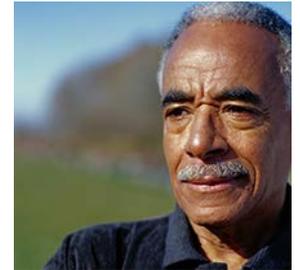


**2015 VA Privacy Matters  
Symposium**

*Opening Session:  
Fostering Stronger  
Working Relationships*



June 9, 2015



**Office of Information Security**  
Privacy and Records Management

# Administrative Items

- Do not use your computer microphone to participate in this meeting. Lync will be used only as a display. Please dial in using the following information:
  - Phone number: 1-800-767-1750
  - Conference ID: 08388
- Please mute your computer microphone and speakers. This will eliminate feedback on the line and make it easier for you and your colleagues to hear the presentation.
- The presenters will address questions at the end of the presentation. For those online, please feel free to type your questions into the Lync Instant Messenger.
- Send technical issues to [VACOPrivacySpeakers@va.gov](mailto:VACOPrivacySpeakers@va.gov).

# Moderator

**LaShaunné David**

Director for VA Privacy Service





# Guest Panelists

## **Ed Grzenda**

Privacy Officer  
Veterans Health Administration  
U.S. Department of Veterans Affairs

## **Erich Fronck**

Regional Information Security Director  
Office of Information Security  
U.S. Department of Veterans Affairs

## **Jeremy Maxwell, PhD**

IT Security Specialist  
Office of the National Coordinator for Health IT  
U.S. Department of Health & Human Services

## **Richard Phillips**

Senior Privacy Analyst  
Office of Privacy Policy and Knowledge Management  
Office of Privacy, Governmental Liaison & Disclosure  
U.S. Internal Revenue Service

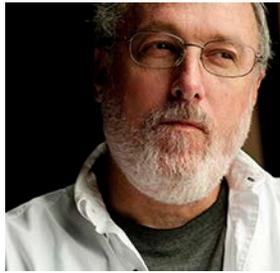


**Ed Grzenda**

*Privacy Officer*

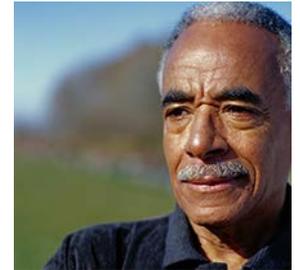
*Veterans Health Administration*

*U.S. Department of Veterans Affairs*



Fostering Stronger  
Working Relationships:  
A Privacy Officer Perspective

Ed Grzenda, Privacy Officer  
Veterans Health Administration  
U.S. Department of Veterans Affairs



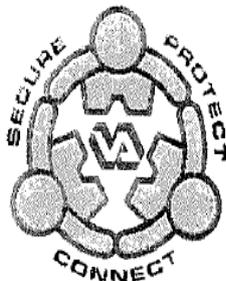
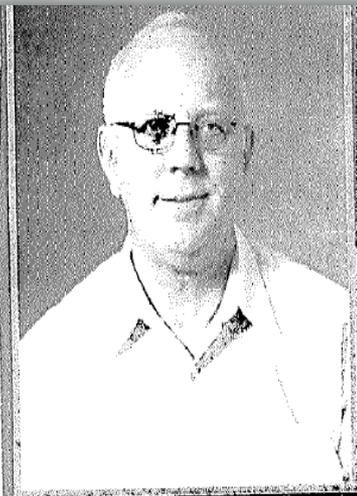
**WANTED**

*For Questioning*



Ed Grzenda  
Coatesville VA Medical Center  
Privacy Officer

*If you see Ed,  
ask him how you can best  
protect the privacy of our  
patients and employees*



VA InfoSec  
**UNITY**  
Together We Make **IT** Happen

# PRIVACY IS EVERYONES BUSINESS

ALWAYS SECURE YOUR COMPUTER & ALL PATIENT &  
EMPLOYEE INFORMATION WHEN YOU ARE NOT USING  
IT REPORT ALL PRIVACY CONCERNS TO THE PRIVACY  
OFFICER AT EXT. 2239



**Edward A. Grzenda, M.S.**  
Privacy/FOIA Officer  
*Privacy is Everyone's Business*



Director's Office (001) 610-384-7711 ext. 2239  
Veterans Affairs Medical Center FAX 610-383-0248  
1400 Blackhorse Hill Road  
Coatesville, PA 19320-2096 edward.grzenda@va.gov

VA Healthcare - VISA 4



People don't care how much  
you know, but they know how  
much you care...  
by the way you listen.

- Bob Conklin

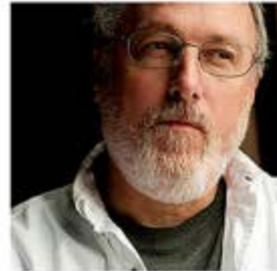


# **Erich Fronck**

*Information Security Director*

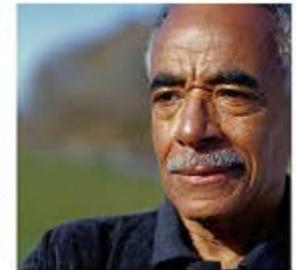
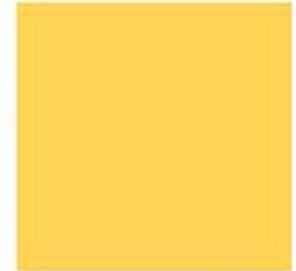
*Office of Information Security*

*U.S. Department of Veterans Affairs*



VA OI&T FIELD SECURITY  
SERVICE (FSS)

Information Security and Privacy



June 2015



**Office of Information Security**  
Field Security Service

# VA Directive 6500

## Establishes the foundation for VA's Information Security and Privacy Program and practices

- Based on NIST 800-53, 800-37, and 800-39
- Appendix E: *Privacy controls*
  - Structured set of controls for protecting privacy
  - VA roadmap for implementation of controls concerning life cycle of Personally Identifiable Information (PII)
- Appendix F: *Security controls*
  - Provides security control baseline

# Information Security Officer

***Responsible to ensure the appropriate security posture is maintained for an Information System and/or Program.***

- Manages Information Security Program and serves as advisor
- Monitors for compliance with Federal security requirements and VA policy
- Collaborates with System Owners and Program staff to verify and validate implementation of security controls
- Assesses Risk

# Privacy Officer

***Responsible for taking proactive measures to ensure that PII collected by VA is limited to that which is legally authorized and necessary; and is maintained in a manner that precludes unwarranted intrusions upon individual privacy.***

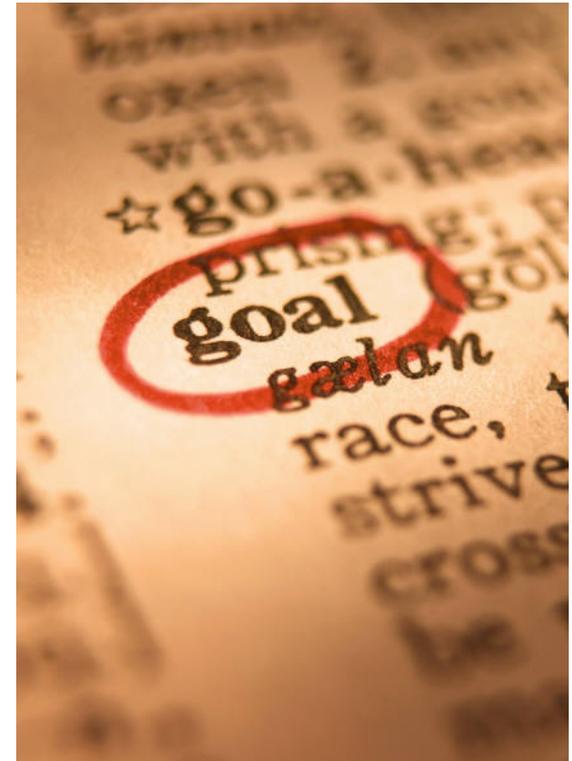
Subject Matter Expert:

- Business Associate Agreement
- System of Records (SORN)
- Data Protection
- Privacy Impact Assessment (PIA)

# Privacy and Security - Common Goals

## Compliance

- Mandatory Training
- Incident Reporting and Response
- Policies and Directives
- HIPAA Security and Privacy Rule
- Contract Security
- Access to Sensitive Information



# Mandatory Training

- New Employee Orientation
  - Complete training prior to receiving system access
  - Understand and sign Rules of Behavior
- Privacy and Security Awareness Training
  - Condition of employment
  - Annual requirement

# Incident Response

- VA Incident Reporting policy
- Support from National Incident Response Team (IRT)
- Incident reports provided to executive level
- Track incidents through closure
- Report policy Violations

# Policies and Directives

- VA Directive 6500 and Handbook Series
- VA Privacy Policy
- FISMA
- Privacy Act
- HIPAA

# Contract Security Requirements

- ISO and PO review the contract with COR
- PO makes a determination regarding sensitive data
- ISO addresses information security requirements
- ISO and PO signature is required

# HIPAA Security and Privacy Rule

- Data Protection and Disclosure
- Physical Security and Privacy
- Access Management
- Encryption
- Personally Identifiable Information (PII)
- Protected Health Information (PHI)

# Access to Sensitive Information

- Least Privilege Rule / Need to Know
- Functional Categories used to identify the appropriate level of access to protected health information
- ISO and PO monitor access to ‘sensitized’ records

# Tools and Resources

- **Privacy and Security Event Tracking System (PSETS)**
  - Centralized Incident Reporting System
  - Shared ISO/PO access to privacy and security tickets
  - Allows for cross-coverage and timely reporting through incident closure

# Tools and Resources (continued)

- **Privacy Threshold Analysis (PTA)**
  - For use by PO, ISO, system owners and other stakeholders to determine whether a VA program, project, or IT system has privacy implications, and if additional privacy documentation is required, such as a Privacy Impact Analysis
- **Privacy Impact Analysis (PIA)**
  - Demonstrates that system owners have incorporated privacy protections throughout the system lifecycle.

# Best Practices

- **Establish a Team**
  - Privacy Officer, Information Security Officer, and Chief Information Officer/System Owner
- **Engage with Leadership**
  - Obtain management support
- **Communicate**
  - Share information



# Best Practices – Incident Response

## Centralized Incident Tracking

- Maintain privacy and security incidents in a single database
- Timely Mitigation
- Executive level Awareness
- Encourages ISO and PO cross coverage

# Best Practices - ISPAW

## **Information Security and Privacy Awareness Week**

Annual event fostering awareness and engages all levels of staff

## **ISO and PO Collaboration**

Team effort to communicate privacy and security information

# What did we learn?

## Continuous Readiness in Information Security Program (CRISP)

- Top-Down Approach
- Continuous Monitoring
- Accountability



# Information Security and Privacy Portal

Site Actions | Browse | Page | Home - OIS Portal Home | Angeli, Chafica (Network 02 ISO)

UNITED STATES DEPARTMENT OF VETERANS AFFAIRS  
Office of Information Security Portal

OIS Portal Home | Projects | This Site: OIS Portal Ho

Welcome to the OIS Portal!

## The revamped *IS Update* is here! For all the latest OIS news and info, [CLICK HERE](#)

**OIS Portal Quick Links**

- Information Security & Privacy Awareness Week
- Business Continuity
- Business Office
- OIS Communications
- Cyber Security
- Enterprise Security Solutions Service
- Field Security Service
- Front Office
- ISO PO Locator
- IT Workforce Development
- Risk Management & Incident Response
- Privacy
- VA-Network and Security Operations Center
- Ask the ISO

[All Site Content](#)

**OIS Portal Latest Announcements**

**OI&T Contact Referral Card** 2/10/2015 1:41 PM  
by Christopher, Daron J. (BAH)

If someone calls you asking about VA's Office of Information & Technology, do you know to whom you should refer them? Take a look at the image on the left, which outlines the various points of contact that inquiring individuals should be directed...

**VA Migration to Internet Explorer 11** 10/2/2014 3:17 PM  
by Christopher, Daron J. (BAH)

VA will upgrade all VA government furnished equipment desktop and laptop computers to Internet Explorer 11 starting in the December – January timeframe. All users should be upgraded by March 2015. Read more at [OI&T 360](#).

**Announcing ProPath: Release 21.0 - STD WBS** 10/1/2014 11:38 AM  
by Christopher, Daron J. (BAH)

The Standardized Work Breakdown Structure (STD WBS) template has been updated to reflect the changes implemented with release 21 of ProPath. The STD WBS can be found in Primavera under project name "STD WBS ProPath r21". It is also available in MS...

**Announcing ProPath: Release 21.0** 9/17/2014 2:26 PM  
by Christopher, Daron J. (BAH)

Process Management (PcM) is pleased to announce the publication of **ProPath Release 21.0**. This release is very large and contains a number of updates. Please read the release announcement in its entirety, but note a few key updates in particular:

-

**Update - ProPath: Release 20.5** 8/26/2014 1:32 PM  
by Christopher, Daron J. (BAH)

The Standardized Work Breakdown Structure (STD WBS) template has been updated to reflect the changes implemented with release 20.5 of ProPath. The STD WBS can be found in Primavera under project name "STD WBS ProPath r20-5". It is also available in MS...

**Information Security Resources**

**OIS INFO TO KNOW**

**CRISP**

**VA Handbook 6500**  
VA INFORMATION SECURITY PROGRAM

**GRC Project Site**

**Agilience RiskVision**

**Important Links**

- Other Important Links
- RiskVision GRC Tool Project Site
- OIS DAS Memoranda
- OI&T 360 Blog
- OI&T Intranet Homepage
- Information Security Update Newsletters
- Information Security and Privacy Awareness Week
- Leadership Bios
- OIS Templates
- OIS Events Calendar
- VA PKI
- VA Talent Management System

(More Links...)

# Portal Highlights

- [ISO PO Locator](#)
  - Central location for Information Security Officer and Privacy Officer contact information
- [Field Security Service \(FSS\)](#)
  - VA-wide Information Security program overview, resources, and major ISO activities
- [Privacy Service](#)
  - VA-wide Privacy program overview and resources
- [VA-Network and Security Operations Center](#)
  - Provides technology and services necessary to maintain secure operations and maintenance of VA's Enterprise Network
- [Ask the ISO](#)
  - FSS program that encourages communication with the ISO community and documents questions and responses for future reference



# **Richard Phillips**

*Senior Privacy Analyst*

*Office of Privacy Policy and Knowledge Management*

*Office of Privacy, Governmental Liaison & Disclosure*

*U.S. Internal Revenue Service*



## **Privacy and Security**

*Hand-In-Hand Collaboration at IRS*

**Richard W. Phillips**

**Office of Privacy Policy & Knowledge Management**

**Office of Privacy,  
Governmental Liaison & Disclosure**

# Privacy and Security Working Together

## Security and Privacy: *Mutual Support*

Security  
protects  
information  
and systems



Privacy  
ensures  
personal data  
is used  
appropriately



# Some Common Business Objectives

Privacy	Intersecting Objectives	Security
Through PCLIAAs, Business PII Risk Assessments	Manage Risk	Implement NIST security risk assessments
Unauthorized Access Prevention Program	Access Control	Audit Trails, Access Controls
Ensure PII is accurate, timely, complete	Data Reliability	Protect data's integrity
Ensure authorized collection, enforce proper records disposition	Minimization	Media sanitization controls, synthetic data
Mitigate PII breaches	Incident Management	Respond to security incidents
Ensure control on personal data used for ID-proofing	Authentication	Ensure fail-safe system for authentication



# Current Privacy/Security Initiatives at IRS

## Policy

- Cybersecurity and Privacy review each other's policy updates

## Training

- Collaboration on annual all-employee Information Protection Mandatory Briefing
- Collaboration on improved security, privacy, and disclosure training for Contracting Officer Representatives (COR)

## Unauthorized access (UNAX) detection and prevention

- Cyber implements access controls, Privacy manages prevention program

## System Authority To Operate (ATO)

- Cyber and Privacy collaborate to ensure ATO



# Current Privacy/Security Initiatives at IRS

## Reporting

- FISMA, other Treasury and OMB reporting

## Strategic Breach Management

- Collaborate through the Threat and Incident Response Center (TIRC)

## Risk Management

- Assist each other's risk management

## Governance

- Privacy and Security Executive Steering Committee and Advisory Board
- Privacy and Cybersecurity Governance Board oversees joint projects
- SBU Usage for Testing purposes
- Oversight of electronic Risk Assessment for online authentication per OMB M-04-04

# Collaboration Strategies

Create ongoing means of communication

- Regular meetings and conferences
- Ensure inclusiveness on projects

Document goals and objectives upfront

- Utilize NIST, OMB, and Federal CIO Council guidance

Cross-functional assignments with personnel

- Privacy staff temporarily assigned to Cyber and vice versa



# New Opportunities for Tighter Collaboration

## Implementation of NIST Privacy Controls

- AR-7 Privacy Enhanced System Design and Development
- DI-2 Data Integrity and Data Integrity Board
- SE-1 Inventory of PII

## NIST Privacy Risk Management Framework

- *Currently in draft*



Richard W. Phillips, CIPP/G/US, CIPT  
Senior Privacy Analyst  
Office of Privacy Policy & Knowledge Management  
Privacy, Governmental Liaison and Disclosure

[richard.w.phillips@irs.gov](mailto:richard.w.phillips@irs.gov)

Department of the Treasury  
**Internal Revenue Service**  
[www.irs.gov](http://www.irs.gov)

# Guest Panelists Q&A

## **Ed Grzenda**

Privacy Officer  
Veterans Health Administration  
U.S. Department of Veterans Affairs

## **Erich Fronck**

Information Security Officer  
Office of Information Security  
U.S. Department of Veterans Affairs

## **Jeremy Maxwell, PhD**

Security Analyst  
Office of the National Coordinator for Health IT  
U.S. Department of Health & Human Services

## **Richard Phillips**

Office of Privacy Policy and Knowledge Management  
Office of Privacy, Governmental Liaison & Disclosure  
U.S. Internal Revenue Service

# Thanks for Attending!

- Thank you for attending the 2015 VA Privacy Service “Privacy Matters” Symposium.
  - We value your feedback, opinions and comments!
  - After this session, you will receive a short questionnaire via email. Please take a moment to complete upon receipt.
- To self-certify Lync Meeting attendance in the Talent Management System (TMS), search:

**Item Title:** VA Privacy Symposium 2015: Opening Session – Fostering Stronger Working Relationships (Live Webinar)

**TMS ID:** VA 3941722

- Visit the new VA Privacy Service website at <http://www.oprm.va.gov> to learn more about Privacy within VA.