A Practical Guide to Privacy Risk Assessment
October 1, 2013
A PRACTICAL GUIDE TO PRIVACY RISK ASSESSMENT
SESSION OBJECTIVES

- Identify your data privacy risk factors.
- Understand the key attributes and what it takes to perform a privacy risk assessment.
- Learn how to conduct and leverage the results of a privacy risk assessment.
- Learn basic Lean Six Sigma tools to evaluate effectiveness of your HIPAA risk assessment program.
INTRODUCTIONS

Eric Dieterich  
Partner  
Sunera LLC  
edieterich@sunera.com  
(786) 390-1490

Janice Schuck  
Chief Privacy Officer  
Clinical Research Administrator  
Holy Cross Hospital  
janice.schuck@holy-cross.com  
(954) 776-3239
We will have Live Voting throughout the session.

- Participation is optional.
- Voting results are anonymous.
- Can TEXT or submit response at:

HTTP://POLLEV.COM/DataPrivacy
Short video clip showing how one little event may lead to a much larger issue.
POLL QUESTION

Has your organization performed a privacy risk assessment in 2013?

- (A) Yes – Standalone Privacy Risk Assessment
- (B) Yes – As Part of a Security Risk Assessment
- (C) Yes – As Part of a Enterprise Risk Assessment
- (D) Yes – Some Combination of Above
- (E) No
Data privacy risks revolve around the inappropriate or unauthorized collection, use, retention, and disclosure of data.

Data privacy risk factors may include:

1. Legal
2. Reputation
3. Operational

Increasing focus on business sensitive information.

“Digital intruders are increasingly targeting information about high-stakes business deals -- from mergers and acquisitions to joint ventures to long-term supply agreements -- and companies routinely conceal these breaches from the public, say government officials and security companies.”

Bloomberg, November 4, 2012
POLL QUESTION

- Has your organization had a reportable breach in 2012 or 2013?
  - (A) Yes
  - (B) No
DATA PRIVACY RISK ASSESSMENT – UNDERSTANDING THE INFORMATION LIFE CYCLE

■ Defining
  – Understand how personal information is collected, processed, stored, and shared throughout the organization.

■ Importance
  – Evaluation of data privacy risk factors.
  – Review the implementation of policies, procedures, and controls that will reduce the complexities, and risks.

■ Strategy
  – Understand the risks around how and where information flows through all business processes.
  – A risk mitigation plan can be developed to ensure personal information is protected throughout the information life cycle.

www.privacyassociation.org
POLL QUESTION

Does your organization have an understanding of the information life cycle for personal and/or business sensitive information?

- (A) Very Limited.
- (B) Some definition of the life cycle for personal information.
- (C) Some definition of the life cycle for business sensitive information.
- (D) Some definition of the life cycle for personal and business sensitive information.
- (E) A high degree of understanding of personal and business sensitive information throughout the organization.
**Key Risk Assessment Activities**

- **Identification** and **understanding** of key business processes that are involved in the collection, processing or storage of personal information.

- Creation of a **risk catalog** for the key business processes.

- An overall **inherit risk** profile is scored for each key process.

- The identification and evaluation of **mitigation techniques** are evaluated leveraging a catalog of **illustrative controls**.

- An overall **residual risk score** for each key process is calculated helping to identify areas of data privacy risk across the enterprise.

- The results can drive the **definition of a roadmap** to mitigate the privacy risks.
**Process Based Analysis**

- Each area of data privacy risk is analyzed by business unit, process and/or sub-process.

<table>
<thead>
<tr>
<th>Elec. PII Risk Process No.</th>
<th>Business Unit</th>
<th>Process</th>
<th>Process Description</th>
<th>PII Data Elements</th>
<th>Inquiry</th>
<th>Vendor</th>
<th>Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Human Resources</td>
<td>New Applicant</td>
<td>Each applicant submits contact detail with work history, criminal history (voluntary) and a copy of a resume. A skills assessment, if required, is completed on the Connect Approver site, Profile XT Assessment and is only used for senior level positions. Only the name and mailing address of the applicant are sent back to the applicant. No PII is sent to the applicant prior to the interview, only informational brochures.</td>
<td>Applicant Information</td>
<td>John Smith</td>
<td>Success Factors</td>
<td>PictureSaver</td>
</tr>
</tbody>
</table>
DATA PRIVACY RISK ASSESSMENT – DEFINING THE RISK CRITERIA

- Four key “buckets” of risk criteria
  1. Electronic Privacy Risks
  2. Application Privacy Risks
  3. Vendor Privacy Risks
  4. Paper File Privacy Risks

- The risk criteria buckets can be added or changed depending on the industry or focus of the risk assessment
## Electronic Privacy Risks

<table>
<thead>
<tr>
<th>#</th>
<th>Risk Factor</th>
<th>Risk Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>R-01</td>
<td>Inappropriate notice provided during collection of PII</td>
<td>A person is not informed or misinformed about the intended use or purpose of PII collected which may lead to non-compliance with stated policies or regulatory standards.</td>
</tr>
<tr>
<td>R-02</td>
<td>Over collection of PII</td>
<td>The PII collected is not required for the intended business activity which increases the exposure during a breach.</td>
</tr>
<tr>
<td>R-03</td>
<td>Inappropriate use of PII</td>
<td>The misuse of PII other than for the purpose stated during collection maybe lead to non-compliance with stated policies or regulatory standards.</td>
</tr>
<tr>
<td>R-04</td>
<td>Inaccurate PII</td>
<td>The PII collected is not accurate, complete or relevant which may lead to inappropriate business actions.</td>
</tr>
</tbody>
</table>
### Application Privacy Risks

<table>
<thead>
<tr>
<th>#</th>
<th>Risk Factor</th>
<th>Risk Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>R-11</td>
<td>Unauthorized administrative access</td>
<td>Personnel may be granted unauthorized access or excessive, inappropriate privileges to PII.</td>
</tr>
<tr>
<td>R-12</td>
<td>Non-unique system accounts</td>
<td>Access to systems may not be traceable to a unique individual in the case of inappropriate disclosure, misuse, alteration, or destruction of PII.</td>
</tr>
</tbody>
</table>

### Vendor Privacy Risks

<table>
<thead>
<tr>
<th>#</th>
<th>Risk Factor</th>
<th>Risk Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>R-24</td>
<td>Insecure electronic transfer of PII to vendors</td>
<td>PII stored at or transferred to a vendor are more susceptible to inappropriate disclosure, alteration or destruction.</td>
</tr>
</tbody>
</table>
DATA PRIVACY RISK ASSESSMENT – DEFINING THE RISK CRITERIA

Paper File Privacy Risks

<table>
<thead>
<tr>
<th>#</th>
<th>Risk Factor</th>
<th>Risk Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>R-16</td>
<td>Unsecured paper files containing PII</td>
<td>Paper documents containing PII are not securely maintained or disposed of which may lead to unauthorized disclosure, misuse, duplication, or destruction.</td>
</tr>
<tr>
<td>R-17</td>
<td>Inappropriate disposal methods</td>
<td>Inappropriate disposal may lead to unauthorized access of PII.</td>
</tr>
<tr>
<td>R-18</td>
<td>Incomplete or insufficient training</td>
<td>Inadequately trained or misinformed business users may inappropriately access, store, or transmit PII.</td>
</tr>
</tbody>
</table>
POLL QUESTION

Where do you believe your organization has the greatest number of data privacy risk factors?

- (A) Electronic Privacy Risks
- (B) Application Privacy Risks
- (C) Vendor Privacy Risks
- (D) Paper File Privacy Risks
- (E) Other
DATA PRIVACY RISK ASSESSMENT – EVALUATING INHERENT RISKS

- For each department, process or sub-process, the inherent risks needs to be evaluated.

- The risk criteria should be defined specific for your organization, ensuring the criteria address all relevant data privacy risks including both paper and electronic.

- The matrix below identifies how the inherent risk could be scored for each risk and unique vendor or application specific risks.

<table>
<thead>
<tr>
<th>Type of NPI (Multiplier)</th>
<th>Pervasive (Additive)</th>
<th>Vulnerability (Additive)</th>
<th>R-01</th>
<th>R-02</th>
<th>R-03</th>
<th>R-04</th>
<th>R-05</th>
<th>R-06</th>
<th>R-07</th>
<th>R-08</th>
<th>R-09</th>
<th>R-10</th>
<th>Vendor Risks</th>
<th>Application Risks</th>
<th>Overall Inherent Risk Score</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>5</td>
<td>-</td>
<td>-</td>
<td>9.3</td>
</tr>
</tbody>
</table>

www.privacyassociation.org
DATA PRIVACY RISK ASSESSMENT – EVALUATE RISK MITIGATION TECHNIQUES

- Through the discovery sessions, you should also attempt to identify any risk mitigation techniques that are in place for each data privacy risk.

- Leveraging a catalog of illustrative controls can assist with the identification of appropriate risk mitigation techniques.

<table>
<thead>
<tr>
<th>#</th>
<th>Illustrative Control Name</th>
<th>Illustrative Control Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C-01</td>
<td>Inappropriate notice provided during collection of PII</td>
<td>Privacy policies and procedures are reviewed and compared to the requirements of applicable laws and regulations at least annually and whenever there are changes to such laws and regulations. Privacy policies state the intended business purpose and use of PII collected where appropriate. Individuals are informed about how they may obtain access to their PII to review, update, or correct the information.</td>
</tr>
<tr>
<td>C-02</td>
<td>Inappropriate use of PII</td>
<td>The entity limits the use of PII to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains PII for only as long as necessary to fulfill the stated purpose or as required by law or regulatory statute, and thereafter appropriately disposes of such information.</td>
</tr>
</tbody>
</table>
A **risk mitigation score** can be assigned including the ability to assign different scores based on the level of certainty that the risk mitigation technique is operating effectively.

The matrix below shows how a risk mitigation technique may be used to lower the inherent risk for each privacy risk factor.

<table>
<thead>
<tr>
<th>C-01</th>
<th>C-02</th>
<th>C-03</th>
<th>C-04</th>
<th>C-05</th>
<th>C-06</th>
<th>C-07</th>
<th>C-08</th>
<th>C-09</th>
<th>C-10</th>
</tr>
</thead>
<tbody>
<tr>
<td>D</td>
<td>E</td>
<td>D</td>
<td>E</td>
<td>D</td>
<td>E</td>
<td>D</td>
<td>E</td>
<td>D</td>
<td>E</td>
</tr>
</tbody>
</table>

| 3    | 3    | 3    | 3    | 3    |      |      |      |      |      |
Taking into account the inherent risk ranking and risk mitigation techniques, an overall residual risk score can be calculated.

The matrix below identifies how the overall data privacy risk score can be calculated.

The overall residual risk score is a key factor in defining a roadmap that helps lowers the data privacy risks identified throughout the enterprise.

### DATA PRIVACY RISK ASSESSMENT – EVALUATE RESIDUAL RISK

<table>
<thead>
<tr>
<th></th>
<th>R-01</th>
<th>R-02</th>
<th>R-03</th>
<th>R-04</th>
<th>R-05</th>
<th>R-06</th>
<th>R-07</th>
<th>R-08</th>
<th>R-09</th>
<th>R-10</th>
<th>Vendor Risks</th>
<th>Application Risks</th>
<th>Average Residual Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Residual Risk</td>
<td>-</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>5.0</td>
</tr>
</tbody>
</table>

www.privacyassociation.org
Managing HIPAA Using Lean Six Sigma
WHAT IS SIX SIGMA??

- Lean Six Sigma – approach focused on improving quality, reducing variations and eliminating waste in an organization.
- Originated – Toyota Motor Corporation in the 1970’s in response to the energy crisis.
- Six Sigma tools uncover what you don’t know.
- A symbol of quality.
WHERE TO BEGIN

- **Define** - the project(s), the goals, and the deliverables to customers (internal and external).
- **Measure** – current performance of the process.
- **Analyze** – and determine the root cause(s) of the defects.
- **Improve** the process problems and their root causes; identify waste and non-value added activities.
- **Control** mechanisms; create procedures and training for new improvements.
WHAT IS IT THAT YOU DO AND DON’T KNOW?

- HIPAA regulatory compliance and workforce understanding is a requirement under federal guidelines – we know
- Workforce receive initial HIPAA training at hire and throughout the year - we know
- HIPAA requires on-going education but does not specify how often or what format – we know
- HIPAA reminders are provided periodically and special training is provided, as needed – we know
- Management is provided additional teaching material to share throughout the year and submission of evidence of training is required – we know

“The height of insanity is doing things the same way and hoping for a different result.”

www.privacyassociation.org
WHAT IS IT THAT YOU DO AND DON’T KNOW?

- Management’s submission of evidence of training needs to be consistent – we know
- Random site audits are performed to determine possible violations – we know
- Random electronic audits are performed to determine unauthorized access to PHI – we know
- Measuring Workforce understanding of HIPAA regulations is necessary and determined through reported incidents and general observation – we know and we don’t know
What is Six Sigma?

- (A) A methodology to help an organization achieve and maintain compliance.
- (B) An approach focused on improving quality, reducing variations and eliminating waste in an organization.
- (C) A method to monitor Workforce performance.
THE PROJECT CHARTER

- Project Name
- Project Overview
- Problem Statement
- Customers/Stakeholders
- What is Important to These Customers – Critical to Quality
- Goal of the Project
- Scope Statement
- Projected Financial or Other Benefit(s)
Understanding Subject Matter
- Measured through random audits
- Direct observation
- Local reporting of possible violations

Quality of Material Provided
- Survey Management
Communication Process Flow

CPO
- Monitor HIPAA Regulations and Current Events
- Identify relevant information
- Generic Information?
  - Yes: See A
    - Send HIPAA Alert via e-mail to “Everyone”
  - No: See B
    - Send to Mgmt. via e-mail
- Document
- Measure Knowledge

Management
- Disseminate to staff
- Document
- Provide documentation to CPO
- Leave

Workforce
- Receive Information
- Understand?
  - Yes: Apply to Operations
  - No: POTENTIAL FALLOUT

www.privacyassociation.org
MEASUREMENT (CONTINUED)

Documentation “C”

CPO

- Maintain Log of Education Provided
- Record Departments Submitting Compliance of Training

Low Compliance

- Assess Reporting Volume
- Y
- E-mail reminder
- Document Compliance
- Final Report to Administration

N
- Appropriate Compliance Rate

Management

- Provide Documentation to CPO

Workforce

www.privacyassociation.org
Measure Knowledge “D”

**CPO**
- Perform Random Floor Audits; HCMG Practice Audits; Home Health Audits; Health Plex Audits
- Perform Random and for cause Electronic Audits (MediTech)

**Management**
- Reported Incidents

**Workforce**
- Reported Incidents
OPERATIONAL DEFINITION

Defining the Measure: Number of Unauthorized Access/Disclosure Incidents

- Baseline measure of Incidents/Exposures
- Categorize exposures to be consistent with Office of Civil Rights (OCR) requirements for annual reporting (Analysis Stage)
- Identify exposures (Area of occurrence)
- Identify exposures as reportable to OCR or Not Reportable
- Identify route causes for exposures (i.e. Carelessness, Intentional, Lack of knowledge)
OPERATIONAL DEFINITION

Purpose

- To appropriately identify those exposures/vulnerabilities that require reporting to the OCR
- To better understand the needs of the organization to reduce vulnerabilities of exposure through education.

Measure the Process

- Random audits of entity system-wide work units.
- Survey via e-mail directed to Management to determine level of satisfaction with currently provided materials (Voice of the Customer (VOC)).
## HIPAA Education Material – Quality (CQ)

### Survey Your Folks

<table>
<thead>
<tr>
<th></th>
<th>Poor</th>
<th>Fair</th>
<th>Satisfactory</th>
<th>Excellent</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIPAA Reminders</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIPAA Articles</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct Response To Questions</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIPAA Annual Education</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Cost of Poor Quality

- Financial Loss
- Reputation Loss (Community)
- Loss of Confidence

[www.privacyassociation.org](http://www.privacyassociation.org)
POLL QUESTION

- Does your organization leverage a Six Sigma approach?
  - (A) Yes
  - (B) No
  - (C) Maybe, but not related to Privacy or Compliance
THE SECRET SHOPPER SURVEY

- What to expect...
- Larger percentage of non-clinical Workforce will answer questions appropriately vs. clinical Workforce
- But...of the inappropriate answers there will be more non-clinical vs. clinical
Incidents of Unauthorized Use/Disclosure of PHI

POSSIBLE REASONS

Why, Why, Why

Machine

- Unsecured PCs
- Associates Failure to Log Off
- Shared Passwords
- Staff Pulled to Assist Patient Needs
- Decreased Staff
- Improve Work Force Efficiencies
- Economics Constraints
- Exposed Monitors
- Placement
- Department Layout
- Physical Constraints
- Networked Printers
- Networked Faxes

Methods

- Improper Disposal
- Apathy
- Lack of Understanding
- Lack of Dept. Management Oversight
- Decreased Staff
- Improve Work Force Efficiencies
- Economic Constraints
- Loss
- Staff Inattentiveness
- MultiTasking
- Added Responsibilities
- Decreased Staff
- Improve Work Force Efficiencies
- Economic Constraints
- Distracted
IMPROVE/CONTROL

- Eliminate general education reporting requirement – mix it up
- Develop Secret Shopper questionnaire based on data collected
- Perform baseline survey of Workforce cross section to determine level of knowledge (50 face-to-face surveys, clinical and non-clinical)
- Identify relevant policies directly related to findings
- Provide baseline findings to management
IMPROVE/CONTROL

- Develop new HIPAA education program requirements
- Resurvey Secret Shopper (6 questions) from identified policy level of understanding
- Determine level of knowledge – share with management
- Success will be measured by number of appropriate responses and number/type of incidents/concerns reported/observed
- Repeat
POLL QUESTION

What is the most critical cost of quality component for your organization?

- (A) Financial Loss
- (B) Reputational Loss
- (C) Loss of Confidence
- (D) All of the Above
OK, SO......ARE WE THERE YET ??

- We Defined the Project - Understanding HIPAA
- We Measured existing information to establish a baseline
- We Analyzed the data—prevalence of type and frequency over time
- We Improved the method of Workforce education to address survey results (specific policies, distilled to a short and readable message)
- We Control through direct observation of reported incidents and periodic resurvey
- We Repeat – Define, Measure, Analyze, Improve, Control
IN CONCLUSION...

THE PROBLEM

DEFINE

IMPROVE / CONTROL

MEASURE

ANALYZE

www.privacyassociation.org
QUESTIONS?

Eric Dieterich  
Partner  
Sunera LLC  
edieterich@sunera.com  
(786) 390-1490

Janice Schuck  
Chief Privacy Officer  
Clinical Research Administrator  
Holy Cross Hospital  
janice.schuck@holy-cross.com  
(954) 776-3239

SUNERA

Resources

- Six Sigma for Managers

www.privacyassociation.org