



Considerations for Storing Data in Regulated Healthcare Environments

Grace Wiechman, CISSP

Guidant Corporation

Grace.Wiechman@guidant.com

- **Healthcare Data Storage Needs**
- **The Regulatory Landscape**
- **Who Needs the Data?**
- **Security Requirements**



Economic Framework

•2002

- 1/7th of the economy
- \$2.4 Trillion
- 13.2% GDP
- Hospital spending – 27.1%
- Physician spending - 16.5%

•2011

- 17% GDP expected
- \$9,216 per person, twice per capita of 2000
- Expected to swell at rate exceeding overall economic growth



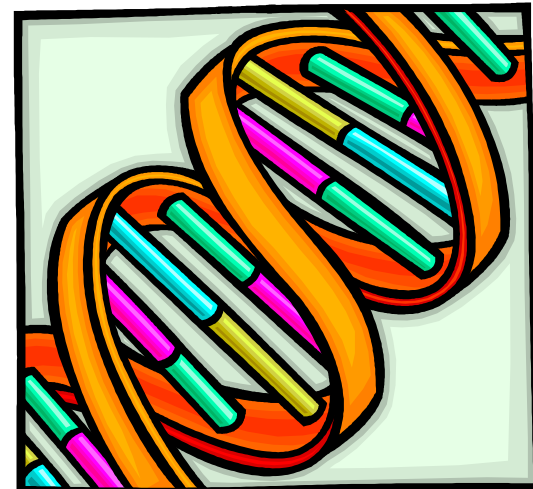
Patient Data Economic Framework

- **Patients – 43.6 million uninsured (1 in 6)**
- **Ageing population (1/3 born 46-61) 100 million**
- **Oldest boomers are 43-58 in 2004**
- **Sweet spot for needing medical attention**
- **90% of healthcare needs are just starting**
- **10% used up to age 50 (not including pregnancy)**

Big need for intelligent storage



- **Patient safety driving many innovations**
- **Patients may have multiple caregivers**
 - No unique way to identify patient
 - Insurance, or lack thereof determines healthcare



IT Factors in Health Care Delivery

- Many hospitals and clinics still use paper
- Conflict for infrastructure resources
- Some places healthcare is 10 years behind other industries
 - Methodology
 - Process
 - Equipment
 - Infrastructure



Not enough physicians

Need increased efficiencies

Cost of healthcare



- **Privacy Requirements**
- **Security Requirements**
- **Regulatory Requirements**

FDA Regulations

- 21 CFR 11 – Electronic Signatures
- 21 CFR (lots of others)

Department of Health & Human Services

- Health Insurance Portability and Accountability Act of 1996 – Administrative Simplification (**HIPAA**)
 - Privacy
 - Electronic Transactions and Code sets
 - Security
 - Identifiers

Proposed Health Care Quality Modernization, Cost Reduction and Quality Improvement Act (Kennedy)

- **Canada – Personal Information and Electronic Documents Act (PIPEDA)**
- **European Union – Data Handling Requirements**
 - Purposes limitations
 - Data quality
 - Data transfers
 - Special protection for sensitive data
 - Data controllers
 - Individual redress

- **Lots of storage**
 - Electronic patient records
 - Pervasive monitoring
- **Ability to retrieve data off archives**
 - 6 – 21+ years retention
- **Security**
- **Large increase of data as new data is added to electronic medical record**
- **Real-time or near real-time data**



Claims, payment, eligibility (X12, NCPDP transactions)

Electronic medical record

- Office Visit (Encounters)
- Lab results
- Referrals
- Medication history
- Implantable device data
- Radiology
- Business office data



Moving towards unique identifiers

- Healthcare providers
- Health plans

Who Needs The Data?

Patients

Hospitals and Clinics (health care providers)

Insurance companies

Disease state management companies

Device & biotech companies

Public health agencies

Researchers



- HIPAA gives patients access to medical records
- Some patients with complicated conditions coordinate medical records between caregivers
 - Most record transfers between healthcare providers are paper
 - Most patients do not understand how medical data will be used outside of treatment
 - Some patients have additional privacy/security requirements
 - Need healthcare



Hospitals and Clinics (health care providers)

- **Provide treatment**
- **Internal quality controls**
- **Regulatory and credentialing reporting**
- **Education**
- **Physicians may practice at multiple facilities**
 - How do you keep track of all patients a healthcare provider sees?
 - How do you know when the patient leaves?
- **Health insurance may dictate where care is provided**

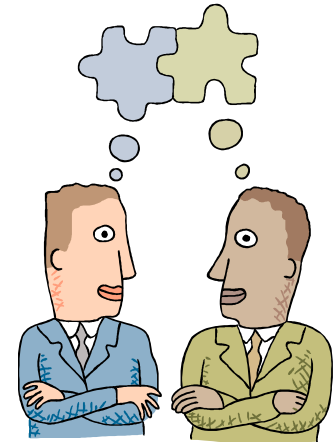
- **Need to pay claims**
- **Need to measure quality of health care service**
- **Care management**
- **Disease state management**
- **Fraud and abuse**
- **Employers determine healthcare coverage**
- **Tracking customers that change employers**
- **May need to keep claims data 21+ years**



- **Reporting disease or injury**
- **Epidemics**
- **Track emerging healthcare trends**
- **Monitor quality of healthcare**
- **Tracking FDA regulated products, post market surveillance, reporting adverse events**



- **Activities designed to develop or contribute to generalizable knowledge :**
 - development,
 - testing
 - evaluation
- **Longitudinal data**
- **Pre-clinical trial data**
- **Large databases collected over long periods of time**
- **De-identified data**



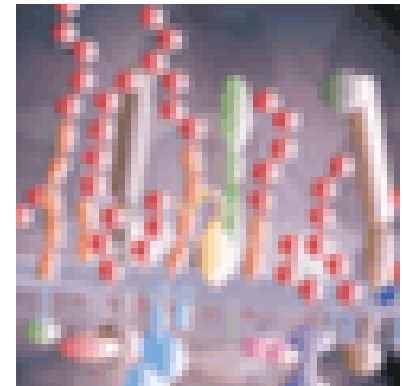
- **Specialty Disease Management**
- **Insurance Companies**

Integrated view of patient treatment

- Office visits
- Medications
- Lab tests
- Access to treatment
- Intervention



- **Pre-clinical trial research**
- **Clinical trial data**
 - Conducting clinical trials
 - Submissions for regulatory approval
- **Post market release data**
- **Integration with other disease information**
- **Human Genome**
- **Tracking patients and devices for FDA requirements**



Lot of requirements on healthcare systems

Not only for privacy and security

- Volume
- Standards
- Needed 24x7
- Long term storage

Government requiring electronic data

Digital signatures

- Clinical trials
- Materials tracking
- Code releases
- Data integrity in storage

- **Patient data may be represented in hundreds of systems within the hospital**
- **Aside from copying them from one system to another, is there a way to intelligently store that data?**
- **How do we make certain that the two John Does don't get their medical information mixed?**
- **How do we restrict information that needs to be protected?**
- **What happens when the patient leaves one healthcare system for another?**

**Big hospitals, big servers, centralized services,
medium-low technical expertise**

**Slow adopters of new IT technology (patient
treatment technology rules)**

Physicians participate in technology decisions

Hundreds of vendors within one setting

Health Information Management Vendors Electronic Medical Records

McKesson



GE-Medical



Epic Systems



Cerner



IDX



Eclipsys Corp



HP

Tandem

IBM –mainframes & Unix servers

Sun

Windows based machines

Linux

- **Fast**
- **Cheap**
- **Secure**
- **Reliable**
- **Easy to Use**

- **Protect Data Confidentiality, Integrity and Availability**
 - **in transit and at rest**
- **Design Security From The Start**
- **Consider digital signing for critical structures**

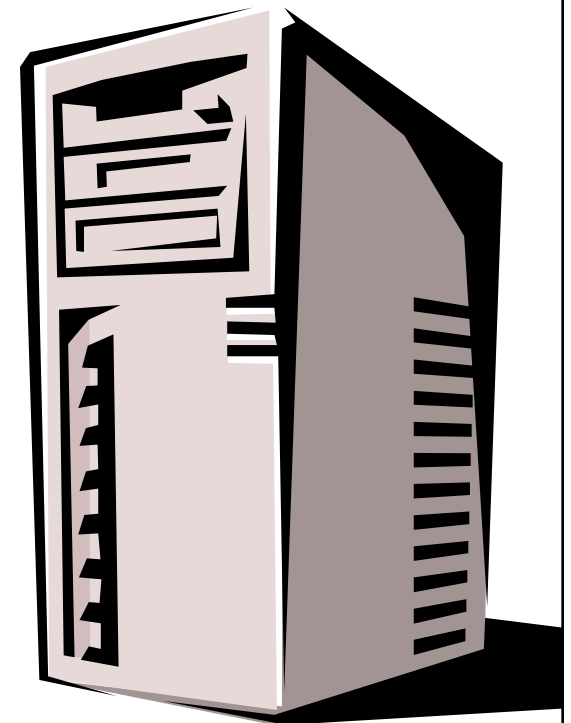
Audit logs - HIPAA

(b) *Standard: Audit controls.*

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

Translation: storage

- How much to store
- How long to store
- Pattern recognition



- **Product Design**
 - Easy to understand security models
 - Properly configured out of the box
 - Fast
 - Recoverable
- **Many healthcare providers are on a steep learning curve for security**

- **Healthcare will be a growth industry for data storage**
- **Need intelligent designs to help manage data from disparate sources**
- **Amount of data will be increasing**
- **Build secure, fast, easy to use structures**



Securing Stored Data in a Regulated Environment

Grace Wiechman, CISSP

Guidant Corporation

Grace.Wiechman@guidant.com