessary to seek payment for these health care services.

HIPAA PRIVACY and DISCLOSURES IN EMERGENCY SITUATIONS

NOTIFICATION

Health care providers can share patient information as necessary to identify, locate and notify family members, guardians, or anyone else responsible the individual's care of the individual's location, general condition, or death.

HIPAA PRIVACY and DISCLOSURES IN EMERGENCY SITUATIONS

IMMINENT DANGER

Providers can share patient information with anyone as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public -- consistent with applicable law and the provider's standards of ethical conduct.

HIPAA PRIVACY and DISCLOSURES IN EMERGENCY SITUATIONS

FACILITY DIRECTORY

Health care facilities maintaining a directory of patients can tell people who call or ask about individuals whether the individual is at the facility, their location in the facility, and general condition.

Great Resource for HIPAA and Public Health

HIPAA Privacy Rule and Public Health:
Guidance from CDC and the U.S.
Department of Health and Human Services
<http://www.cdc.gov/mmwr>

Security Drivers

Lesson Learned

Even though initially NCEDD was collecting a limited data set with no PHI and thus not covered by HIPAA, a business decision was made to comply with the proposed Security Rule.

Security Drivers

Why comply with HIPAA Security even though ePHI was not collected?

- To reduce concerns from CIOs & CSOs for increase voluntary participation
- Future NCEDD versions could collect PHI thus the need for an enabling security architecture

Key Lesson Learned

*The NCEDD Data Use Agreement
with Hospitals-*

An important aspect for security and thus participation (both voluntary and mandated)

NCEDD Data Use Agreement

Developed By:

- Hospital Attorneys, Public Health Attorneys
- CISO
- NCHICA- North Carolina Health Information and Communication Alliance (example RHIO)

NCEDD Data Use Agreement

- Right to collect and use all PHI provided to it by the Hospital for the research, public health or health care operations purposes.
- The software will convert the patient identifier and visit identifier to unique recipient identifiers.
- The software will also encrypt the data file.
- The Hospital retains ownership of all raw data processed by this software.
- The conversion of identifiers will happen before the collection of data elements leaves the Hospital's network.
- Only the limited data set will leave the hospital's network and be received by the recipient.

NCEDD Data Use Agreement

- Division of Public Health may use the limited data set for public health surveillance and investigation.
- Data which specifically identifies the hospital will be accessible only by that hospital and/or its designees. Hospitals may use their data as allowed under HIPAA.
- Covered entities will view only their data and data aggregated from all hospital participants.
- Individual hospitals will not be identifiable within the aggregate data.
- The hospital may not attempt to re-identify an individual or another hospital through use of the data.
- The recipient requires Internal Review Board (IRB) approval or waiver for any research projects using the data.

Security Drivers

State Legislation: §130A-480. Emergency department data reporting

- Hospitals shall submit electronically available emergency department data as specified by rule by the Commission
- Public Health shall collect a limited data set (5 digit zip code)
- The State Health Director may share data with local health departments – no commercial use
- A person is immune from liability for actions arising from the required submission of data under

Security Drivers

PHIN

- The Public Health Information Network (PHIN) is CDC's vision for advancing fully capable and interoperable information systems in the many organizations that participate in public health.
- PHIN is a national initiative to implement a multi-organizational business and technical architecture for public health information systems.

Security Drivers

**Public Health Information Network
Functions and Specifications
Version 1.2 – December 18, 2002**

<http://www.cdc.gov/phn/>

Security Drivers

Functional Specification #9 IT Security and Critical Infrastructure Protection

To ensure that sensitive or critical electronic information and systems are not lost, destroyed, misappropriated or corrupted

PHIN

Functional Specification #9

- Client and server X.509 digital certificates or comparable strong authentication methodology should be required for access to sensitive or critical resources from the Internet.
- Role-based, mandatory access control protocols, as well as realistic and effective policies for use and administration of information technology resources, should be established.

PHIN

Functional Specification #9

- Security patches and configuration corrections should be applied promptly.
- Desktop and server based virus scanning, intrusion detection, network vulnerability analysis including port scanning; security policy monitoring, regular penetration testing and active threat intelligence should be employed.
- Continuity of operations planning and procedure implementation should incorporate man-made and natural catastrophic event management.

PHIN

Functional Specification #9

- Security policies will be implemented with authentication based on industry standard X.509 certificates, secure tokens, and other applicable means as identified.
- Access and control of data via selective integrated repository authorization.
- An encryption engine and appropriate use of encrypted data; and access control through a firewall by data routing to programs and other organizations.

PHIN

Functional Specification #9

- External verification of security and continuity processes and technology for public health agencies that support critical information systems should occur on at least a yearly basis. Independent validation and verification should include disaster simulations and intrusion detection.

Security Architecture

Security Approach*

Step 1: Understand the rules
(HIPAA, PHIN, State Laws)

Step 2: Assign Responsibility

Step 3: Develop a Plan

Step 4: Conduct a Risk Analysis

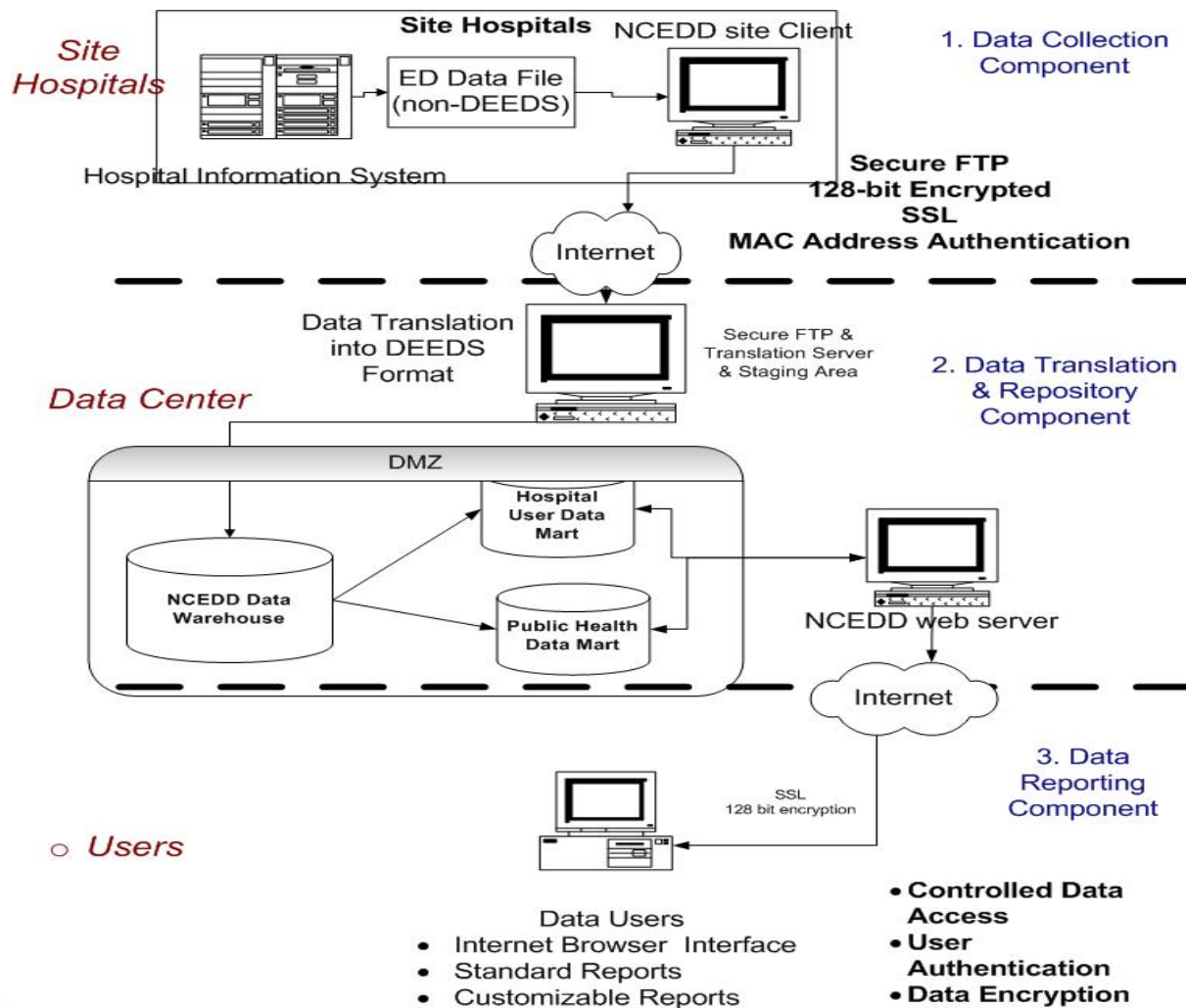
Step 5: Develop Security
Policies

Step 6: Implement
administrative, Physical, and
Technical Controls

Step 7: Develop and deliver
Security Training and
awareness

Step 8: Develop Ongoing
Security Monitoring Process

Architecture



Security Architecture

Security Attribute	Data Sources to Server	Delivery of NCEDD Web reports
Encryption: A method of scrambling information while it moves from one source to another to prevent others from viewing the contents.	Yes	Yes
Secure Transaction: A transaction that is protected from outside tampering.	Yes	Yes
Workstation authentication: A method of positively identifying a specific workstation.	Yes	No
User authentication: A method of positively identifying a specific User of the system.	No	Yes, Two-factor planned for future enhancement

Role-based User Access

	Hospital-based PHEs	DPH	Local / Regional
User Types			
Manager	NCEDD Data Hospital Network Data All hospitals within network	NCEDD Data All PHRST region data All individual county data	NCEDD Data PHRST Region Data All individual counties from assigned PHRST region
Group Only	NCEDD Data Hospital Network Data	N/A	NCEDD Data Data from assigned PHRST region
Single Site Only	NCEDD Data Hospital Data	N/A	NCEDD Data Data from assigned county

Summary

- Good security is essential for voluntary hospital participation
- Privacy and Security are inextricably linked
- Do not collect patient identifiable information unless absolutely necessary
- Research and plan user access roles and controls thoroughly
- Include HIPAA & PHIN standards, State Laws, and hospital concerns in security planning
- Follow industry standards & best practices for detailed security implementation (NIST, ISO 17799, COBIT, etc.)

Acknowledgements

- Patrick Alston – Systems Analyst/Programmer
- Clifton Barnett – Database Analyst/Programmer
- John Crouch – EMT-P Student Assistant
- Terri Eubanks – Project Director
- Dennis Falls - ETL Specialist/Data Base Administrator
- Dr. Stephanie Haas – Vocabulary Development Specialist
- Amy Ising – Technical Team Director
- Jennifer Kerwick – Office Manager/Administrative Asst.
- Aaron Kipp – Graduate Research Assistant (Epi)
- Meichun Li - Reports Specialist/ Programmer
- Dr. Matt Scholer - Clinical Information Specialist
- Dr. Debbie Travers - Text Processing Specialist
- Lorraine Waguespack – Graduate Research Assistant (Clinical)
- Dr. Anna Waller – Principal Investigator

Thank you!

QUESTIONS?

John R. McLamb, MSIA, PHDM
Adjunct Assistant Professor
Director of Informatics
Department of Emergency Medicine
University of North Carolina at Chapel Hill
Neuroscience Hospital, CB# 7594
Chapel Hill, NC 27599
919-843-0523
jmclamb@med.unc.edu