Healthcare Security: Assessing the Third Party Risk

This webinar is generously sponsored by:

PREVALENT®
Healthcare SIG Webinar Contributors

Stephen Fitton
  Information Security Officer - Clinicient, Inc.

Karen McMillen, CISSP
  Security Analyst - Asante

Andrew Reeder, CISA, CISM, CISSP
  Director, Privacy & Security – Rush University Medical Center

Roy Wattanasin, CSSLP
  Information Security Officer – MITM
“A chain is no stronger than its weakest link, and life after all is a chain.”

- William James
Discussion Points

Third Party Risk Assessments (TPRA):

- Some History
- What is a TPRA?
- Why So Important Now?
- Where and When to Use Them
- Examples/Types
- How to Manage Them
- Who Can Help
Some Relevant History

- **Evolution of Healthcare Patient Care Model**
  - Focus from Acute Care to Continuum of Care
  - Electronic - Medical Record AND Medical Devices
  - Evidenced Based: Metrics and “Big Data” management
  - Individuals Rights: Use, Disclosure, and Access to Their Data

- **Associated Evolution of HIT model**
  - Wide Scope of Data Sharing - The data “supply chain”
  - Networked Medical Systems – and life- supporting medical devices
  - Very Large Stores of Sensitive Data
  - Emphasis on Privacy and Security

- **And HIT must Follow the Evolution of Global IT**
  - Commoditized - BYOD
  - Online, Collaborative – Outsourcing and Cloud Technology
  - Mobile – eMR on your iPhone
  - Virtualized – Telemedicine and “virtual hospitals”
What is a “Third Party”?

For our purposes, a “third party” is an outside entity with access or controls to Enterprise systems and/or data and may provide a service to an organization.

Examples include:

- Business Associates AND other entities which provide functions or activities for the organization
  - Business Partners
  - Contractors
  - Vendors
  - Cloud Services
  - Other Managed Service Providers (e.g., transcription services)
What is a Third Party Risk Assessment (TPRA)?

- A documented assessment of a third party’s information security risk profile

  Derived from one or more of the following:
  - Security control documentation/checklists
    - Standardized Information Gathering (SIG)
  - Facility walkthrough Verification
    - E.g. Contract Agreed Upon Procedures (AUP)
  - Staff Interviews
  - Security Testing
    - website and system scan results
    - System configuration and log reports
  - External Audit Reports (SSAE 16, etc.)
Why are TPRAs Important?

- Regulatory Requirement - Risk Assessments
  - OCR will investigate and can penalize cases of “willful Neglect”

- Stakes are High
  - 70% of reported breaches are from Business Associates
  - Patient dependence on systems - loss of availability risk

- Increased Use and Dependency Upon TPs
  - Cloud Migration and outsourcing
  - Response to paradigm shift: *Infrastructure security model vs. data-centric security model*

- Business Associate agreements is usually not specific enough for litigation
  - A signed BAA does not protect Covered Entities and Business Associates from liability.

**BOTTOM LINE:** TPRAs must be a key element of any Security Program.
HIPAA Security Rule - Includes requirements for Administrative, Technical, and Physical safeguards which are either Required or Addressable. The conduct of a Risk Assessment is required and found under the Administrative Standards of “Security Management Process” (CFR 164.308 (a)(1)(i)) and “Evaluation” (CFR 164.308(a)(8))


Federal and State requirements - Typically don’t define HOW to conduct an risk assessment; only that one be accomplished. A TPRA can be considered a best practice and should be part of ongoing risk assessment activities.

Checking for the existence of Security Risk Assessment efforts is included in the audit program of the Office for Civil Rights.
Also – Industry Requirements

Examples:

**PCI 3.0**

12.8.2 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.

**ISO**

Required for ISO 27001 Information Security Certification

**NIST**

SP 800-39 Managing Information Security Risk

A *key component of NIST compliance*
The TPRA Conundrum

- Lack of Consistent or Standard Templates, Content & Methodology

- Different Vulnerability and Control Types According to Object of Review
  - Application – company hosted
  - Cloud Services - SaaS, PaaS and IaaS
    - Cloud Security Alliance - Cloud Control Matrix (CCM)
  - Medical Devices - MDS2
    - Manufacturer Disclosure Statement Medical Device Security form
  - Healthcare Services – e.g., Transcription Services
  - Mobile Device Controls
  - SSAE 16 and other third party risk assessments
TPRA Support & Tools
You Don’t Have to Create Your Own!

Well Known Framework Controls & Questionnaires:

NIST, HITRUST, ISO, PCI

Shared Assessment Program (est. 2005):
Standardized and objective vendor assessment methodology
Member input and annual review of tools

International Computer Alliance Security (ISAC):
In response to 1998 UK Data Protection Act (DPA). Categories of assessment according to third party type/size

CIS – Center for Information Security “Benchmarks”
Platform specific security control baseline recommendations

GOOGLE – Scalable Vendor Security Reviews: VSAQ Framework

Vendor Shared Assessment Programs – Industry-specific offerings
# TPRA Example 1

## Cloud Security Alliance Cloud Controls Matrix

<table>
<thead>
<tr>
<th>Control Domain</th>
<th>CCM V3.0 Control ID</th>
<th>Updated Control Specification</th>
<th>Architectural Relevance</th>
<th>Corp Gov Relevance</th>
<th>Cloud Service Delivery Model Applicability</th>
<th>Supplier Relationship</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datacenter Security</td>
<td>DCS-08</td>
<td>Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Unauthorized Persons Entry</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Datacenter Security User</td>
<td>DCS-09</td>
<td>Physical access to information assets and functions by users and support personnel shall be restricted.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption &amp; Key Management</td>
<td>EKM-01</td>
<td>Keys must have identifiable owners (i.e., keys to justify) and there shall be key management policies.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Encryption Entitlement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption &amp; Key Management</td>
<td>EKM-02</td>
<td>Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., key lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility or implementation of the control.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Key Generation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption &amp; Key Management</td>
<td>EKM-03</td>
<td>Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Sensitive Data Protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
TPRA Example 2
Medical Device

Manufacturer Disclosure Statement for Medical Device Security – MDS²

<table>
<thead>
<tr>
<th>Device Category</th>
<th>Manufacturer</th>
<th>Document ID</th>
<th>Document Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diagnostic Viewing and Processing System</td>
<td>102120</td>
<td>V1.0</td>
<td>1st April 2015</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Device Model</th>
<th>Software Revision</th>
<th>Software Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>IntelliSpace Portal Server</td>
<td>R7.0.0</td>
<td>1st April 2015</td>
</tr>
</tbody>
</table>

Intended use of device in network-connected environment:
The Philips IntelliSpace Portal is an enterprise solution that delivers advanced imaging and analysis capabilities in a thin client-server architecture. It processes clinical images from different modalities and enables advanced visualization of the images. When used by qualified personnel, it provides useful diagnostic information. IntelliSpace Portal can be used remotely by multiple users with compatible devices. The client and server communicate normally through a local area network (LAN). The server provides storage and query/retrieve capabilities for multiple modality images to and from imaging systems and PACS. The IntelliSpace Portal Management Tool provides configuration and maintenance services such as user management and DICOM connectivity.

MANAGEMENT OF PRIVATE DATA

Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
<th>See Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Can this device display, transmit, or maintain private data (including electronic Protected Health Information [ePHI])?</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B Types of private data elements that can be maintained by the device:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B.1 Demographic (e.g., name, address, location, unique identification number)?</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B.2 Medical record (e.g., medical record #, account #, test or treatment date, device identification number)?</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B.3 Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B.4 Open, unstructured text entered by device user/operator?</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B.5 Biometric data?</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B.6 Personal financial information?</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C Maintaining private data - Can the device:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C.1 Maintain private data temporarily in volatile memory (i.e., until cleared by power-off or reset)?</td>
<td>Yes</td>
<td>Yes</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>C.2 Store private data persistently on local media?</td>
<td>Yes</td>
<td>Yes</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>C.3 Import/export private data with other systems?</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C.4 Maintain private data during power service interruptions?</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D Mechanisms used for the transmitting, importing/exporting of private data – Can the device:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D.1 Display private data (e.g., video display, etc.)?</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D.2 Generate hardcopy reports or images containing private data?</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D.3 Retrieve private data from or record private data to removable media (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick, etc.)?</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D.4 Transmit/receive or import/export private data via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire, etc.)?</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note:

- Yes
- No
- N/A
- See Note
**TPRA Example 3**

**SharedAssessments.com - SIG**

### SIG Lite

<table>
<thead>
<tr>
<th>Question/Request</th>
<th>Response</th>
<th>Additional Information</th>
<th>AUP Reference</th>
<th>ISO Ref Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Have the policies been reviewed in the last 12 months?</td>
<td></td>
<td></td>
<td>B.1 Procedure: d</td>
<td>Review of the policies for information security</td>
</tr>
<tr>
<td>Is there a vendor management program?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there a respondent information security function responsible for security initiatives?</td>
<td></td>
<td></td>
<td>C.3 Security Organization Roles/Responsibilities</td>
<td>Information Security Roles and Responsibilities</td>
</tr>
<tr>
<td>Do external parties have access to Scoped Systems and Data or processing facilities?</td>
<td></td>
<td></td>
<td></td>
<td>Supplier relationships</td>
</tr>
<tr>
<td>Is there an asset management policy or program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?</td>
<td></td>
<td></td>
<td>D. Assessment Management: 8.1</td>
<td>Responsibility For Assets</td>
</tr>
<tr>
<td>Are information assets classified?</td>
<td></td>
<td></td>
<td>D.1.c.6</td>
<td>Classification of information</td>
</tr>
</tbody>
</table>

### C. Organizational Security

### D. Asset Management

### E. Human Resource Security

### Healthcare Security: Assessing Third Party Risk
TPRA Example 4
Website Scan
Managing the TPRA Process

- Know where Your Third Parties Are
  - Begin with your Contracts & Purchasing Departments
  - Network Scans help locate non-inventoried vendor systems

- Begin with Education
  - Executive
  - Enterprise Policies & Procedures
  - Targeted Departments (e.g., Purchasing, Legal, PMO)

- Create Appropriate Business Processes/Work Flows
  - Capital Purchase Request notification to IT Security
  - Clinician Education of vendor security requirements

- Develop or Purchase Tools
  - Assessment templates (surveys, checklists)
  - GRC database/reporting

- Obtain Sufficient Staffing to Support TPRA
  - Part of Management Education Process
  - Vendor Support Becoming Available
The Vendor Risk Management Maturity Model (VRMMM)

- Three Components:
  - Program Definition, Execution and Management
- Five Levels of Proficiency/Maturity
- Provides a Good Roadmap for Improvement
- Provides a Good Management Reporting Tool

And what is your VRMMM rating?
Other Points to Consider

- **Remember that all data has a lifecycle**
  Address destruction or return of data from Business Associates after the contract ends

- **Ask your Business Associates** how they perform due diligence on securing THEIR Business Associates as well
  
  “...an upstream entity will be in violation of the regulations if it “knows” of “a pattern of activity or practice” which “constitutes a material breach or violation” of the Business Associate Contract, and fails to either take “reasonable steps to cure the breach,” or terminates the contract. “


- **Ask your Legal Department** how your vendor contracts address security requirements beyond the BA – e.g, is the contract void if the vendor does not fulfill its security agreement?

- **Cyber Insurance** Do your Executives expect cyber Insurance to cover third party breaches? Will it?
Summary

- TPRA have become a key element of any Information Security Program. *Lack of a TPRA program = risk*
- TPRA have grown out of the changes in Healthcare Model, HIT and global IT trends.
- TPRA are required for HIPAA compliance.
- TPRA management requires management education and the development of internal and external business process.
- TPRA best practices and standards are still evolving.
- Industry Support and third party security management niche vendors are developing – but growing!

*Pay Attention to What’s Going On. It’s important.*
Guest Speaker & Panelist

Jonathan Dambrot, CEO/Co-Founder Prevalent, Inc.

Jonathan is the CEO and Co-Founder of Prevalent. He has spoken on the need for third-party risk management at the leading industry events including RSA, Shared Assessments Summit, ISACA, ISSA, Infragard, NYSE, and others. Jonathan also helped develop the Risk Assessment Body of Knowledge (RABOK) as part of the development of Shared Assessments efforts to develop the first of its kind certification for third-party risk professionals (CTPRP).

Jonathan is currently the Chair of the Shared Assessments Steering Committee, Former Chair of the Shared Assessments SIG Committee, and sits on the Penn State Outreach Advisory Board.

Prior to working in the technology industry, Jonathan launched a highly successful, consumer products company where he won several collegiate entrepreneurial awards. Jonathan is a graduate of Fairleigh Dickinson University, received his MBA from The Pennsylvania State University, is a Certified Third-Party Risk Professional (CTPRP), and a Certified Information Systems Security Professional (CISSP).

Prevalent is a leader and industry visionary in third-party risk management and threat intelligence monitoring. They have revolutionized the way organizations manage and monitor their 3rd and 4th party vendor relationships and they recently introduced Prevalent Synapse – the first Unified third-party risk assessment, threat monitoring and collaboration platform.
Only 26% of respondents say the process they use to assess third party risk is effective.

56% of respondents say they do NOT know what IP and other high value "crown jewels" are in the hands of third parties.

75% of respondents consider 3rd Party Risk serious & increasing, while 70% say that 3rd Party Risk is SIGNIFICANTLY INCREASING.
A Unified Platform

The First Unified Third-Party Risk Assessment, Threat Intelligence & Collaboration Platform

ASSESSMENT  THREAT INTELLIGENCE  COLLABORATION
The Synapse Approach

• Current methods focus on a one-to-one relationship model
• Synapse approach focuses on scale, automation, and leveraged content to build a third-party assessment ecosystem that continuously grows
Synapse Use Cases

1. **Enterprise Networks**
   - **Example: PayPal** - automate processes, reduce costs & scale to a large number of global vendors using the Synapse approach.

2. **Vertical Networks**
   - **Example: Legal Vendor Network** - top global law firms have standardized assessment & continuous monitoring using the Synapse approach.

3. **Service Provider Networks**
   - **Example: Ellie Mae** – enabling Ellie Mae vendors and partners to provide third and fourth-party visibility to clients.
Vertical Network Example

Healthcare network coming soon!

• What is Legal Vendor Network?
  • A membership-based program designed for law firms to assess and monitor 3rd party vendors for security and data risk

• What are the Benefits?
  • Vendor Repository in Prevalent’s Vendor Risk Manager
  • Scaled to assess vendors of all sizes; 2 person to 100,000 person vendors
  • Mechanism to determine whether other firms use vendor
  • Pre-Assessment to determine vendor importance and leveling
  • Threat intelligence and network sharing available to all members
PANEL Q & A