

# Identity & Access Management Case Study

## A Health Plan's Identity and Access Management Implementation

ISSA

September 19, 2006

Presenter: Dee Chouinard, CIPP, CISSP

# Road Map to Implementation

*Harvard Pilgrim Health Care, a regional health plan, when faced with HIPAA's privacy and security mandates, made a decision to implement an Access and Identity Management Program. Currently in year two of a three-year implementation, there have been successes and many lessons learned. The following is a case study that will outline the road map used and the journey thus far.*

## Planning

- Key Drivers
- Requirements Gathering
- Choosing a Vendor
- Communicating the Opportunity
- Management Buy-In

## Building the Infrastructure (Years 2 and 3)

- Technical Build
- Courion Configuration
- Roll-out Strategies
- Current Status

## Setting the Stage (Year 1)

- Implementation Approach
- Password Management
- Role Engineering
- Facilitating a Culture Shift

## Ongoing Maintenance (Year 3)

- Governance
- Administration/Operations

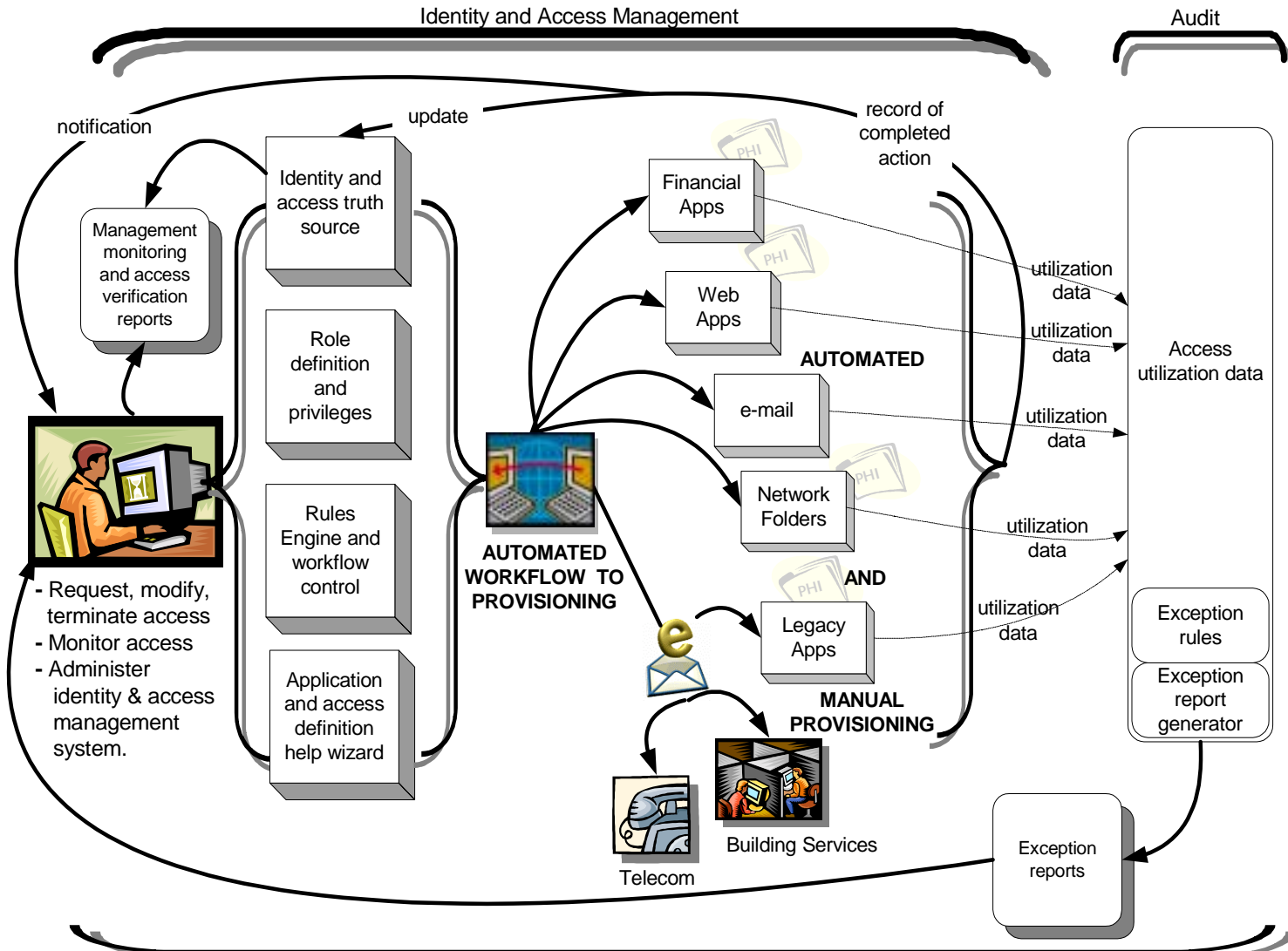
# Planning: Key Drivers

- Both HIPAA's Privacy and Security Rules have a requirement to implement access controls
- Privacy Rule evaluation and Security Rule Risk Assessment indicated:
  - Need to clean-up inappropriate access
  - Need for consistent, auditable management practices for account provisioning
- Account management is key focus of audits in post Sarbanes-Oxley environment
- Meet customer expectation of adhering to minimum necessary or least privilege when accessing member data
- IT decision-makers view Identity and Access Management as a chief security concern

# Planning: Requirements Gathering

- Requirements were developed by interviewing a cross section of 30 business and technical staff - *3 month process*
- Business requirements were bucketed into four key functional areas:
  - 1) Request Management Workflow (25 requirements)
    - User business/access profile information
    - Identity information and historical records of access granted
    - Role definitions and privileges
  - 2) Provisioning Workflow (10 requirements)
    - Rules that will dictate the workflow of approvals and pre-requisites
  - 3) Account Re-Validation (8 requirements)
  - 4) Administration and Monitoring (17 requirements)
- Technical requirements consisted of a CRUD Matrix for Operating Systems and applications (16 requirements)

# Planning: Requirements Gathering



Administration, Maintenance and Monitoring

# Planning: Communicating Opportunity

- Began planning and sowing the seeds for the opportunity in the technology space 6-12 months prior to requirements gathering
- Gained support and understanding of CIO
- Used HIPAA projects as showcase for access management issues - enforced principle that IAM is *'not just an IT project'*
- Project assigned to Service Excellence & Operations Committee - used as a sounding board and avenue to educate
- Presented to department teams a primer on both Access Management and Role Engineering
- Used a successful implementation of a Password Management Tool as a way to build awareness

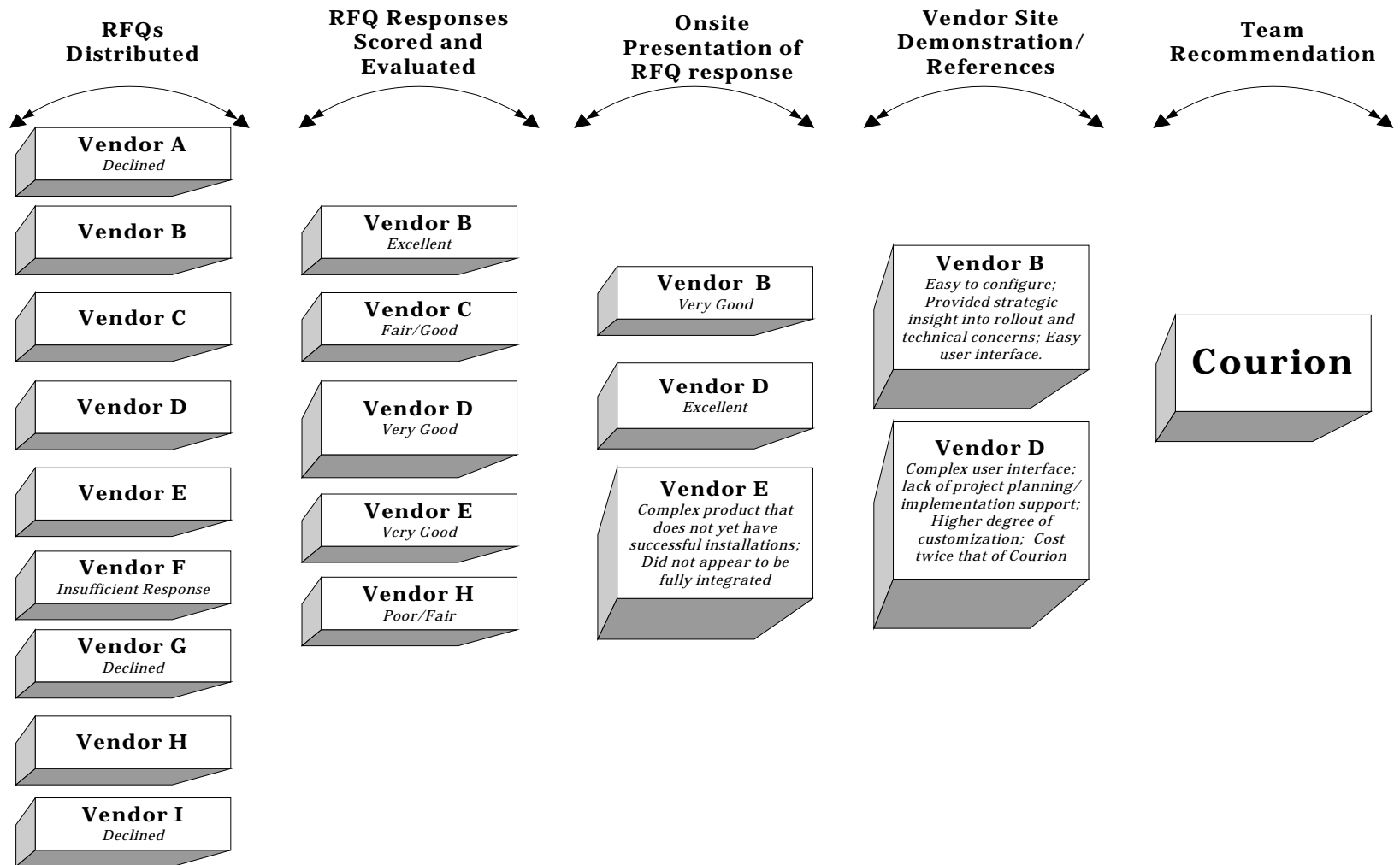
# Planning: Management Buy-In

- Used results from Privacy Rule evaluation and Security Rule Risk Assessment
- Surveyed industry experts for status of other similar health plan efforts
- Identified phases and sub-projects with distinct deliverables and timelines
- Used well publicized security related incidents to drive home issues - *'not if but when'*

# Planning: Vendor Selection

- Consultation with Gartner/industry experts to identify appropriate vendors
- Request for Quote (RFQ) documentation was distributed to nine vendors
- Developed scoring criteria for assessing RFQ responses
- Small core team scored responses and narrowed down the finalists to three
- Finalists were invited to present their response, demonstrate their product and entertain questions from a large cross section of business and technical representatives
- Vendor site visits and reference calls were made
- Selection made - *4 month process*

# Planning: Vendor Selection (continued)



# Planning: Lessons Learned

- Education and awareness techniques critical to success
- Involve wide range of technical and business stakeholders
- Gaining executive support and sponsorship helped smooth the way for resource acquisition
- Do not underestimate time for both planning and implementation - 3-4 year process not an overestimate
- Handpick your Steering Committee and charge them with being champions of the project
- Obtain professional consultation for vendor selection

# Setting the Stage: Implementation Approach

- Small, distinct projects each with own merit
- Discovery period - Courion understands HPHC's infrastructure, HPHC understands Courion's product capabilities and implementation methodology
- Obtain quick 'win' and exposure with Password Management Implementation
- In order to reach long term goal, might need to implement short term inelegant solutions to meet immediate business need
- Current access cannot be migrated to new product, must engineer roles

# Setting the Stage: Building the Team

- Oversight - Service Excellence & Operations Committee
- Project Sponsors - CIO and CISO
- Steering Committee - IT Strategy, IT Security, IT Solutions, IT Customer Service, HR, Internal Audit and various key business users
- Core Team - Business Project Manager, Technical Project Manager, Courion Liaison, Sr. Business Analysis, IT Security Liaison, Project Coordinator, and Program Manager
- Added to Core Team as a result of implementation - Integration Project Manager, Special Teams Project Manager
- Technical resources planned on an annual basis
- Business resource need communicated via Service Excellence & Operations Committee

# Setting the Stage: Password Management

- Implemented Courion's PasswordCourier
  - Quick win
  - Best way for players to get to know each other
  - Needed to mitigate risk for user compliance with Password Policies
- Identified key applications to be included
- Made decision to implement voice biometric password reset for forgotten passwords
- 7 month implementation
- 100% of users trained, registered and using password reset utility within 60 days

# Setting the Stage: Role Engineering

- The process of identifying the appropriate mix of access levels/access to resources and rules to define a role
- Assigning role(s) to workforce members thus creating role based access to all resources required to perform a task or job function
- Roles are not tied to job titles but rather to job functions
- One user may have multiple roles
- Multiple users may share a common role; should have finite number of roles
- Access is guided by the principle of “minimum necessary” or least privilege
- Clean-up of current access while defining roles

# Setting the Stage: Role Engineering (continued)

## *Role Engineering - 12 month process*

- Collected all current accounts
- Using cluster analysis, determined by business unit, likely roles and those resources falling outside of roles for each user
- Developed a series of reports and business unit analysis instruction set
- Collected changes and re-defined roles per department analysis
- Conducted a security review, key stakeholder review for cross functional roles
- Obtained final sign-off from senior departmental staff member
- True-up to Roles

# Setting the Stage: Facilitating a Culture Shift

- Building awareness through both password management and role engineering processes
- Continued education with business leadership through executive committees and project portfolio presentations
- Informal discussions with human resources and internal audit to understand concerns and best practices
- Brochures at annual internal trade event
- Communication in corporate newsletters
- Exposure at all levels of the organization

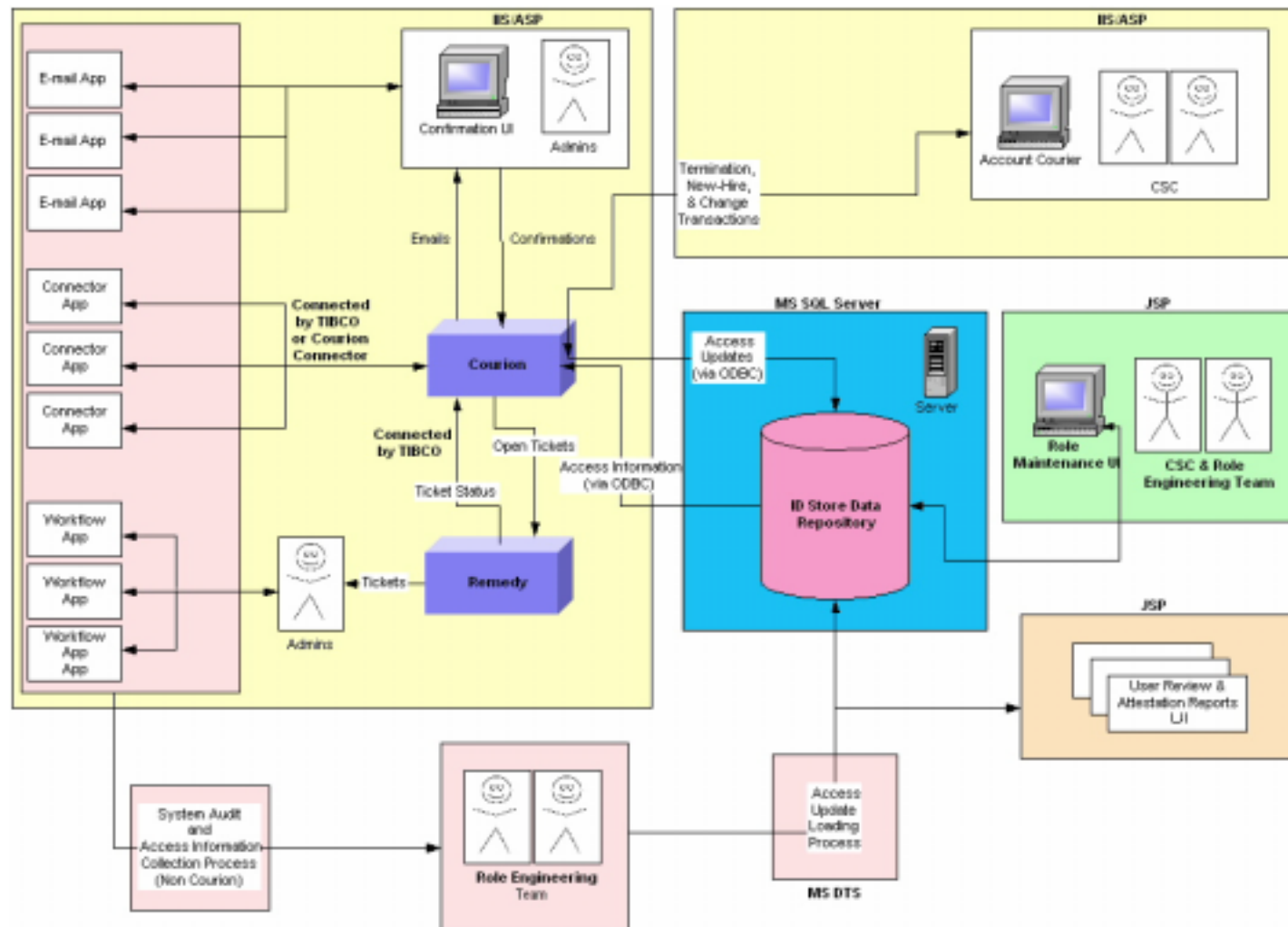
# Setting the Stage: Lessons Learned

- Education and awareness techniques critical to success
- Ill-defined business processes take time to resolve
- Triple your planning and discovery estimates – you really don't know everything that's out there – don't try to integrate every application at once
- Not all applications are created equal and there may be technical hurdles to overcome – non-standard configurations take extra time to work out
- Policy compliance may be implemented differently and takes extra time to standardize across platforms
- Stick to scope but be flexible to achieve success
- Keep your eye on the prize

# Building the Infrastructure: Technical Build

- Identified source of information for all data elements needed for the provisioning transaction - user account profiles, provisioning rules, role data and corporate policies
- Determined need to create formal ID Store to house data related to IAM transactions
- Year 2 Tasks Include:
  - Create utility to house and update role data
  - Develop an Account Re-validation utility to be used until migration to ComplianceCourier (Year 3)
  - Automate collection and data normalization of account data in order to make available for use by Courion and for Account Re-Validation
  - Migrate from Role Engineering Tactical Store to permanent ID Store

# Building the Infrastructure: Technical Build (continued)



# Building the Infrastructure: Courion Build

- Integrate HPHC's traditional project management approach with Courion's prototype approach
- Made decision to configure Courion while building the technical infrastructure
- Key Workflows include:
  - New Hire Transactions
  - Termination Transactions
  - Transfer Transactions
  - Change Transactions
- Key technical configuration includes:
  - Building automated connectors to key applications
  - Building automated workflow to Remedy/OPAS (Technical Customer Service Request Management System)
  - Building email notifications

# Building the Infrastructure: Roll-out Strategies

- Focus on key business and compliance needs first
- Make impact on business users as painless as possible
- Use network of business unit 'experts' to facilitate business process change for account requests
- Create awareness and expectation through multiple communication vehicles: signage, newsletter articles, supervisor email messaging
- Create incentives where possible
- Initial Courion Roll-out to IT Customer Service Center
- Engage Internal Audit consultation for interim and long term solutions

# Building the Infrastructure: Current Status

- Role Engineering completed
- True-up to roles will be complete within next month
- Account Re-Validation roll-out begins end of October
- Courion AccountCourier configuration on schedule for completion by early October
- Courion roll-out to IT Customer Service staff by end of November
- Year 3 initiatives include:
  - Build/connect to truth source for user information
  - Roll-out of Self-Service AccountCourier
  - Configuration and Roll-out of ComplianceCourier
  - Build additional automated connectors

# Building the Infrastructure: Lessons Learned

- Education and awareness techniques critical to success
- Expect the unexpected
- Integration amongst sub-projects is critical
- Anticipate 'traffic jams' and have contingency plans
- Be prepared to provide education and awareness about project road map over and over again
- Clean-up access prior to attempting to engineer roles
- Pick the right department for pilot testing

# Ongoing Maintenance: Governance

- Very little industry knowledge on which to build a governance program
- Must designate ownership for all IAM components
- Must determine how roles and rules are monitored and changed
- Must determine ongoing role analysis and frequency of update
- Must determine administration mechanism for roles and rules
- Form workgroup to brainstorm and make recommendations to Steering Committee
- Be prepared to facilitate a culture shift

# Ongoing Maintenance: Administration/Operations

- Identify ongoing administrative needs
- Designate data ownership and maintenance responsibilities
- Design reporting and alerts to workflow trouble shooting
- Identity performance metrics
- Create audit reports to ensure compliance with policies

# Ongoing Maintenance: Lessons Learned

- Education and awareness techniques critical to success
- Share with other companies facing similar issues
- More to come....



And the journey continues.....