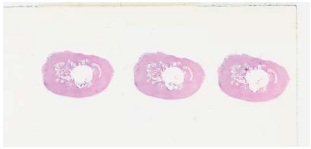

# Security Use Cases

*Joyce Peng & Brian Gilman*

# Use Case I

- Two organizations form a collaboration where researchers are given access to proprietary databases

  (e.g. histopathology databases).



- Researchers are given access to only a subset of the data.
- There is often a need to disallow access to certain data (name, SSN, etc) but allow access to other information (phenotype, affected status, etc).

# Use Case II

- A database of phenotype/genotype and drug sensitivity data has been made available to an international group of researchers collaborating over the Internet.
- Patients are asked to fill in diagnostic forms on the website. Patients are not allowed to modify their answers. Full confidentiality of the patients' contact information is required by law.
- Doctors are only allowed to see the inputs from a subset of patients whom they have been assigned to.

# Common Requirements

- FDA requirements enforce digital signature of documents, experiments, and samples
- Must ensure identity and authority in computer systems
- Must provide facility to disallow access to subsets of data
- Often set up a hierarchy of role based query and access control
- Must provide means to disallow identification of patient based on analytical results and samples taken from patient

# Why Security is Critical in Life Sciences?

- **Enable Collaboration**
- **Protect Intellectual Property**
- **Comply with Regulatory Requirements**
  - 66% of health care providers' top priority would be upgrading security on IT systems to meet **HIPAA** requirements – *HIPAA survey*
  - Y2K is 20%-25% in scale compared to the **21 CFR Part 11** challenge – *IDC*
  - The industry-wide cost of **Part 11** compliance would reach $2 billion by 2006 - *The Pharmaceutical Research and Manufacturers of America*
- **Reduce Financial Risks**

# Protect Intellectual Property

- **First to Invent Rule**
  - One page of electronic experiment data could cost millions in an IP lawsuit.
- **Maintain the integrity of the legally-defensible records for a long period of time**
  - Time stamp
  - Write once
  - Signed by the researcher and the witness

# 21 CFR Part 11

- **Part 11 establishes the criteria under which the FDA considers electronic records and electronic signatures *"to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures."***

- **FDA's Stance on Part 11**
  - **Primary concern: ensuring public health and safety**
  - **Risk-based compliance**
  - **$500 million fine paid for plant violations by large pharmaceutical**
  - **FDA now has a softer perspective on enforcement.**

# 21 CFR Part 11

- **Technical Requirements**
  - **Strong Security** - to ensure the authenticity, integrity, and confidentiality of electronic records.
    - **Unique user name/password**
    - **Limit system access to authorized individuals**
    - **Detect and report unauthorized use**
    - **Use of document encryption and digital signature standards**
  - **Audit Trail**
  - **System Availability**
  - **Operational System Checks**
  - **Electronic Signatures** – to ensure that the signer cannot readily repudiate he signed record.

# HIPAA

- **Health Insurance Portability and Accountability Act**
- **Administrative Simplification Act**
  - **Privacy Rule:** "what" individual health information must be protected
  - **Security Rule:** "how" organizations need to protect health-related information
- **Noncompliance would put you in jail.**
- **75% Polices/Procedures, 25% Technology**

# HIPAA Security Requirements

- **"Ensure the confidentiality, integrity, and availability of all electronic protected health information."**
- **Technical Safeguards**
  - **Access Control**
    - **Unique user identification**
    - **Emergency access procedure**
    - **Automatic logoff**
    - **Encryption and decryption**
  - **Audit**
  - **Integrity**
  - **Authentication**
  - **Transmission Security**
    - **Integrity Control**
    - **Encryption**