HIPAA Privacy
Developing Meaningful Minimum Necessary Standards

Kevin Lawlor, JD
Joseph Hales, PhD
Intermountain Health Care
Salt Lake City, UT
June 5, 2003
Outline

- Background – IHC
- Background – Access control
- Motivation
- Access control framework
- Implications
- Discussion
IHC Geography

- 22 hospitals
- 400 employed MDs
- Health plan
- 117,871 admissions
- 4,895,384 outpatient visits
- ~$2Billion budget

June 5, 2003

Developing Meaningful Minimum Necessary Standards
Intermountain Health Care (IHC)

- Founded in 1975
- #1 Integrated Health Care System
- Top 100 Most Wired
IHC Information Security

- Information Systems
- Information Security Committee
- Clinical Programs Leadership Team
- Corporate Compliance
IHC Information Systems

- 30+ years of experience
- Internally developed mainframe system (HELP)
- Internally developed fat client system (Clinical Workstation)
- Internally developed Web-based system (Results Review)
IHC IS (continued)

Developing Meaningful Minimum Necessary Standards

HELP

Ancillary IDX PACS

eGate

Services

CDR

Internet

4.8M records
Motivations for Access Control

- Emergence of the longitudinal record (Clinical Data Repository or CDR)
- Moving beyond IHC-employed users
- HIPAA
Longitudinal Record Tears Down Walls and Fences

Medical record
- Facility-based
- Paper
- Access only from facility

Longitudinal record
- Enterprise-based
- Electronic
- Access anywhere

June 5, 2003

Developing Meaningful Minimum Necessary Standards
Loss of Walls and Fences Creates Issues

- Greater risk of inappropriate access
- More complex decisions to make
- More complex decision making process
Exposure

- Access to 4.8 million patient records
- Individual records
  - IHC executives
  - High profile patients
- Affiliated physicians and practices
Reduce Exposure

Access Control Criteria
(aka HIPAA Minimum Necessary)

4,800,000 records

500 records
HIPAA Minimum Necessary Standard for Uses

- Classes of persons
- Categories of information
- Conditions appropriate to access
First Pass (one of them . . .)

### Categories of PHI

<table>
<thead>
<tr>
<th>Problems</th>
<th>Labs</th>
<th>History</th>
<th>Progress Notes IP</th>
<th>Progress Notes OP</th>
<th>Sensitive Materials (e.g. HIV)</th>
<th>Etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physicians</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Floor Nurse</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coders</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rad Tech</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Etc.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Classes of Persons

- **P** = PCP
- **C** = Other physician, actively treating patient
- **A** = Patient in facility, terminal in facility
- **L** = Patient on unit, terminal on unit

### Conditions Appropriate to Access

- **P** = PCP
- **C** = Other physician, actively treating patient
- **A** = Patient in facility, terminal in facility
- **L** = Patient on unit, terminal on unit

June 5, 2003

Developing Meaningful Minimum Necessary Standards
Classes of Persons

- Employed Physician
- Hospital Administrator
- Affiliated Physician
- On Floor Nurse
- ER Nurse
- Clinic Nurse
- Pharmacist
- Physical Therapist
- Respiratory Therapist
- Dietician
- Home Health Nurse
- Medical Assistant
- Clinic Clerk
- Hospital Registration Clerk
- Health Plans Clerks
- Radiology Technicians
- Instacare Nurse
- Instacare Clerk
- IS Clinical Systems Developer
- IS Infrastructure Support DBA
- IS Infrastructure Support Network
- Graduate Students
- IS Interfaces, Vocabulary Mappers
- Lab Technicians
- Ward Clerks
- Pulmonary Function Technicians
- Other Departmental: Blood Bank
- Orderlies
- Phlebotomists
- Occupational Therapist
Categories of Information

- Problems
- Meds In/Out
- Labs
- History
- Discharge Summary
- Rad Card
- Nurse
- Respiratory Therapy
- Physical Therapy
- Occupational Therapy
- Psych Notes
- Phone Notes

- Progress Notes I/P
- Progress Notes O/P
- Microbiology (last 6 mos)
- Microbiology (not time limited)
- Drug Levels
- OB Notes
- Sensitive Material (HIV, Serum Illicit Drugs)
- Cardiology
- Census
- Allergies

June 5, 2003

Developing Meaningful Minimum Necessary Standards
Conditions Appropriate to Access

**Conditions**
- **P = PCP**
- **C = Other physicians/care providers, actively treating patient**
- **A = Patient in facility, terminal in facility**
- **L = Patient on unit, terminal on unit**

**Intended to limit access based upon:**
- Treatment relationship to patient
- Physical proximity to patient
- Relationship between time of access and time that patient was last treated
Break the Glass ("BTG")

- Allows person to access information not otherwise permitted by access control
- Access logged
- In some cases PCP or Compliance Department notified
Issues with “First Pass”

- Too granular
- Never addressed complex decision making process
- Did not address operational issues:
  - Ease of use
  - Reviewing instances of BTG
  - Assigning roles
- Fundamentally was not achieving goal of reducing exposure
Fundamental Goal: Reduce Exposure

Access Control Criteria
(aka HIPAA Minimum Necessary)

4,800,000 records

500 records
“Second Pass”: Process

- Focus Group
  - Framework
  - Use cases

- Feedback Sessions
  - Ad hoc sessions
  - Organizational presentations

- Requirements Specification
Focus Group Participants

- CIO  Corporate VP
- Chief Medical Informatics Officer
- Dir. IT Architecture
- Corporate Legal Counsel
- Corporate Health Information
- Project Management
- Regional IS Directors
- Corporate IT Security
- Programming Lead
- Implementation Lead
Guiding Principles

Create tools/processes to manage IHC’s IT Security and Access Control processes

1. One standard enterprise-wide approach (technology & process)
2. Provide security & appropriate access as perceived by management, users, patients
   a. Require unique authentication credentials for every user
   b. Enable access when legitimate “need to know”
   c. Provide for “urgent” verification & access
   d. Provide extra protections for certain classes of data
Guiding Principles (continued)

3. Easy to use and manage
   a. Simple/logical (roles, process, technology)
   b. Manage at the level where the pertinent information is known

4. Compliant with IHC’s policies
Tensions

- Difficult process $\rightarrow$ password sharing
- Limit access $\leftrightarrow$ patient safety
- Limit access $\leftrightarrow$ customer service
- BTG $\leftrightarrow$ patient to provider relationships
Somewhere Between Principles and Design

- Corporate policy
- Technical infrastructure
- Execution of rules in applications
Functional Design

- **Role**
- **Where:** User Location
- **Who:** Patient Access
- **What:** Data Access
User Location Criteria

*Where the user can see*

- User role
- User location
Patient Access Criteria

**Who the user can see**

- User role
- User location
- User home base
- Patient activity (time and location)
- Patient to provider
- Provider to provider
Data Access Criteria

*What part of the record the user can see*

- User role
- Patient activity (time)
- Class of data
Home Base

- Specifies permitted range of operation
- Multiple home bases permitted
- Hierarchical structure
  - Enterprise
  - Region
  - Facility
  - Department/Service
Patient-to-Provider Relationship

- Patient Registry
  - My Patient List
  - Scheduled visit/procedure
  - Orders
  - Documented care
  - Break the Glass
- Referral
Provider-to-Provider Relationship

Patient Registry “once removed”
- Partners/Practice
- Service
- Employer/Employee relationship
- Consulting/Referral pattern
Enhanced Break the Glass (BTG)

- Define work processes which require BTG
- Define processes for verifying requests
- Separate processes
  - Associate patient and provider
  - Access patient data
- Add time component
  - Expired relationships
  - Expand window of available data
Some Things Never Change

- Two-level access security
- Physical network security
- Logging of CDR access
- Auditing
Role Assessment

Campus (Hospital)
- MD/mid-level
- Ancillary staff
- Staff RN
- Registration clerk
- Billing clerk

Non-campus (Clinic)
- MD/mid-level
- Clinicians
- Registration clerk
- Billing clerk
Use Case: Billing Clerk (non-campus)

User Location
- *Access system only in the workplace*

Patient Access
- *Access only patients with activity at or relationship with a provider at the facility*

Data Access
- *Access only “recent” data*
Use Case: Billing Clerk (campus)

User Location
- *Access system only in the workplace*

Patient Access
- *Access only patients with activity at the facility*

Data Access
- *Access only “recent” data*
Use Case: Registration Clerk
(campus and non-campus)

User Location

- Access system only in the workplace

Patient Access

- Access all patients

Data Access

- Access only EMMI data
Use Case: Clinicians (non-campus)

User Location
- *Access system only in the workplace*

Patient Access
- *Access only patients with activity at or relationship with the user or a provider at the facility*

Data Access
- *Access only “recent” data with BTG by time*
Use Case: Ancillary Staff (campus)

User Location

- Access system only in the workplace

Patient Access

- Access only patients with activity at or relationship with the user or a provider at the facility

Data Access

- Access only “recent” data by class appropriate to role with BTG by time

June 5, 2003

Developing Meaningful Minimum Necessary Standards
Use Case: Staff RN (campus)

User Location

- *Access system only in the workplace*

Patient Access

- *Access only patients with activity at or relationship with the user or a provider at the facility*

Data Access

- *Access all longitudinal data and only “recent” encounter data with BTG by time*
Use Case: MD/mid-level (campus and non-campus)

User Location

- Access system anywhere

Patient Access

- Access only patients with activity at facilities or relationship with the user or a provider at the facility

Data Access

- Access all longitudinal data except special classifications (e.g., substance abuse treatment)
Implementation of Process

- IT Services Agreement
  - Access and Confidentiality Agreement
  - Business Associate Agreement
  - Cross-indemnification
Implementation of Process (continued)

- **Data Security Administrator**
  - Local trusted user
  - Knowledgeable of organization
  - Regular accountability
  - Limited tools
Issues

1. Home base
2. Sensitive data
3. Patient activity
4. Temporary user access
5. User location
6. Session management
7. Auditing
Issues (continued)

8. IT access
9. Disneyland technology
10. Patient-Provider and Provider-Provider architecture
11. Users with multiple roles
12. Mapping roles to access rules
13. Health Plans special requirements
14. Restrict application modules by user roles