The VA’s Battle for Privacy Protection: Best Practices from the Digital Front Lines
Agenda

• Introductions
• Background on the VA organization and privacy program specifics
• VA Approach to Privacy and Compliance
• The Challenges-Openness, Privacy Risks, Confidentiality and Funding Concerns
• A Best Practices Approach to Privacy and Risk Management through automated compliance and collaboration
• The Role of Technology Solutions-How can Collaboration Solutions assist (case study- best practices approach to enterprise wide governance for their enterprise SharePoint environment)
Who We Are

John Buck, Director, Office of Privacy and Records Management, US Department of Veterans Affairs

Dana Louise Simberkoff, JD, CIPP/US, Vice President, Public Sector, HiSoftware, Inc.
Background on VA and Privacy Program

• Over 325,000 employees, contractors and volunteers
• Administrations and staff offices
• Approximately 463 Privacy Officers – most are collateral duty
• VBA/VHA/NCA – full time PO (approx. 152)
• Both covered and non-covered HIPAA entities
• VA Privacy Service – staff of nine with two Privacy Officers supporting over 7,000 OIT Staff
• Privacy Service line of authority
VA Approach to Privacy and Compliance

• Balance protection of sensitive and/or “need to know” information
  – Compliance vs. life and death information sharing
  – Transparency
  – Collaboration within and across government
The Challenges

- Organizational size
- Prioritize Need vs. Funding
- Shared drives – only limitation is size of drive
- Medical Devices
- Accessibility, Privacy and Risk
- Reduce risk without impact to services
- Sharing data – both internal and external
- Governance and oversight
- SharePoint Sites
  - Over 700 VA sites
  - 2010 – Public facing potential
Best Practices

• IT controls
  – Filters
  – Scans
  – External Devices
• Data Protection and Management
• Training
• Visibility to the Desktop
  (patches/Security/Data in motion)
Mapping a Path from Here to There

Balancing transparency and collaboration with data protection and management

- People
- Policy and Process
- Technology

- Training
- Governance and Oversight
- Technical Enforcement
The Role of Technology Solutions

• Frequency of data/records management/multiplication of risk
• False positives
• Determine sources of sensitive data
• Intent to remove duplications, ensure unprotected data is secured and risk reduced or eliminated
• Protect employees from themselves-limited personal use
SharePoint Case Study

Optimizing SharePoint 2010 for Secure Collaboration and Storage of Sensitive Data

- Audit Document Libraries, Sites, Forums & Communities
- Prevent Data Breaches (PII & PHI)
- Comply with HIPAA/HITECH, Section 508/WCAG 2.0, FISMA
- Support Site Quality, Brand Integrity Guidelines
- Scan data as part of a migration strategy-on file shares or other legacy systems

www.privacyassociation.org/summit
HiSoftware-VA SharePoint Compliance Pilot Achievements

• Pilot (Sept 2010 – Aug 2011)
  – Phase 1 Installation at 6 sites
  – Scans for Accessibility and Privacy
  – Help Desk
  – Training Materials
  – Lessons Learned
  – Analysis of MOSS Environment

• Scope of Discovery
  – VA has millions of SharePoint pages across six pilot sites
  – Accessibility issues abound
  – Sensitive and private information exists in this environment
    • Whether or not it belongs is somewhat a moot point if it’s not under a strong Governance Policy
Findings Summary

Accessibility Total

- 70% 2,051,763
- 19% 570,946
- 7% 200,651
- 3% 95,390
- 1% 31,603

- All pages that have links to files that require a reader or plug-in must contain a link to the reader or plug-in.
- All IFRAME elements are required to contain element content.
- All INPUT elements are required to contain the ALT or TITLE attribute, or use a LABEL.
- Validate that the alt text does not contain the text: .jpg, .gif, .bmp, .jpeg.

www.privacyassociation.org/summit
Findings Summary

Privacy Total

- All Web Pages should be free of third party content or advertising - Links
- Telephone Number (US)
- Email Address
- Identify if there is a website purpose statement link
- External Link Disclaimer
- Security Practices/Policy Notice
- Check for VA PII Indicator Terms (Sample)
- Validate that pages with mailto links also have an opt-out link
- Privacy Policy Notice
- Validate that pages with mailto links also have a privacy policy link
- Operational Information - Address
- Audit
- Identify possible inclusion of Social Security numbers on a page

www.privacyassociation.org/summit
Compliance Project-September 2011
New Three Year Award

- VA has extended a one-year pilot implementation of HiSoftware Compliance Sheriff for SharePoint, through the award of a new three-year contract for HiSoftware Solutions for SharePoint compliance.

- This project includes an evaluation of the VA’s existing SharePoint environment to determine how to best leverage the technology that they have already deployed, as well as a forward look at how they should utilize SharePoint in the years ahead.

- Project is funded through multiple offices at the VA and requires collaboration from VA Privacy Service, Section 508 team, and newly created SharePoint Governance Board.
Three Key Components

• Set up SharePoint 2010 Model Farm
  – Feed-in to VA Governance
    • This farm will model:
      ✓ Business Requirements that define a range of scenarios in which agencies use SharePoint (i.e. public facing Web sites, doctors sharing calendars, collaboration on draft documents with sensitive information, management of procurement documents pre and post award, etc)
      ✓ Compliance Requirements that explore the various privacy and security regulations that will apply to the business scenarios to determine both if PII PHI SSI should be allowed and, if so, with what kinds of protection and oversight
      ✓ Technical Requirements that determine how Compliance Sheriff together with SharePoint and other Microsoft technologies (RMS, Active Directory, etc) can be applied to automate enforcement and oversight of the compliance requirements

• Add two new SharePoint 2010 sites
• Expand existing MOSS sites
  – Continue to make improvements/Automated notification/Continue scanning of existing sites
Why is Compliance a Challenge

- Diverse set of content contributors
- Content changes all day, every day
  - Documents uploaded / edited
  - Email communications sent
  - Social collaboration through blogs, wikis
  - External and internal website content
  - Documents stored on file shares may have non-compliant content that can create a threat

80 percent of enterprise content is unstructured and growing at 36 percent a year.

- Doculabs
The Migration Opportunity

Mixed Junk IN

Prioritize for Business Need

Filter for Compliance

Structure for Governance

Organized Gold OUT
Make Control Part of the Process

1. Analyze the Current Environment
2. Identify Non-Compliance
3. Prioritize the Business Needs
4. Diagram New Security Boundaries
5. Architect in GovSec
6. Undertake Migration
7. Maintain Control
Conclusion

• Balance with data management and protection
  – Honor data privacy and security policies, laws and regulations
  – Enable enforcement
  – Minimize risk of data loss or misuse
  – Minimize potential impact of data loss or theft
  – Generate proof of effectiveness and execution of data protection policies and measures: Measure compliance
Questions

John Buck, Director, Office of Privacy and Records Management
202-632-7385
john.buck1@va.gov

Dana Louise Simberkoff, JD, CIPP/US, Vice President, Public Sector, HiSoftware, Inc.
1-603-496-0359
danalouise@hisoftware.com
References/Acronyms

- FISMA-Federal Information Security Management Act
- HIPAA-Health Insurance Portability and Accountability Act of 1996
- HITECH-Health Information Technology for Economic and Clinical Health Act
- OIT-Office of Information Technology
- PHI-Protected Health Information
- PII-Personally Identifiable Information
- PO-Privacy Officer
- Section 508-Section 508 of the Rehabilitation Act of 1973 (covers access to electronic and information technology procured by Federal agencies.)
- VA-United States Department of Veterans Affairs
  - VBA-Veterans Benefits Administration
  - Veterans Health Administration
  - National Cemetery Administration
- WCAG 2.0-Web Content Accessibility Guidelines version 2.0 (a guideline available from the World Wide Web Consortium (W3C)