CYBERSECURITY CONSIDERATIONS & RISK ANALYSIS PROCESSES

THE THREAT IS REAL

89% of healthcare organizations surveyed have suffered at least one data breach in the last 2 years

- 45% of CEOs have experienced more than five data breaches over the past 2 years
- 61% of BAs have experienced data breaches
- Data breaches could be costing the U.S. healthcare industry an average of $6.2 billion annually
- The average economic impact of data breaches per organization is $2.2 million.

Source: Sixth Annual Study on Patient Privacy & Security of Healthcare Data, Ponemon Institute, May 2016
THE THREAT IS REAL

Medical information is sold on the black market typically at a premium, reports range widely on the actual cost, but they go for well above the cost of stolen credit card info. An interactive map of healthcare breaches by number of occurrence can be found at the World Privacy Forum website.

Source: [http://www.worldprivacyforum.org/medicalidentitytheft.html](http://www.worldprivacyforum.org/medicalidentitytheft.html)

AREA OF SCRUTINY

Deficient Risk Analysis!
ENFORCEMENT

Phase II will mostly consist of “desk audits,” but some will be selected for an on-site more comprehensive audit, starting in 2017.

All entities are eligible for selection for the on-site audits EVEN those who have already gone through a “desk audit.”

A report of the summarized findings will be created and made available sometime after the conclusion of the planned audits in 2017.

Desk Audit Scope
- Privacy – Notice of Privacy Practices (does not apply to BAs)
- Breach Notification – Timing and Content of Breach Notifications or Breach Risk Assessments
- Security – Risk Analysis and Risk Management

Audit Protocols – Updated and available now

ENFORCEMENT

Add @hhs.gov as a known address to avoid losing emails in spam

Covered Entities - make sure you have a list of your Business Associates ready

Your documentation should be able to stand on its own because the main interaction with OCR is uploading your documents:
• Can they be understood by an auditor?
• Would they benefit from a narrative that explains them?

Assess against the protocols
• Desk audit focus
• Comprehensive

ENFORCEMENT

HIPAA compliance reviews and complaint investigations are even more thorough than the Phase II audits.

Complaint Investigation – complaint driven

Compliance Review – breach driven

Trending Issues
- Lack of BAA
- BAA not updated after HITECH
- Incomplete or inaccurate Risk Analysis
- Lack of transmission security
- Patching of software
- Audit logs
- Insider threat
- Improper disposal
- Insufficient backup and contingency planning

HIPAA Penalties vs. Settlements
• OCR most often “settles” and creates “corrective action plans”
• These amounts are vastly reduced compared to what they could enforce through actual civil monetary penalties under the HITECH Act
EVALUATION VS. RISK ANALYSIS

Evaluation
- Gap assessment comparing compliance practices against the individual standards/requirements
- Guidance may be found at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html

Risk Analysis / Risk Management
- Identify and assess risks to all of your ePHI
- Take action to reduce risks and vulnerabilities to a reasonable and appropriate level
- Guidance may be found at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html

<table>
<thead>
<tr>
<th>Standard</th>
<th>Requirement</th>
<th>Specification</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>§164.308(a)(8)</td>
<td>§164.308(a)(8)</td>
<td>Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity’s security policies and procedures meet the requirements of this subpart.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Standard</th>
<th>Requirement</th>
<th>Specification</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>§164.308(a)(1)</td>
<td>§164.308(a)(1)(i)</td>
<td>Implement policies to prevent, contain, and correct security violations.</td>
<td>Risk Analysis</td>
</tr>
<tr>
<td>§164.308(b)(1)</td>
<td>§164.308(b)(1)</td>
<td>Conduct an accurate and thorough assessment of the significance of the risk and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.</td>
<td>Risk Analysis</td>
</tr>
<tr>
<td>§164.308(b)(2)</td>
<td>§164.308(b)(2)</td>
<td>Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.</td>
<td>Risk Management</td>
</tr>
</tbody>
</table>
PERFORMING AN EVALUATION

OCR HIPAA Audit Protocol has been updated
Foundational & comprehensive starting point
Significantly enhanced, but still does not guarantee compliance

Security Rule Educational Series
HHS's website has a Security Rule Educational Paper Series that provides further clarification to the Security Rule requirements
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html
Has links to a number of good reference documents including some developed specifically to clarify the Security Rule

2.3 Security Gap Evaluation – Observations and Recommendations Matrix
While high-level guidance has been issued, there are no baseline standards from the federal government in support of “risk analysis” efforts.

OCR issued “Guidance on Risk Analysis Requirements under the HIPAA Security Rule” on July 14, 2010:
- Definitions
- Elements of a Risk Analysis
- 9 pages

NIST SP 800-30 – Guide for Conducting Risk Assessments
- 41 pages

**ELEMENTS OF A RISK ANALYSIS**

1. **Scope of Analysis**
   - An organization's risk analysis should include the potential risks and vulnerabilities to the confidentiality, availability and integrity of all ePHI that an organization creates, receives, maintains, or transmits. (45 C.F.R. § 164.306(a))
     - All ePHI, regardless of the particular electronic medium in which it is created, received, maintained or transmitted or the source or location of its ePHI.
   - Hard Drives/USB Drives/Floppy Disks
   - CD/DVD
   - Cell Phones/PDAs
   - Backup Media/Transmission Media
   - Etc.

2. **Data Collection**
   - Identify and document where the ePHI is stored, received, maintained or transmitted. (45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1))
     - Questionnaires, Interviews, Automated Scanning Tools

**AREA OF SCRUTINY**

Scope of your Risk Analysis is a big area for OCR

Audit protocol
- Does the entity conduct an accurate and thorough assessment of the potential risks...to the confidentiality, integrity, and availability of all the ePHI it creates, receives, maintains, or transmits?
- Obtain and review the written risk analysis documentation for:
  - A defined scope that identifies all of its systems that create, transmit, maintain, or transmit ePHI
  - The word “all” appears four different times in this one protocol

Resolution Agreements
- Failure to conduct risk analysis and implement risk management plans (MAPFRE 1/18/17 $2.2m)
- Failure to conduct a thorough risk analysis of all of its ePHI (Lahey Hospital 11/24/2015, $850k)
- Neither entity had conducted an accurate and thorough risk analysis (New York Presbyterian and Columbia University 5/7/2014, $4.8m)
HIPAA VS. MEANINGFUL USE

The big picture - certified EHR data is not the only important data, all ePHI must be addressed.

- All ePHI required by HIPAA
- Include in your risk analysis/mgmt
- ePHI contained in CEHRT
- Must attest for Meaningful Use

SCOPE – EXAMPLES

<table>
<thead>
<tr>
<th>Applications</th>
<th>Asset Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>EHR</td>
<td>Desktops/Laptops</td>
</tr>
<tr>
<td>Email</td>
<td>Desktops/Laptops</td>
</tr>
<tr>
<td>Network Shares</td>
<td>Server</td>
</tr>
<tr>
<td>Electronic Voicemail</td>
<td>Server</td>
</tr>
</tbody>
</table>

ELEMENTS OF A RISK ANALYSIS

1. Identify and Document Potential Threats and Vulnerabilities

   - Identify and document reasonably anticipated threats and vulnerabilities to ePHI. (45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii))
   - Threat - “[t]he potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.”
     - Natural – Floods, Earthquakes, Tornadoes, etc.
     - Human – Inadvertent data entry, malicious software upload, unauthorized access to confidential data
     - Environmental – Long term power failure, pollution, chemicals, liquid leaks
   - Vulnerability – “[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy.”
THREAT & VULNERABILITY – EXAMPLES

<table>
<thead>
<tr>
<th>Assets</th>
<th>Threat</th>
<th>Vulnerability</th>
<th>Security Measures (Controls)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktops, Laptops, etc.</td>
<td>Malware – theft of data</td>
<td>Lack of sufficient anti-malware</td>
<td>1. Employees are educated</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(installed/updated)</td>
<td>on social engineering</td>
</tr>
<tr>
<td>Desktops, Laptops, SAN, etc.</td>
<td>Hacker – theft of data</td>
<td>Unpatched vulnerabilities in</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>network systems</td>
<td></td>
</tr>
<tr>
<td>Desktops, Laptops, Smartphones,</td>
<td>Burglar/Thief – theft</td>
<td>Media is not handled and</td>
<td></td>
</tr>
<tr>
<td>USBs, etc.</td>
<td>of equipment</td>
<td>guarded properly</td>
<td></td>
</tr>
<tr>
<td>Desktops, Laptops, Smartphones,</td>
<td>Careless IT personnel –</td>
<td>Media is not properly disposed</td>
<td></td>
</tr>
<tr>
<td>USBs, etc.</td>
<td>improper</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>destruction/disposal</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>or reuse of media</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Desktops, Laptops, SAN, etc.</td>
<td>System Cracker –</td>
<td>Employees are educated and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>social engineering</td>
<td>educated/unaware of social</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>engineering tactics</td>
<td></td>
</tr>
</tbody>
</table>

ELEMENTS OF A RISK ANALYSIS

4. Assess Current Security Measures

- Assess and document the security measures an entity uses to safeguard ePHI (45 C.F.R. §§ 164.306(b)(1), 164.308(a)(1)(ii)(A), and 164.316(b)(1))
  - Documentation – Policy, Procedure, Process, etc.
  - Practice – Physical or logical controls in place

SECURITY MEASURES – EXAMPLE

<table>
<thead>
<tr>
<th>Assets</th>
<th>Threat</th>
<th>Vulnerability</th>
<th>Security Measures (Controls)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktops, Laptops, Smartphones,</td>
<td>Burglar/Thief –</td>
<td>Media is not handled and</td>
<td>1. Employees are educated</td>
</tr>
<tr>
<td>USBs, etc.</td>
<td>theft of equipment</td>
<td>guarded properly</td>
<td>on social engineering</td>
</tr>
<tr>
<td>Desktops, Laptops, SAN, etc.</td>
<td>System Cracker – social</td>
<td>Employees are educated and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>engineering</td>
<td>educated/unaware of social</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>engineering tactics</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ELEMENTS OF A RISK ANALYSIS

5. Determine the Likelihood of Threat Occurrence

- Document all threat and vulnerability combinations with associated likelihood estimates that may impact the confidentiality, availability and integrity of ePHI of an organization. (45 C.F.R. §§ 164.308(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii))
  - Threat-source motivation and capability
  - Nature of the vulnerability

<table>
<thead>
<tr>
<th>Likelihood Level</th>
<th>Likelihood Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.</td>
</tr>
<tr>
<td>Medium</td>
<td>The threat-source is moderately motivated and sufficiently capable, but controls are in place that may impede successful execution of the vulnerability.</td>
</tr>
<tr>
<td>Low</td>
<td>The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.</td>
</tr>
</tbody>
</table>

6. Determine the Potential Impact of Threat Occurrence

- Assess the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability. (45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii))
  - Quantitative vs. Qualitative Assessment
  - Loss of Integrity, Confidentiality, Availability

<table>
<thead>
<tr>
<th>Magnitude of Impact</th>
<th>Impact Definition</th>
</tr>
</thead>
</table>
| High                | Exceeds the maximum loss of integrity, confidentiality, or availability of ePHI.
| Medium              | Involves the loss of integrity, confidentiality, or availability of ePHI.
| Low                 | Results in the loss of integrity, confidentiality, or availability of ePHI.

7. Determine the Level of Risk

- Assign a risk level based on the average of the assigned likelihood and impact levels. (45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii))
  - Inherent Risk = Likelihood * Impact
  - Residual Risk = Inherent Risk - Safeguards (Controls)

Source: OCR's "Guidance on Risk Analysis Requirements under the HIPAA Security Rule"
### RISK DETERMINATION – EXAMPLES

<table>
<thead>
<tr>
<th>Assets</th>
<th>Threat</th>
<th>Vulnerability</th>
<th>Security Measures (Controls)</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktops, Laptops, Smartphones, USBs, etc.</td>
<td>Burglar/Thief - theft of equipment</td>
<td>Media is not inventoried and guarded properly</td>
<td>1) Employees are educated to protect the physical security of the device on a yearly basis</td>
<td>High (5)</td>
<td>High (5)</td>
<td>Critical (25)</td>
</tr>
<tr>
<td>Desktops, Laptops, Servers, SAN, etc.</td>
<td>System Cracker - social engineering</td>
<td>Employees are overly trusting and uneducated or unaware of social engineering tactics</td>
<td>1) Employees are educated on social engineering threats yearly</td>
<td>Moderate (3)</td>
<td>High (5)</td>
<td>High (15)</td>
</tr>
</tbody>
</table>

### ELEMENTS OF A RISK ANALYSIS

8. Finalize Documentation
- The Security Rule requires the risk analysis to be documented but does not require a specific format. (45 C.F.R. § 164.316(b)(1))

9. Periodic Review and Updates to the Risk Assessment
- Conduct continuous risk analysis to identify when updates are needed. (45 C.F.R. §§ 164.306(e) and 164.316(b)(2)(iii))

### ELEMENTS OF RISK MANAGEMENT

Risk management is the implementation of security measures to sufficiently reduce an organization’s risk of losing or compromising its ePHI and to meet the general security standards.

#### Example Risk Management Steps
- Develop and implement a risk management plan [This plan describes what will be done to further mitigate the identified risk.]
- Implement security measures.
- Evaluate and maintain security measures.

---
RISK MANAGEMENT – EXAMPLES

<table>
<thead>
<tr>
<th>Assets</th>
<th>Threat</th>
<th>Vulnerability</th>
<th>Controls</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktops, Laptops,</td>
<td>Burglar Theft</td>
<td>Need is not</td>
<td>1) Employees are educated to protect the physical security of devices on a</td>
<td>High (5)</td>
<td>High (5)</td>
<td>Critical (25)</td>
</tr>
<tr>
<td>Smartphones, USBs, etc.</td>
<td></td>
<td>handled and</td>
<td>yearly basis</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>guarded</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Risk Management Plan: Encrypt all devices that may receive ePHI. Implement a MDM solution to manage these devices. Use the MDM solution to perform monthly inventory checks to see if any devices have gone missing and investigate. Remotely wipe any devices that cannot be located.

Responsible Party: CIO
Remediation Date: Est. 10/1/2017

---

<table>
<thead>
<tr>
<th>Assets</th>
<th>Threat</th>
<th>Vulnerability</th>
<th>Controls</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktops, Laptops,</td>
<td>System Cracker –</td>
<td>Employees are</td>
<td>1) Employees are educated on social engineering threats</td>
<td>Moderate (2)</td>
<td>High (5)</td>
<td>High (15)</td>
</tr>
<tr>
<td>Servers, SAN, etc.</td>
<td>Social Engineering</td>
<td>overly trusting</td>
<td>2) Social engineering tests are performed twice a year to assess the</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>and uneducated</td>
<td>employees’ awareness</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>or unaware of</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>social</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>engineering</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>tactics</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Risk Management Plan: Increase education to occur quarterly through a variety of different avenues. Communicate the results of the social engineering tests to reaffirm the issue with the workforce. Use real-life examples to further enhance awareness.

Responsible Party: Education Team
Remediation Date: Est. 12/31/2017

---

AREA OF SCRUTINITY

OCR will be looking for evidence that you took action on the identified risks in some form or fashion.

- Obtain and review documentation demonstrating the security measures implemented and/or in the process of being implemented as a result of the risk analysis or assessment. Evaluate and determine whether the implemented security measures appropriately respond to the threats and vulnerabilities identified in the risk analysis according to the risk rating and that such security measures are sufficient to mitigate or remediate identified risks to an acceptable level.
- Have this info documented.

HIPAA Penalty Enforcement

- February 1, 2017 – OCR levied a $3.2 million civil money penalty against Children’s Medical Center of Dallas for lack of addressing known security risks.
- Encryption was identified as a risk in 2007, was not remediated until 2013.
- Children’s suffered 2 breaches during this time that encryption would have protected against.

---
TRENDING RISK AREAS
RISKS TO LOOK FOR IN YOUR ENVIRONMENT

TRENDING RISK AREAS – VENDOR MANAGEMENT

- Vendors are a key part of many healthcare organization’s business processes, but have also been an avenue for compromising of PHI/ePHI.
- Threat: Vendors are not diligent in their security measures.
- Vulnerability: Vendor’s lack of controls may put your data at risk.
- Recommended Controls:
  - Robust contracts and BAAs that specify the requirements to protect the data and implications for failure to do so.
  - Vendor management and assessment process up-front and ongoing to assess the controls the vendor has in place. Could be accomplished through:
    - Reviewing SSAE16 SOC Reports (Third party’s assessment of controls)
    - Questionnaire to vendor
    - Audits of vendor to test controls effectiveness
  - Process to monitor for new vendor’s, working with Contracting/AP/Supply Chain, etc.

TRENDING RISK AREAS – MEDICAL DEVICES

- Threats: Hackers, Patients, Malware, etc.
- Vulnerabilities: Unpatched vulnerabilities, out of date operating systems, default user/admin credentials, weak wireless encryption, etc.
- Recommended Controls:
  - Physically secure devices
  - Segment these devices network segments
  - Regular vulnerability scans
  - Implement a life cycle management program for devices
  - Need to be managed throughout the entire life cycle:
    - Planning & Requirements
    - Procurement & Contracting
    - Implementation
    - Maintenance
    - Decommission

FDA RECALLED:
- Hospira Symbiq Infusion System – Cybersecurity vuln.
- Alaris Medley Large Volume Pump – Defective part
TRENDING RISK AREAS – BUSINESS CONTINUITY / DISASTER RECOVERY

- With the increased reliance on electronic records and applications in the healthcare industry, the more important it is to have proper business continuity/contingency/disaster recovery plans in place.
- Threats: Natural disasters, man-made disasters, cyber attacks, IT changes, etc., etc., etc.
- Vulnerabilities: Proper business continuity and/or disaster recovery (IT) plans are not in place or are not actionable, plans are not tested for readiness, etc.
- Recommended Controls:
  - Detailed Business Impact Analyses to determine key technologies, people, and processes, and required recovery time objectives (RTOs) and recovery point objectives (RPOs)
  - Documented Business Continuity and Disaster Recovery Plans
  - Regular testing of the plans including operationally how workforce would continue functioning without critical applications/network access/etc.
  - Regular testing of the ability to recover critical applications, and the associated timeframe for doing so through different scenarios.

TRENDING RISK AREAS – SOCIAL ENGINEERING

- Threats: Attackers External or Internal
- Vulnerabilities: Users not aware of social engineering tactics
- Recommended actions:
  - Education, education, education (upon hire, annual reminders, ad-hoc updates, learning experiences, etc.)
  - Testing of your users, perform phishing efforts, do physical walkthroughs, perform phone calls, etc.
  - Ensure other security controls are strong.
  - Use multi-factor authentication (where possible, does not mean two different passwords)
  - Administer least-privilege access (network, apps, devices, etc.)
  - Segment the critical data
  - Perform proactive penetration testing and vulnerability assessments to identify weaknesses and address accordingly
  - Have good backups and a solid and ready Disaster Recovery Plan

DELIVERY NOTICE

HOTEL CONFIRMATION

Your package has been delivered
Thank you for using our service.

Shipment Details

- Delivery Date: [Date]
- Delivery Time: [Time]
- Delivery Address: [Address]
- Delivery Signature: [Signature]
- Delivery Notes: [Notes]

You may track your package at: [Tracking URL]
TRENDING RISK AREAS – SOCIAL ENGINEERING

PAYMENT NOTIFICATION

SECURE EMAIL

The following social engineering attack was attempted:
- Tampering: An attacker tried to tamper with a payment notification email.

TRENDING RISK AREAS – RANSOMWARE

• Threats: Malware, Attackers External and Internal, Social Engineers/Phishing
• Vulnerabilities: Users not aware of threats, poor network security measures, lack of data backups
• Recommended Controls:
  - Education of workforce
  - Testing of network security controls through penetration testing
  - Testing of data backups and disaster recovery readiness
  - Block unnecessary (malicious) replies from users (block office macros, block executable file coming from external domains, restrict administrator tasks on workstations, etc.)
  - Have a plan

CLOSING REMARKS
WHAT YOU SHOULD BE DOING TODAY

Take action on the following:

- Monitor Phase 2 audit developments and apply lessons-learned.
- Ensure sufficient Gap Evaluation and Risk Analysis efforts have been completed.
- Periodically test the operating effectiveness of compliance/control activities (not just design).
- Remediate identified gaps/risks in a timely manner.
- Create documentation/evidence that can stand on its own.
- Continue building a "culture of compliance" at your organization!

43

Continue building a "culture of compliance" at your organization!

Q&A

CONTACT US

Matt Jackson
Director
matthew.jackson@protiviti.com
Phone: 469-276-8179

Kevin Dunnahoo
Senior Manager
kevin.dunnahoo@protiviti.com
Phone: 972-798-6229

Matt is a founding member of Protiviti and is a Director in the Dallas MMA with more than 17 years of professional experience in bringing operational, technology, and regulatory consulting and internal audit services to the healthcare industry. Matt serves as Protiviti's National Healthcare Information Technology Leader as well as Protiviti's HIPAA Solutions Leader. He is a frequent speaker on and has published various articles related to internal audit, compliance and information technology improvement initiatives.

Kevin is a Senior Manager with Protiviti Dallas office and has more than 9 years of professional experience providing IT consulting and auditing services to the Healthcare industry. Kevin is a member of Protiviti's National Practice and is a key lead for HIPAA Security Compliance services. In the Healthcare Industry, Kevin has provided value to his clients through his insights and understanding of the HIPAA Security regulations, information security practices, business continuity, and IT audit. Kevin is a Certified HCCA-P, CISSP, and HITRUST CSF Practitioner, and has also consulted various fortune 100 companies implementing HIPAA regulatory initiatives...