Using Intranet Web Applications to Meet Security Needs

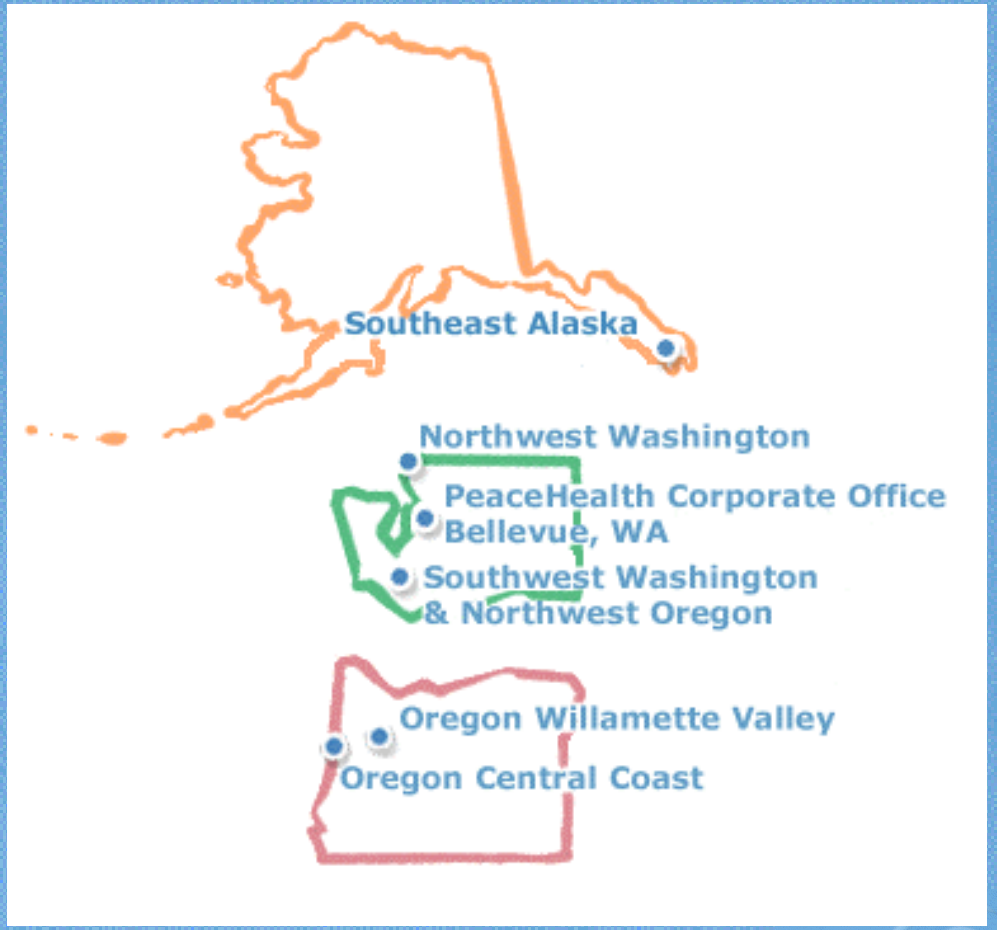
Kevin Johnston, RN
Regional Coordinator for Privacy & Security
PeaceHealth, Eugene, Oregon

Two Sections:

- Implementing an Online System for Executing and Renewing Confidentiality Agreements
- Organizing and Centralizing the Access-granting Process for Multiple Information Systems Containing PHI

Background on PeaceHealth

- Sponsored by the Catholic Sisters of St. Joseph of Peace
- 6 hospitals, 200+ physician practices, 3 home health agencies in 5 regions, 3 states
- 8,500 employees
- 12,000 info system users



Background on PeaceHealth

info systems that link our entities together:

- "Community Health Record"
  - IDX LastWord
  - IDXtend
- Organization-wide Intranet – "Crossroads"
- Other organization-wide systems
  - ESI (materials mgmt, surgery)
  - Infinium (HR)
  - Applix (Corporate Help Desk)
  - Etc.

Part 1
Online Confidentiality Agreements

Mandate:

- Create a system to capture annual renewals of confidentiality agreements electronically for all PeaceHealth information system users
- Block access to information systems for all users who fail to renew their agreements.

Narrowing the Scope
(issues)

- Requirement for annual renewal was a new concept for some PeaceHealth Regions
- No uniform policy requiring annual renewal
- Separate systems track “Users” vs. “Employees.”
  - Despite significant overlap, interconnectivity between the two is inadequate
- Majority of non-employee users are Providers and their office staff
  - Require special handling

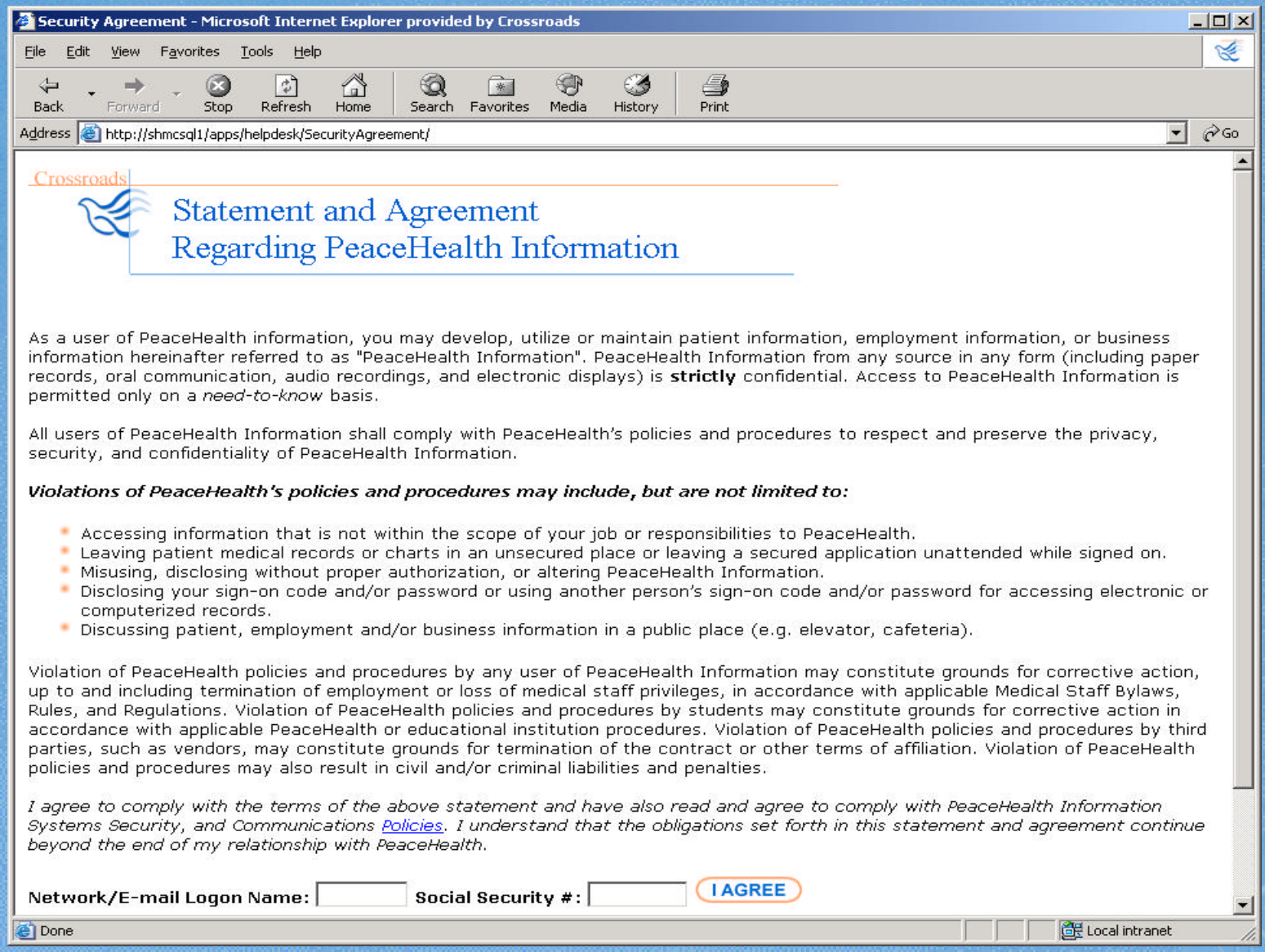
Narrowed Scope for First Year (2001)

- Limited to PeaceHealth employees
- No concrete consequences for failure to renew
- Scope to be expanded in subsequent years

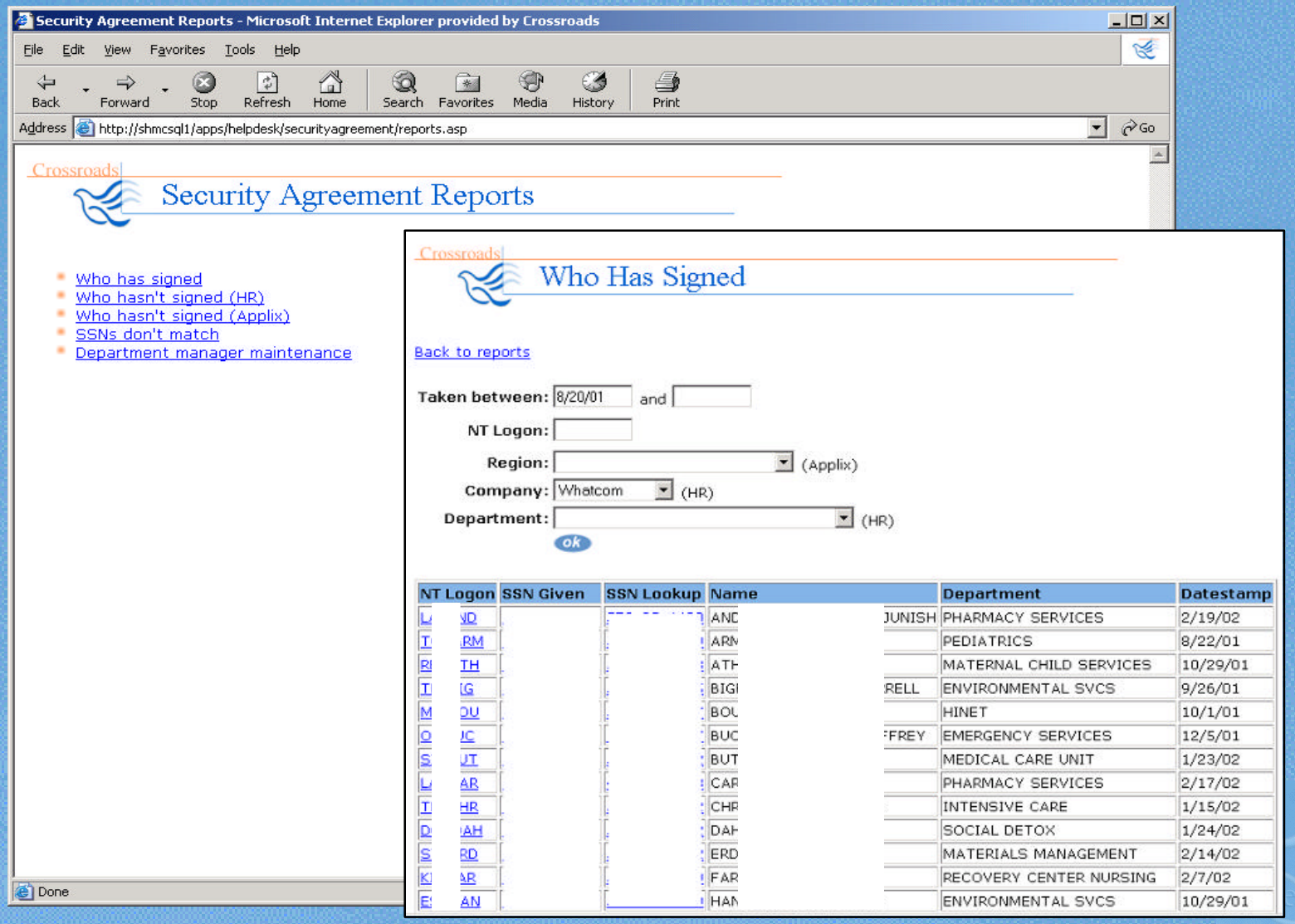
Technical Design

- Data resides in Applix (Help Desk) caller database
  - Network user ID
  - SSN as entered by user
  - SSN as stored in Applix Caller table
  - Date stamp
- “Signature” captured via intranet web page linked to Applix DB
- Detailed reports available to Region Coordinators online
- Nightly download sends data to Infinium HR system
- Managers able to view compliance data for their employees via HR “Manager Dashboard.”

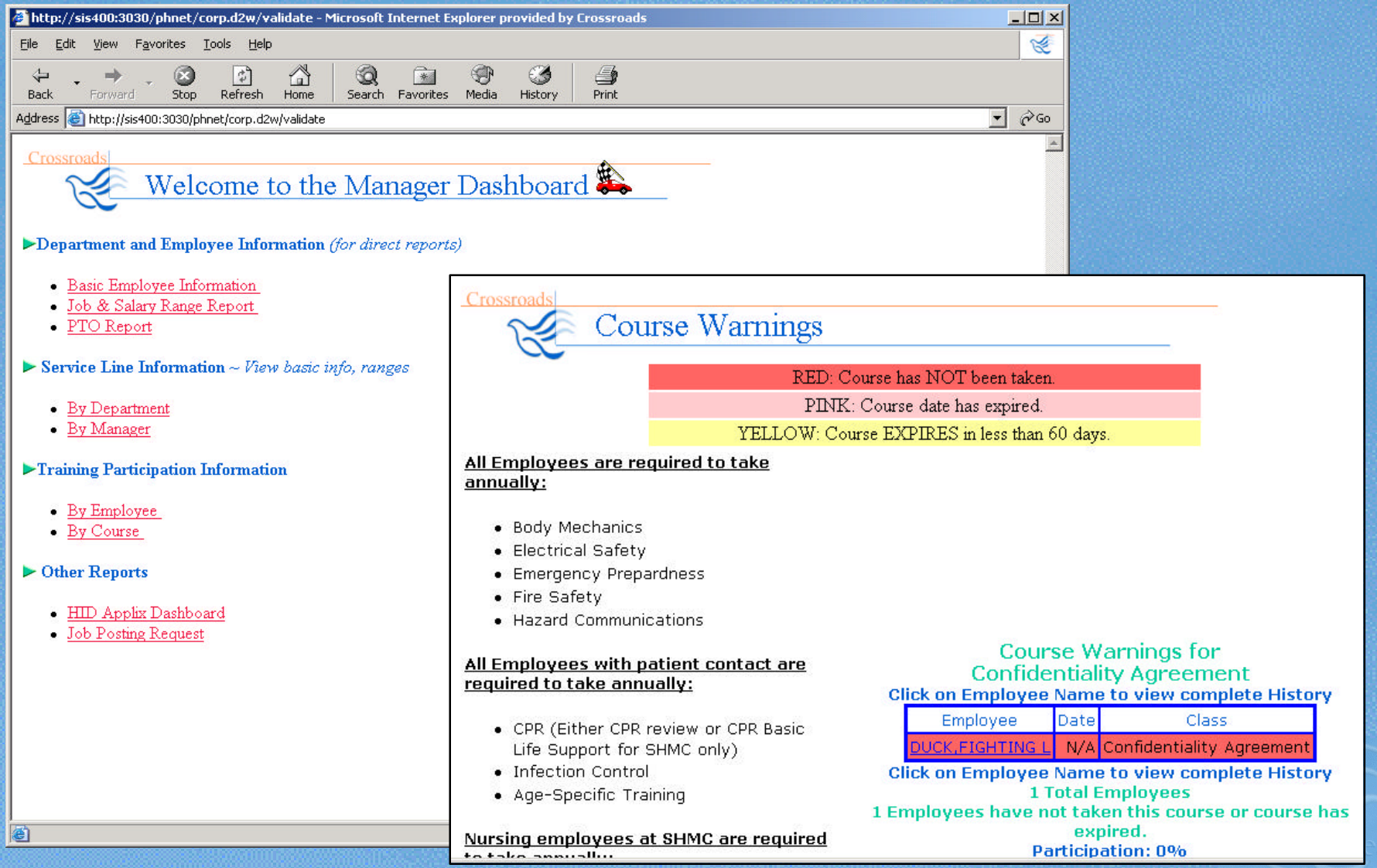
Technical Design: Online Agreement



Technical Design: Online Administrative Reports



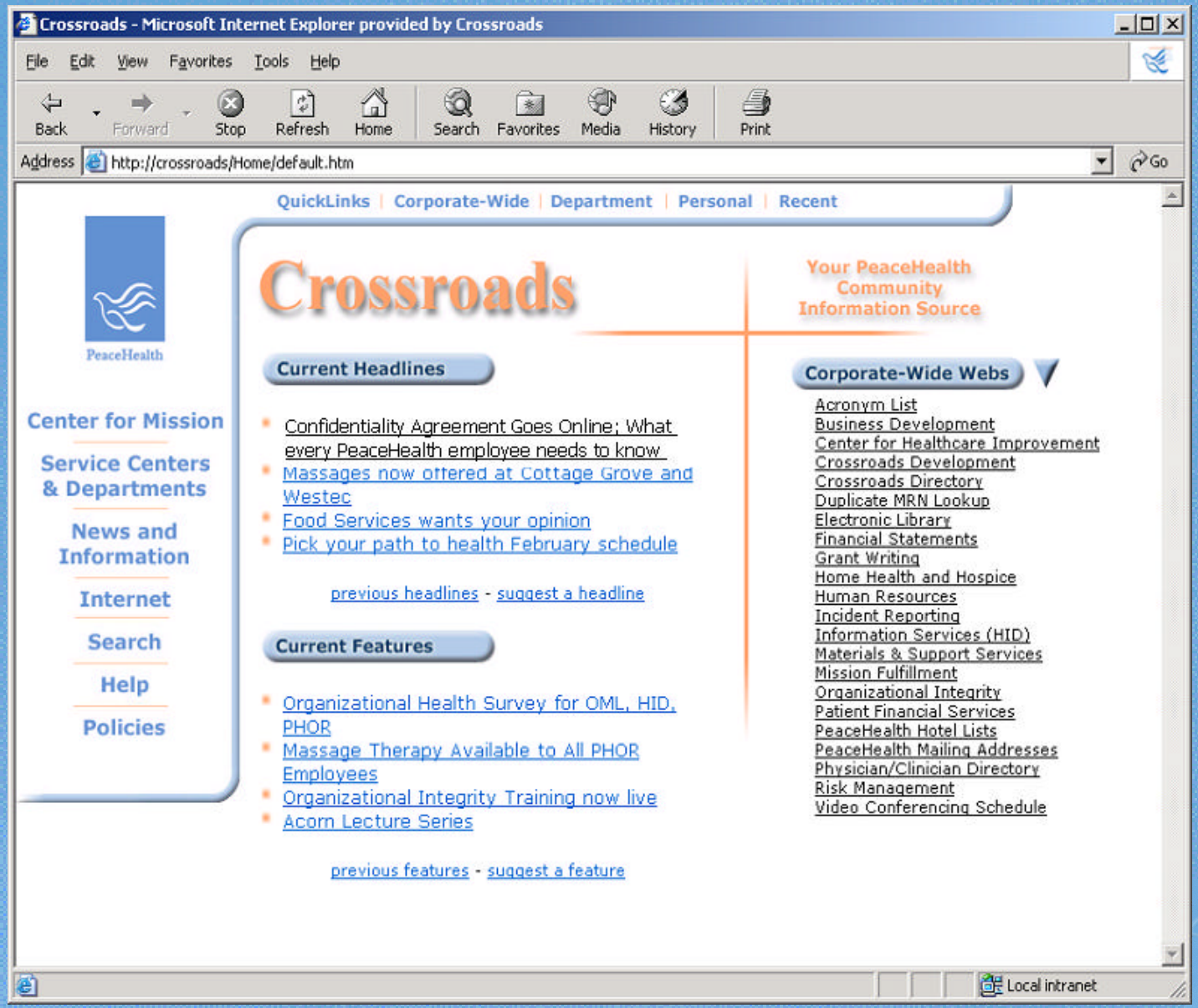
Technical Design; Manager Dashboard



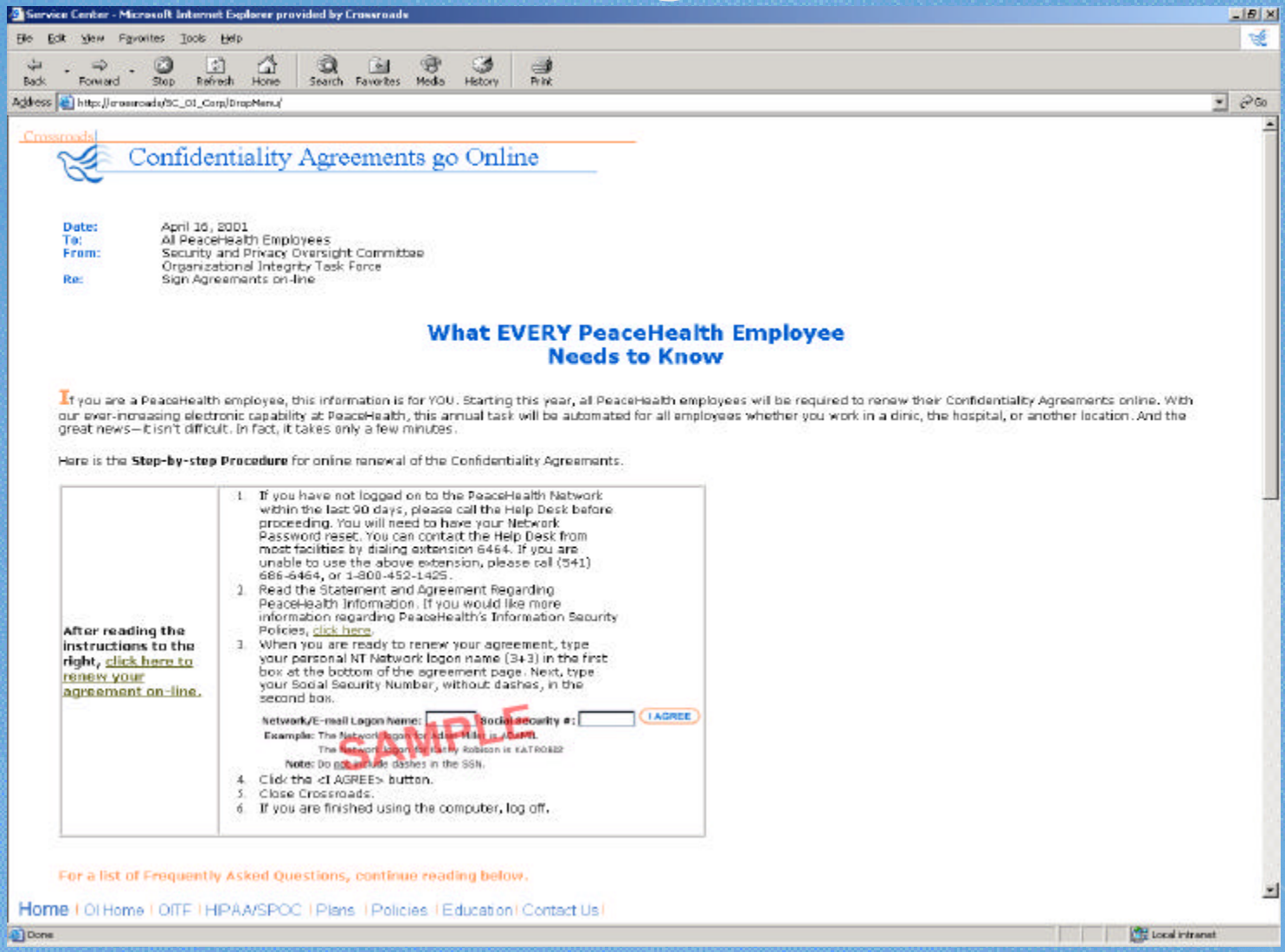
Communications

- Announcements made in regional management meetings
- E-mail announcement to all management
- Announcements in regional employee newsletters
- Bulletin board posters
- “Headline” article on intranet home page
- Reminder e-mails

Communications: Intranet Homepage



Communications: Instructions & Link to Agreement



Renewal Month – Process

- Started with e-mail announcement (with link to instructions) to all employees
- Weekly reports to managers
- Weekly e-mail reminders sent to those who had not yet renewed (auto-generated distribution list)
- Troubleshooting, assisting, responding to questions and issues

Renewal month; Weekly Reports to Managers

(also available via Manager Dashboard)

Crossroads

Who Hasn't Signed (HR)

Back to reports

Report for Corporate, ORGANIZATIONAL INTEGRITY department.

Name	Title	SSN
BA	HIPAA PROJECT LEADER	[illegible] 10
BE	AA ORGANIZATIONAL INTEGRITY	[illegible] 51
CH RET	DIR IS SECURITY	[illegible] 23
HA	DIR CORP CMU CQS HI	[illegible] 52
JC N	REG COORD, SECURITY & PRIVACY	[illegible] 39
RA	REG COORD, SECURITY & PRIVACY	[illegible] 93
SH LE	REG COORD, SECURITY & PRIVACY	[illegible] 11
VA NE	CORPORATE INTERNAL AUDITOR	1 30

Renewal month; Reminder e-mail

From: Johnston, Kevin
Sent: Wednesday, May 02, 2001 1:58 PM
To: DL:SJH-Unsigned Security Agreement
Subject: Re-Sign On-Line

Re-Sign On-Line!

This is the month for you to renew your confidentiality agreement with PeaceHealth.

As part of our efforts at PeaceHealth to be diligent about confidentiality and security of private information, we have automated our annual confidentiality agreement renewal process. An electronic renewal form is now available on Crossroads, and it takes only a few minutes to complete.

Renewal is required for all PeaceHealth employees, so don't delay! Renew your confidentiality agreement today.

To learn more about the Online Confidentiality Agreement, click on:
<http://phcinet1/News_CorporateCenter/Agreement.htm>

To go directly to the online confidentiality agreement, click on:
http://shmcsql1/apps/helpdesk/SecurityAgreement/

If you have any questions about renewing your confidentiality agreement online, please contact Tonya Ramsay, your Regional Coordinator for Security and Privacy at (360) 738-6300, ext. 2265.

Thank you!

Renewal month: Issues encountered

- New hires
  - Newly hired employees signed a paper agreement, but show up in the system as not having renewed.
- Social Security Number
  - Some employees uncomfortable with entering SSN online

Solutions – New hires

- Decided that, if hired > 6 months prior, not required to renew
- Communicated this repeatedly
- Some managers had new hires renew anyway to “clean up” data on Manager Dashboard

Solutions – SSN

- Provided information on actual confidentiality of SSN
- Provided information on our use of SSN
- Came up with a “witness” process for those who absolutely refused to enter SSN

Results from first year

- Over 95% of PeaceHealth employees renewed their agreements
- Some regions began to use online renewal system to capture original signatures, not just renewals

Planning for Year 2

- Policy requiring annual renewals of confidentiality agreement needed
- Desire to expand scope to:
  - include non-employees
  - block access for those who fail to renew
- Eliminate problems with new hires and SSN

PeaceHealth

Year 2
Expanded Scope & Improvements

1. Require independent providers and their office staff who have access to our info systems to renew agreements annually
2. Block access to information systems for most users who fail to renew their agreements.
3. Eliminate use of SSN
4. Account for new hires

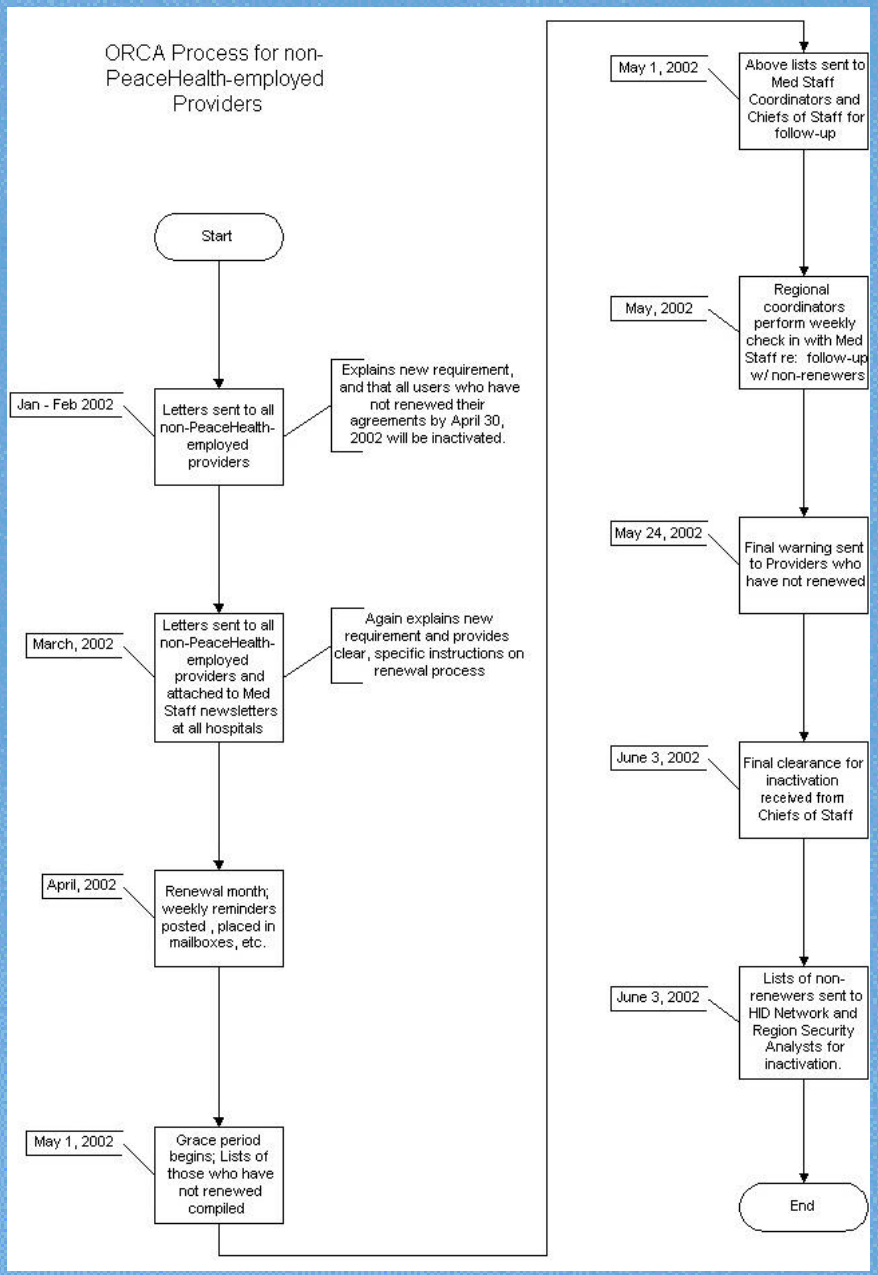
1. Include independent providers and their office staff

- Identification: Independent providers are registered in our systems no differently than employed providers
- Not all are set up as Network users – required for online agreement renewal
- Deactivation of independent providers a sensitive issue

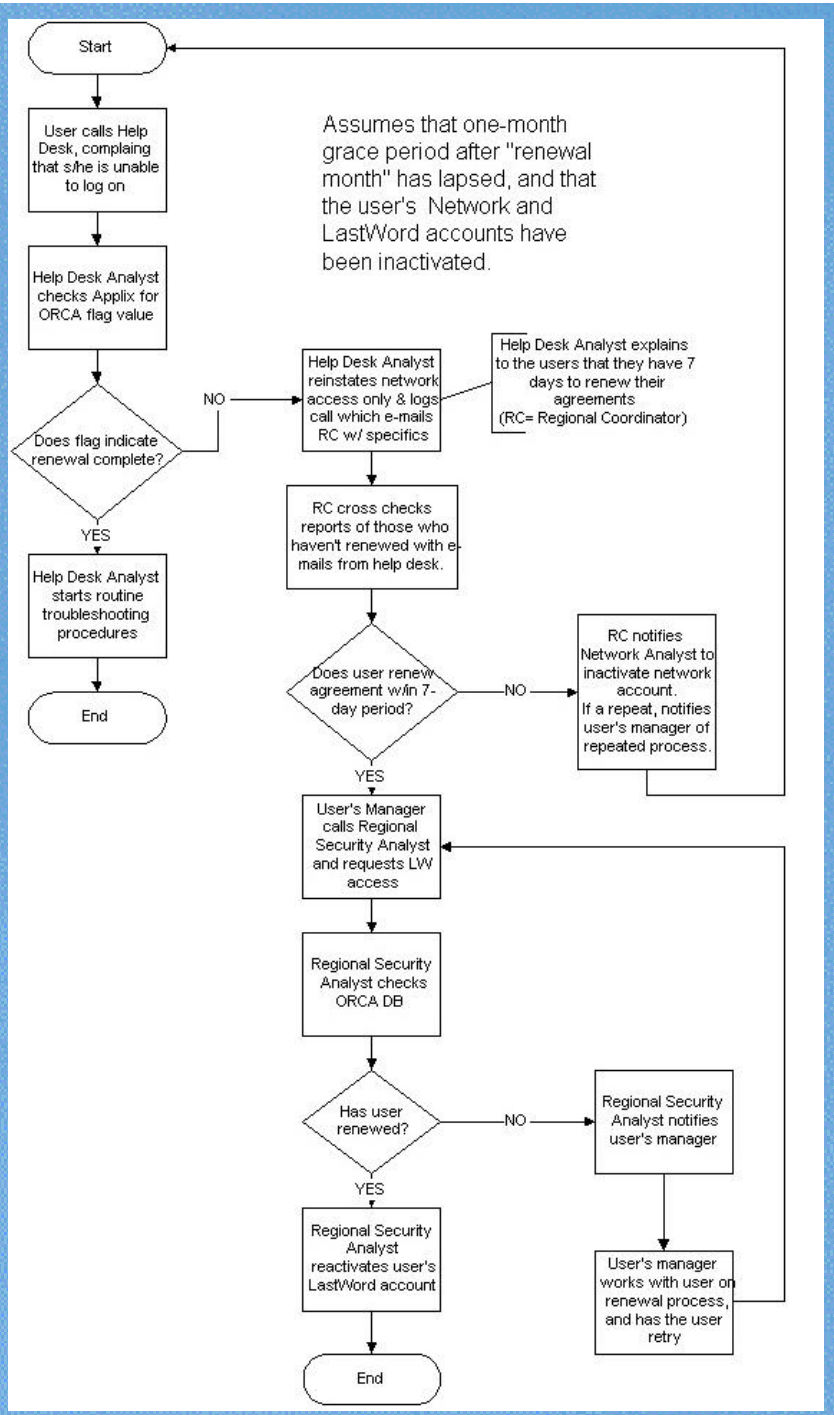
2. Block access to information systems for most users who fail to renew their agreements

- Politically charged; inactivated personnel will be unable to work
- Requires parallel processes; significant applications (LastWord, IDXtend, etc.) don’t require network login for access
- Reactivation process complex and involves many players

Deactivation Process (Independent Providers)



Reactivation Process (LastWord)



3. Eliminate use of SSN

- SSN was used only to link renewal record with user's HR record
- HR system now stores network ID for each employee
- Programming change enacted to transfer renewal record to HR system using network ID as link instead of SSN

4. Account for new hires

- Some regions are having new hires sign agreement electronically
- New policy requires that, when signed on paper, HR must enter record of agreement in electronic system
- Manager Dashboard now correctly reflects new hire signatures

Renewal Month Process; Year 2

- Communicate re: potential loss of access for failure to renew
  - Letters to independent providers
  - Announcements to management
  - Announcements in employee newsletters
- Weekly reports to managers
- Weekly e-mail reminders sent to those who have not yet renewed (auto-generated distribution list)
- Troubleshooting, assisting, responding to questions and issues

Planning for the future

- Include all other systems users
  - Students
  - Vendors
  - Volunteers
- Technical possibilities
  - Integrate with other systems better
  - Systems access database?
  - Automate deactivations?

Part 2

Organizing the Access-granting Process for Multiple Information Systems Containing PHI

Systems and Applications in use at PeaceHealth

(a partial list)

- Network/E-mail
- IDX LastWord (Clinical/ HIS)
- IDXtend (Practice Mgmt.)
- Antrim (LIS)
- Lanier Transcription Services
- ESI (Materials Mgmt; Surgery)
- Enterprise View (Clinical Data Warehouse)
- Applix (Help Desk; User database)
- Infinium (HR, Training/ Education tracking)
- Morrisey (Med Staff Mgmt.)
- Cascade (Inpatient coding)
- HcM (Financial Decision Support)
- Pyxis (Pharmacy)

Current Processes
involve in various combinations:

- Managers
- Desktop Support Analysts
- Systems Administrators
- Data Stewards
- Security Analysts

Defining the need

- Define “access”
- Comply with HIPAA rules (Privacy & Security)
- Centralize access-granting, modification, and termination processes
- Facilitate manager involvement
- Make it auditable

Defining the Need: What is "Access?"

- Noun: the ability or right to enter or use
  - (a non-material possession)
- Verb: to make contact with or gain access to
  - (an action)

Defining the Need: Levels of Access

- Level 1: everything up to, and including, general access to an information resource; one can “open the door”
- Level 2: once you're “in the door” of the information resource, what “rooms” you can get into
- Level 3: once you are “in the room,” what you actually do (behavior)

Defining the Need: Comply with HIPAA Rules

Privacy § 164.514(d)(2)(i) re: Minimum Necessary

A covered entity must identify:

- (A) Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and
- (B) For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access.

PeaceHealth

Defining the Need: Comply with HIPAA Rules

Security (proposed) § 142.308(a) re: Administrative Procedures; Information Access Control

- Access authorization policies and procedures
- Access establishment policies and procedures
- Access modification policies and procedures

Defining the Need: Comply with HIPAA Rules

Security (proposed) § 142.308(c) re: Technical Security Services; Access Control

- Context-based access
- Role-based access
- User-based access

Defining the Need: Centralize the access granting, modification, and termination processes

- Eliminate questions about who controls access to what
- Create a place for “one-stop shopping” for access control

Defining the Need: Facilitate manager involvement

- Managers are typically the ones to request access for staff
- Managers are typically most knowledgeable about what their staff people do and need access to
- Managers typically have front line accountability for staff behavior

Defining the Need: Make it auditable

- We should be able to monitor our compliance with our policies and with HIPAA rules

Envisioning a Solution

Q: What can we realistically control centrally?

A: Level 1 Access, some Level 2 Access

Envisioning a Solution: Different Needs

- New hires
- Job/responsibility changes
- Terminations
  - voluntary
  - involuntary

Envisioning a Solution: Different Systems

- Different attributes define a user in each system
- Different user name/ID conventions
- Some systems have less than complete user data (SSN)
- Different people manage systems – in some cases, different cultures

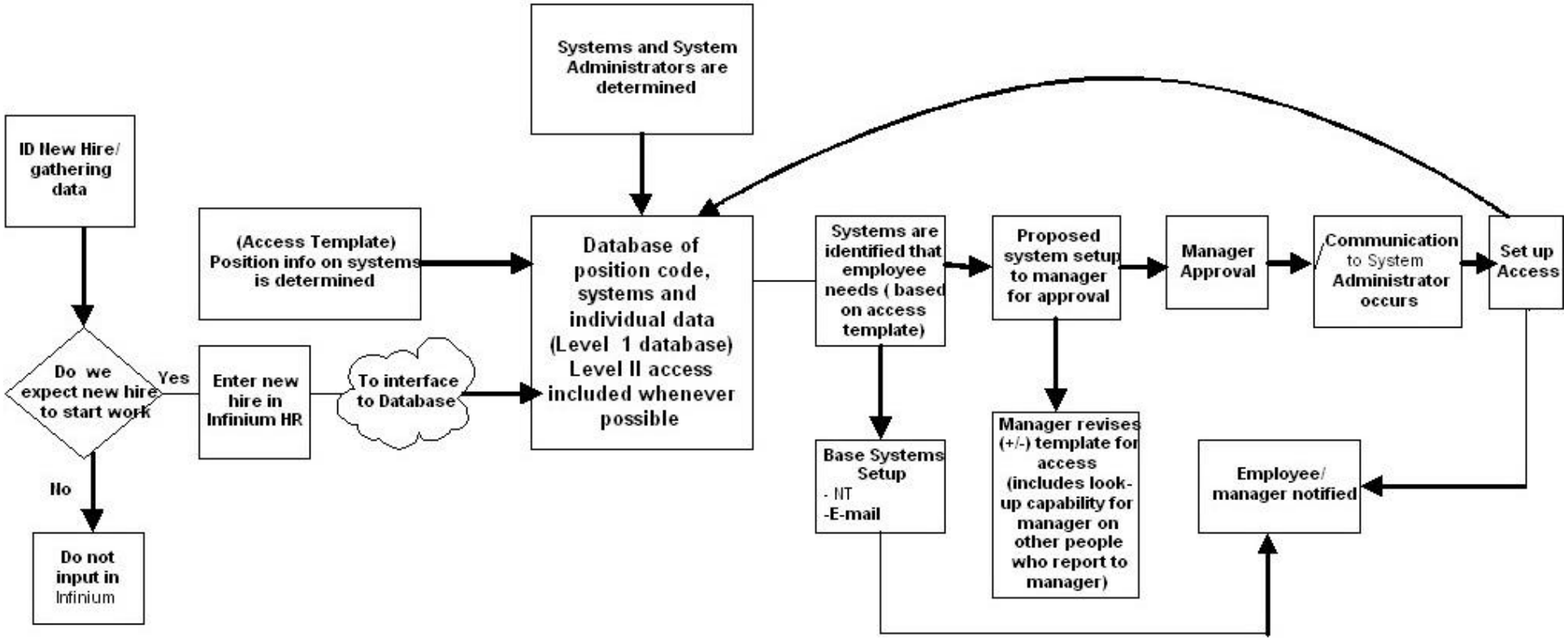
Envisioning a Solution: Putting it all Together

- Find ways to interface with the user file/table in each system
- Gather data
- Combine user data with employee data (job classes)
- Create User Access Templates
- Create system/processes that use, update, and reinforce templates

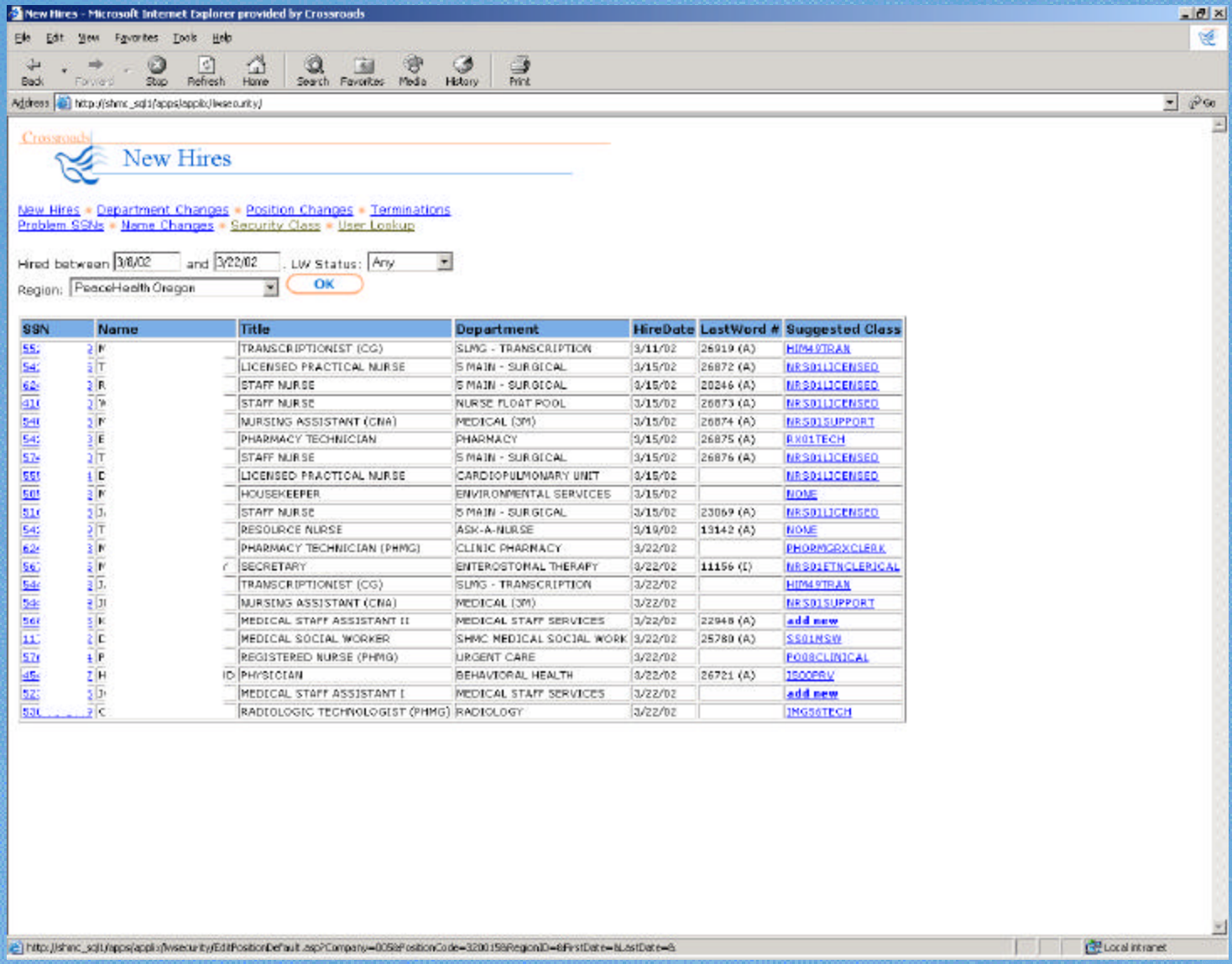
Putting it all Together, cont.

- Manager interface to allow:
  - Viewing user access templates
    - Per user
    - Per template
  - Adding or deleting selections for a user
  - Automatic reinforcement of user access templates
- Audit capabilities – templates and users

New Hire Process



System progress to date



Crossroads

User Details

- Back

Human Resources Information

SSN	Pref. Name	First Name	Last Name	MI	Cost Center	Gender	Location	Supervisor
	KEVIN	KEVIN	JOHNSTON	B	87160	?		?

Title	Department	2nd Job	2nd Department	Hire Date	Term Date
REG COORD, SECURITY & PRIVACY	ORGANIZATIONAL INTEGRITY			10/21/85	

LastWord security

User #	First Name	Last Name	MI	DOB	Active	Title	Class	Pointer	Password Change	Last Login
213	KEVIN	JOHNSTON	B	06/01/1956	A	REGN COORD		00038	11/8/01	8/7/00 11:18:10 AM

VMS security

Account #	Name	Status
X213	KEVIN B JOHNSTON	Disuser

IDXTend security

User #	Mnemonic	Name	Profile	Sessions
213	KBJ01	JOHNSTON,KEVIN B		1

System Security

Caller	System	Comments	Date Granted	Date Revoked
kevjoh	NT	PHC - Johnston, Kevin Organizational Integrity - Eugene	1/14/98 11:01:31 PM	
kevjoh	Exchange	Kevin Johnston Corporate Organizational Integrity	3/19/98 10:03:38 AM	
KEVJOH	LastWord	JOHNSTON, KEVIN B	1/1/00	

Applix Information

Caller	Workgroup	Rep	Notes	Access Removed Date	Post Term Access
KEVJOH	PHC_OI_EUG	DAVCRA			N

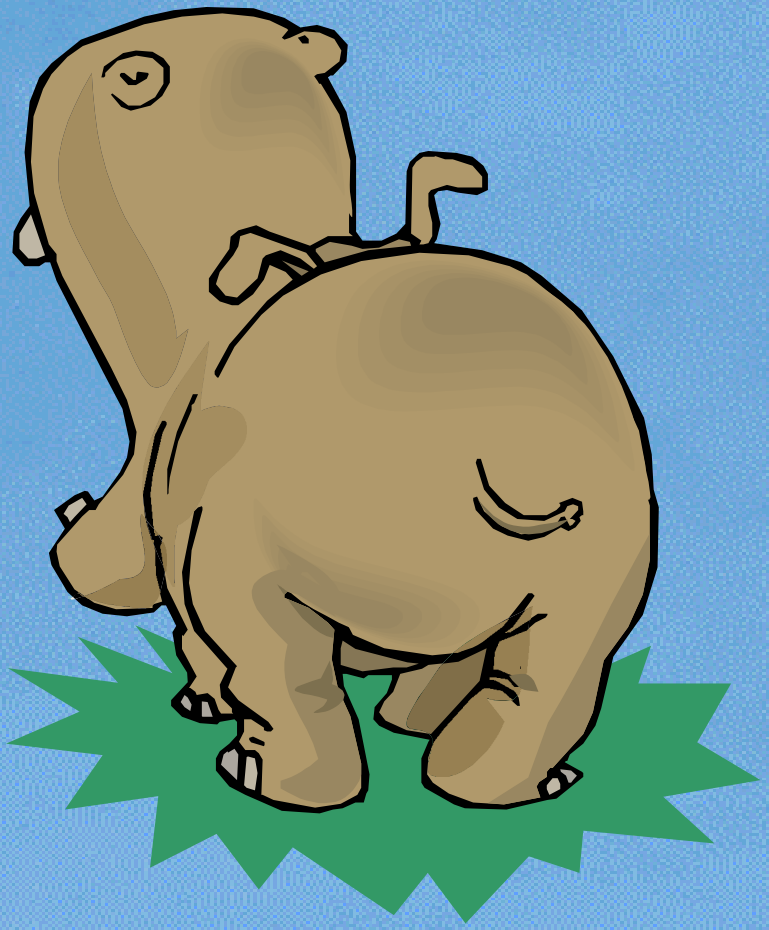
PeaceHealth

Plans for the Future
(immediate)

- Provide manager access to systems access database via Manager Dashboard
- Display user access templates
- Suggest Level 1 access template per job class
- Allow manager interaction – selection and/or de-selection of specific systems Level 1 access

Plans for the Future
(long term)

Systems Access database may interact with other systems such as:

- Single Sign-On system
- Online Renewal of Confidentiality Agreements
- Others?

Questions?