Baxter PSAS
Privacy Self Audit System

An exercise in process re-engineering

Jeff Bailey
Winter/Spring 2006
CS 491
PSAS – Background

- Baxter Data Privacy and Security function requires an annual audit of all business processes, vendors, and systems to ensure compliance to global privacy policies.
  - HIPAA
  - US EU Safe Harbor
  - Country Specific Regulations
- Incomplete or late audit may result in temporary suspension of vendor contracts or system shut down.
PSAS - Current Process

- Process or system owner completes up to four audits.
  - 5 to 16 questions each.
- Completed audits are routed to the appropriate reviewer.
  - Transmitted via fax or intra-office mail to a Data Privacy Coordinator.
  - Data Privacy Coordinator identifies appropriate reviewer.
  - Forwarded to reviewer via fax or intra-office mail.
PSAS - Current Process

- Review Process.
  - Approved
    - Update master approval list (Excel spreadsheet)
    - Original documents are transferred to remote facility (Iron Mountain) for long term storage.
    - Other copies are destroyed.
  - Rejected
    - Audit returned to owner with comments.
    - Owner makes necessary corrections.
    - Audit submitted to Data Privacy Coordinator.
PSAS – Problems

- **Slow**
  - Average turn around time on audits is more than five (5) weeks.
- **Risky**
  - Owners must “remember” when audits are due.
  - System shut-downs are not uncommon.
- **Complexity**
  - Less than half the questions can be answered without assistance.
    - No access to prior audit data.
    - 5% of responses differ from prior audits.
PSAS – Problems

- **Reporting**
  - Reconstructing an audit history is not possible.
  - Master approval list inaccurate.
- **Communications**
  - Personnel changes result in chaos.
PSAS – Solution

- J2EE web application for tracking audits and approvals.
- Corporate Integration
  - IBM Websphere – Application Server
  - Oracle 10g – Data Store
  - Microsoft Active Directory – Authentication
- Open Source Libraries
  - Webwork – Web Framework
  - Sitemesh – Interface Templating
  - Spring – Transaction Management, IoC (injection)
  - Hibernate – Object Relational Persistence
PSAS – Benefits

- Streamlined process
  - Immediate routing and notification to responsible party.
    - No more confusion and delays due to lost submissions.
  - Focus on changes
    - Improved accuracy.
    - Less effort.
  - Eliminate procedures around storage and transfer of paper records.
- Reporting
  - Full audit and approval history
    - Makes lawyers happy (for a change)
- Storage
  - NO MORE PAPER!
PSAS – Objectives

- Complete development by May 1, 2006
- In production June 1, 2006 in time for Q2 audits.
- Data Migration (from paper) by June 30, 2006
PSAS – Progress

- Business requirements signed off.
- Application development
  - User interface – done
  - Primary flows – 85% complete
  - Notification system – 10% complete
  - Reports – not started
  - Data Migration – 20% complete
- Q/A
  - Unit tests – 85% complete
  - User Acceptance Testing – not started
- Deployment
  - Request production database – done.
  - Schedule deployment – not started.
PSAS – Next Steps

- Notification system.
- Reports and audit history.
- Finalize audit questions.
- Testing Testing Testing!
- Schedule deployment.
- Data migration
  - Paper to Spreadsheet – in progress
  - Spreadsheet to SQL – not started
PSAS: Privacy Self Audit System

Businesses & Systems

⇒ Safe Harbor Reminder! (Instructions, Businesses & Systems List)

- If a Baxter entity currently manages or will manage private data, the completion and submission of a Privacy Self Audit is required. An audit that is being completed for Safe Harbor certification will must be submitted and approved by the compliance readiness date, which is typically during June of each year. For more information, please go to Baxter's Global Privacy Practices website.

- In addition to the Privacy Self Audit, a hard copy signature and certification is required for Safe Harbor readiness. If your Privacy Self Audit submission has a Safe Harbor requirements, please download, complete and fax (847-948-3927) or mail (DF2-2W) the Recertification Worksheet to Suzanne Emmer, Safe Harbor Taskforce by the compliance readiness date.

⇒ Self Audit Instructions (Businesses & Systems List, Reminder)