Mergers & Acquisitions in Healthcare and Information Security

Session Agenda
Agenda

- Introductions and Overview
- Mergers and Acquisition in Healthcare
- Steps for Performing Security and Compliance Due Diligence
- Conclusion
- Questions

Meditology Overview & Introductions
Who is Meditology?

- Focused exclusively on the healthcare industry with a core competence in security, privacy, and HIPAA compliance.
- Conducted hundreds of engagements for healthcare clients across the country ranging in size and complexity from community hospitals to 2000+ bed health systems.
- An average of 15+ years of combined “Big 4” healthcare IT security and compliance leadership experience.
- Certifications include: CISSP, HCISPP, HITRUST (CCSFP), PMP, CCNA, CPHIMS, CISA, CEH, and CNSS.
- Team has directly relevant operational experience as CISO’s and Chief Privacy Officers of health systems.
- Worked with clients under OCR investigation, made multiple presentations to OCR, and very knowledgeable about the OCR audit process.
- Lead architect of the HITRUST Common Security Framework.
- Advisors to ONC / HHS on healthcare information security, ethical hacking, and medical device security.

Serving Healthcare Clients Coast to Coast
Presenter Introductions

Ryan Freeman-Jones
Meditology Services
Senior Manager, IT Risk Management
West Coast Practice Leader

Martin Ignatovski
Eye Care Leaders
Chief Information and Compliance Officer

Mergers and Acquisition in Healthcare: Setting the Stage
Mergers and Acquisitions in Healthcare: Setting the Stage

- Healthcare mergers, integrations, and acquisitions are on the rise:
  - Modifications to regulatory incentives and government programs including the Patient Protection and Affordable Care Act
  - Innovations in healthcare Information Technology
  - Evolving care and payments models
  - Advances in Accountable Care Organization (ACO) models
  - Rising delivery costs and squeezed operating margins
  - Cost and reimbursement constraints

The Wall Street Journal estimates that, "Merger activity for the healthcare industry doubled in the first part of 2015 and represents over a quarter of all M&A activity across industries."¹

That trend continued into 2016 and the industry appears to be headed for further consolidation in 2017 and beyond

Healthcare mergers and acquisitions dominate the global M&A market for 2017.

---

The industry segments most likely to experience a merger or partnership event include long term care, hospitals, and physician practice groups.
Mergers and Acquisitions in Healthcare: Challenges

- Information security, privacy, and compliance teams often not given much warning or insight into mergers and partnerships.
- Organizations tend to accumulate a large portfolio of applications, IT solutions, network components, and entrenched processes over time.
- Complexity introduced for securing patient information and systems across organizational boundaries.
- Maturity of security and compliance often varies from organization to organization.
- Culture shock introduced for entities going from a less-secure to a more-secure posture.
- M&A often increase unmanaged healthcare vulnerabilities.
- Healthcare already a turbulent cyber threat landscape.

Mergers and Acquisition in Healthcare: What’s Next
Mergers and Acquisitions in Healthcare: What’s Next

- Set realistic expectations, healthcare integrations can be lengthy
  - Identify Risks
  - Develop Corrective Action
  - Operate security and compliance
- Be proactive, plan take action early, be thorough and methodical
- Document and measure

Performing Security and Compliance Due Diligence
Recommended Steps for Performing Security and Compliance Due Diligence

First 60 Days

- Conduct an internal and external ethical hacking / penetration test
- Perform a gap analysis of compliance with company security and privacy policies
- Inventory existing security tools and solutions
- Review entity’s prior risk analysis and compliance documentation
- Establish a communication plan and governance model

60 - 180 Days

- Develop an integration strategy and road map
- Convene governance teams and implement communication plan
- Remediate quick wins
- Perform a skill set and resource analysis
- Identify in-flight security and compliance projects
- Integrate security policies
- Consolidate corrective action plans & regulatory documentation

180 Days +

- Continue integration with:
  - Access controls
  - Configuration management
  - Endpoint protections
  - Mobile device management
  - USB and portable media security
  - Vulnerability management
  - Incident and breach response
  - Audit logging and monitoring
  - Intrusion detection / prevention
  - Wireless security
  - Network security
  - Education, training, & awareness

The First 60 Days: Conduct Ethical Hacking Testing

- Conduct ethical hacking or penetration testing exercises to quickly assess and identify technical security exposures
- Meditology recommends a targeted ethical hacking test be conducted to simulate a real-world attack

---

The First 60 Days: Perform a Security Controls Gap Assessment

- Perform a targeted gap assessment: identify inconsistencies in security controls, understand new risk exposure to the organization, and evaluate controls compliance with policies.
- Reference Healthcare industry standard security frameworks to validate that the review covers relevant control areas. Example frameworks include:
  - HITRUST Common Security Framework (HITRUST CSF)\(^5\)
  - NIST Cybersecurity Framework (NIST CSF)\(^6\)
  - Center for Internet Security Critical Security Controls (CIS Controls)\(^7\)
- If a full-scale controls or risk assessment is not feasible, organizations should look to collect procedures and implementation evidence for critical security controls aligned with the parent organization’s policies.

\(^5\) [https://hitrustalliance.net/hitrust-csf/](https://hitrustalliance.net/hitrust-csf/)
\(^6\) [https://www.nist.gov/cyberframework](https://www.nist.gov/cyberframework)
\(^7\) [https://www.cisecurity.org/critical-controls.cfm](https://www.cisecurity.org/critical-controls.cfm)

The First 60 Days: Inventory Existing Security Tools & Review Prior Risk Analysis and Compliance Documentation

- **Inventory Existing Security Tools**
  - Discover overlapping security tools and solutions like anti-malware, endpoint encryption, intrusion detection, and other technologies.
  - Inventory of security tool capabilities should be completed for both the parent organization and partner organization to be referenced for future analysis and integration.

- **Review Prior Risk Analysis and Compliance Documentation**
  - Industry regulations and incentive programs, including HIPAA and Meaningful Use, require healthcare entities to conduct routine risk analyses of potential threats to patient information.
  - Collect and review past risk analyses and compliance reports to help gain an understanding of the security and compliance maturity of the partner organization.

\(^8\) [https://www.healthit.gov/providers-professionals/meaningful-use-definition-objectives](https://www.healthit.gov/providers-professionals/meaningful-use-definition-objectives)
The First 60 Days: Establish Communication Plan and Governance Model

- Mergers, acquisitions, and partnerships generate a great deal of activity and moving pieces as organizations move from courting one another into active integration
- Manage process to limit breakdown in communication as it relates to security and privacy integration
- Develop formal structures and mechanisms to maintain communication between various groups responsible for security and compliance including:
  - Identifying point persons for security, privacy, and compliance across entities
  - Integrating or creating formal governance committees
  - Establishing leadership reporting for both entities

Performing Security and Compliance Due Diligence: 60 – 180 Days
60 – 180 Days

- The activities in the first 60 days are intended to identify and manage high-risk exposures introduced by mergers and partnerships and to lay the ground work for further integration.

- The following months should be geared toward creating formalized action plans to continue with integration of security and compliance personnel, processes, and technologies.

---

60 – 180 Days: Develop a Security and Compliance Integration Strategy

- A formal integration strategy and road map should lay out the short-, medium-, and long-term objectives of integrating security and compliance functions across the partnering entities.

- Develop an integration strategy:
  - Discrete set of projects
  - Prioritized by level of risk
  - Level of effort, cost (both operational and capital)
  - Dependencies
  - “Quick wins” that when implemented, will move the partner organization from the current security posture to the desired security posture over a set period of time (typically 2-3 years).

- This plan should include prioritized projects, resource allocations, budget considerations, regulatory requirements, and other strategic compliance and security technology initiatives.
60 – 180 Days: Convene Governance Teams and Implement Communication Plan & RemEDIATE Quick Wins

- **Convene Governance Teams and Implement Communication Plan**
  - The communication and governance processes outlined in the first 60 days should be formally convened and executed as the integration efforts continue between the organizations.
  - Where possible, organizations should look to incorporate privacy, security, and compliance discussions into established forums rather than creating new bodies and standing meetings.

- **RemEDIATE Quick Wins**
  - Merging organizations should work together to remediate technical and compliance exposures that have high or medium risk ratings and a low level of effort to complete (i.e. quick wins).
  - Larger or more complex initiatives should be planned for future implementation.

60 – 180 Days: Perform a Resource and Skill Set Analysis, & Identify In-Flight Security and Compliance Projects

- **Perform a Resource and Skill Set Analysis**
  - Potential to combine security, privacy, and compliance resources occur during M&A. Allows efficiency to execute the security and compliance mission.
  - Perform an analysis of skill sets and resource allocation to devise a plan for applying resources to continued corrective action, implementation and operational efforts.

- **Identify In-Flight Security and Compliance Projects**
  - Most entities are in a state of continual improvement and remediation of known HIPAA compliance and information security risks.
  - Organizations should identify and inventory in-flight projects for the partnering organizations and determine prioritization of initiatives going forward.
  - These prioritizations should also be incorporated into the strategic plan and integration road map.
60 – 180 Days: Integrate and Update Policies & Consolidate Corrective Action Plans and Regulatory Documentation

- **Integrate and Update Policies**
  - Information security, privacy, and breach response policies should be inventoried for both organizations and stored in a central location.
  - Organizations should commission an initiative internally or seek third party subject matter expertise and support to consolidate and update policies to create a single set of requirements to address compliance requirements for both organizations’ needs.
  - The updated policies should also be vetted through the newly organized communication and governance processes.

- **Consolidate Corrective Action Plans and Regulatory Documentation**
  - Organizations should consolidate and track compliance-related documentation for both entities and seek to merge and prioritize initiatives; if separate corrective action plans and compliance documentation were discovered in the first 60 days.

Performing Security and Compliance Due Diligence: 180 Days and Beyond
180 Days and Beyond

- The specific security and compliance initiatives to undertake for longer-term integration activities for merged organizations will vary depending on the areas identified in the first 180 days.
Conclusion

- The current trend of consolidation within healthcare is driven by shifting systematic and economic conditions.

- The rapid pace at which healthcare organizations are partnering or merging with other entities presents significant challenges in the areas of security, privacy, and compliance on a broad scale.

- Teams of healthcare IT professionals that set out to prevent unwanted exposures will be required to develop proactive plans and procedures to rapidly assess the security posture of acquired entities or new partners.

QUESTIONS?
Thank you