Integration of Privacy and Security – A Strong Alliance

October 17, 2013

Stacey Carr, Division Privacy Officer

Ram Ramadoss, Director, Privacy and Information Security oversight

Catholic Health Initiatives

KEY OBJECTIVES

- HIPAA & Healthcare Industry Overview
- Overview of Omnibus Rule Changes
- Understand the Responsibilities of Business Associates
- Understand the Approach for Successful Integration

KEY OBJECTIVES

- Understand the Skills Development for the Team Members

- Key Areas of Integration between Privacy and Security

TECHNOLOGY IS DRIVING HEALTHCARE

- **Clinical & Business Intelligence**
  - Positively impact patient care delivery, health outcomes and business operations
- **Clinical Informatics**
  - Promotes understanding, integration, and application of information technology in healthcare settings.
- **Electronic Health Records (EHR)**
  - Longitudinal electronic record of patient health information generated by one or more encounters in any care delivery setting.

TECHNOLOGY IS DRIVING HEALTHCARE (Continued)

- **Health Information Exchange (HIE)**

- **Implantable Medical Devices**

- **Consumer Mobile Applications**
  - Roughly 100,000 health applications available in major app stores, and the top 10 mobile health applications generate up to 4 million free and 300,000 paid daily downloads.

TECHNOLOGY IS DRIVING HEALTHCARE (Continued)

- **Social Networks in Health Care**
  - About one-third of Americans who go online to research their health currently use social networks to find fellow patients and discuss their conditions. Sixty percent of surveyed physicians and 65 percent of surveyed nurses are interested in using social networks for professional purposes. (Source: Deloitte)

- **Personalized Health Repository (PHR)**

OMNIBUS RULE

- Final rule implementing regulations for many provisions of the Health Insurance Technology and Economic and Clinical Health Act (HITECH Act). Informally referred to as the ‘Omnibus Rule’, it addresses changes to many areas of the HIPAA Privacy and Security Rule providing final regulations and definitive requirements for compliance. Notable changes have occurred within the following:
  - Business Associates
  - Breach Notification
  - HIPAA and GINA (The Genetic Information Nondiscrimination Act interactions)

BUSINESS ASSOCIATE (BA)

- BAs directly subject to the HIPAA Security Rule, including requirement for administrative, technical and physical safeguards.
  - Must conduct a Risk Assessment/Gap Analysis and implement all required standards.
  - Appoint a Security Officer

- BAs also subject to certain provisions of the Privacy Rule.

BUSINESS ASSOCIATE (BA)

- BAs must ensure that any Subcontractor that creates, receives, maintains, or transmits PHI on behalf of the BA agrees to the same restrictions and conditions that apply to the BA with respect to PHI.

- BAs subject to civil and criminal penalties for violations.

ENTITIES DESIGNATED AS BAs

- Health data transmission organizations, including Health Information Organizations
  - Must be more than a mere conduit; must routinely access PHI in the course of performing their BA duties
- E-Prescribing Gateways
- Patient Safety Organizations

ENTITIES DESIGNATED AS BAs

- Personal Health Record Vendors who manage the health records of Covered Entities

- First tier Subcontractors and all downstream Subcontractors who have access to PHI

BREACH NOTIFICATION

- Breach redefined to clarify:
  - An impermissible acquisition, access, use or disclosure or Security Incident is <u>presumed to be a breach</u> unless the Entity or BA demonstrates:
    - there is a low probability the PHI has been compromised, or
    - one of the other exceptions to the definition of "breach" applies

- There is no definition of "compromise".

BREACH NOTIFICATION

- Removes the “risk of harm standard”.

- Burden on the Entity to demonstrate low probability of compromise through four part risk assessment.

RISK ASSESSMENT

- Risk Assessment to cover (at least) these four areas – the “objective factors”
  - The nature and extent of PHI involved, including the types of identifiers and the likelihood of re-identification;
  - The unauthorized person who used the PHI or to whom the disclosure was made;
  - Whether PHI was actually acquired or viewed; and
  - The extent to which the risk to the PHI has been mitigated

RISK ASSESSMENT (CONTINUED)

- Uncertainty about how to weigh factors in the four part analysis.

GENETIC INFORMATION NON-DISCRIMINATION ACT OF 2008

- The Omnibus Rule modifies the Privacy Rule as directed by the Genetic Information Nondiscrimination Act of 2008 (“GINA”).

GENETIC INFORMATION NON-DISCRIMINATION ACT OF 2008

- GINA prohibits discrimination based on an individual’s genetic information in both health coverage and employment.
  - Prohibits the use of genetic information in the employment context (e.g., hiring and firing);
  - Restricts employers from requesting, requiring or purchasing genetic information; and
  - Limits the disclosure of genetic information.

GINA

- “Genetic Information” includes:
  - An individual’s genetic tests;
  - Genetic tests of family members;
  - The manifestation of a disease or disorder in a family member; and
  - Any request for, or receipt of, genetic services or participation in clinical research that includes genetic services by an individual or family member;
  - But not an individual’s age or sex.

UNDERSTAND THE APPROACH FOR SUCCESSFUL INTEGRATION

- Review your organization structure
- Historical reasons for keeping these functions separate
- Emerging technologies require a closely collaborative approach

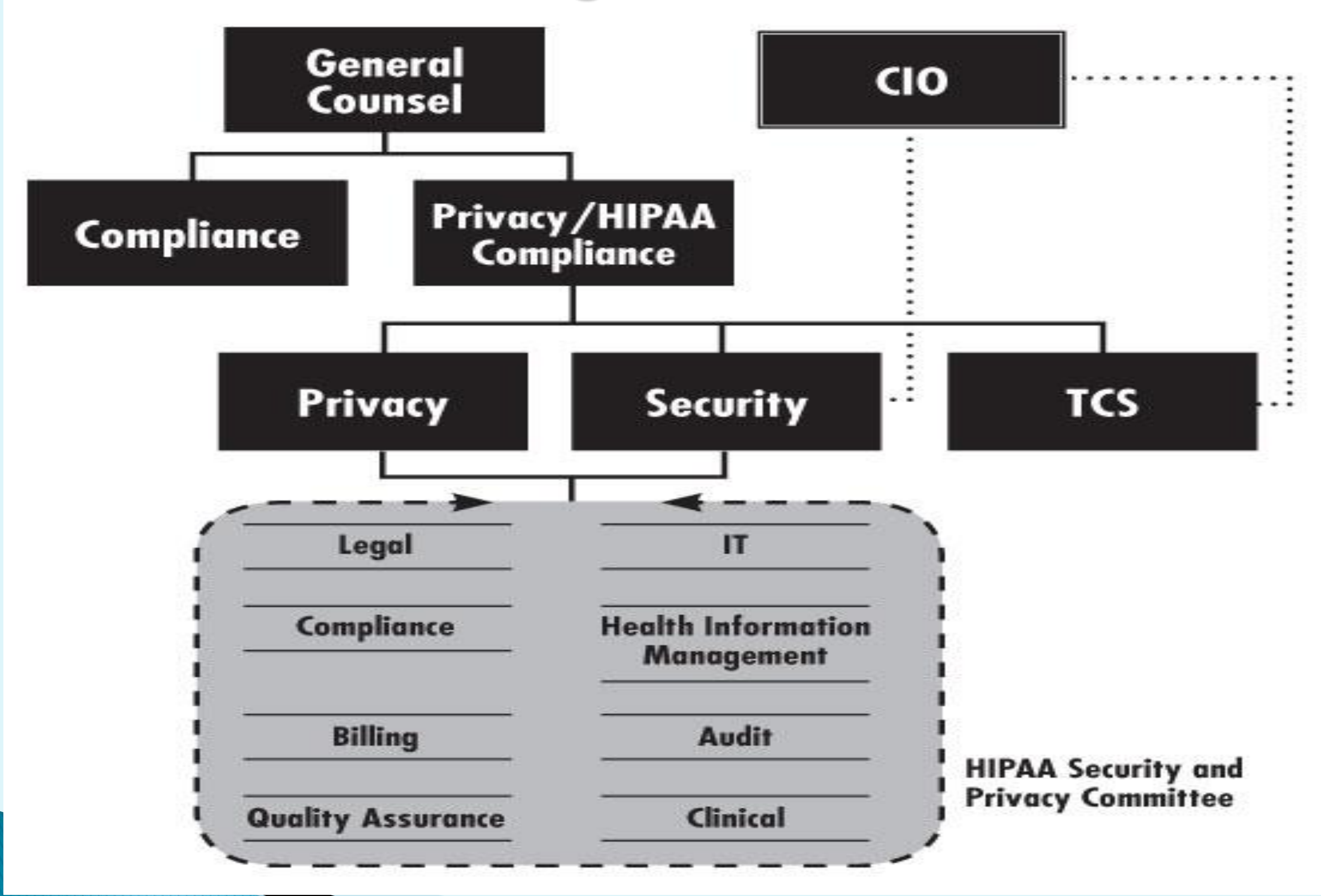
UNDERSTAND THE APPROACH FOR SUCCESSFUL INTEGRATION

- No single solution will work for all organizations

- Review your committees and task forces
  - Security Steering Committees and Privacy Oversight Groups

- Top Management Commitment

Recommended Org. Structure - AHIMA



SKILLS DEVELOPMENT FOR THE TEAM MEMBERS

- Privacy team members should have a good understanding of information security controls and technologies
  - How we can address the data protection?

- Security team members must understand the expectations from privacy instead of focusing on tactical controls
  - Why we are doing it?

KEY AREAS OF INTEGRATION – PRIVACY AND SECURITY

- Policies and Standards
- Education – Awareness and Training
- Risk Assessments
- New Product/Service and Technology Review

KEY AREAS OF INTEGRATION – PRIVACY AND SECURITY

- Incident Management & Breach Investigations
- Data Leakage Prevention (DLP) and Monitoring
- Supplier Risk Assessment

POLICIES AND STANDARDS

- Privacy and Security team members - review and provide inputs

- Mobile Device Security and BYOD (Bring Your Own Device) Policies
  - Legal and Privacy are major stakeholders

- Integration is critical for creating strong foundation

EDUCATION – AWARENESS AND TRAINING

- Determining the best training approach for your organization is a significant task. You may decide to make training part of a comprehensive HIPAA educational program or part of an even broader educational program.

- Similarities in the Privacy and Security requirements invite combined training efforts. Both rules include training of all personnel, ongoing training, and documentation.

EDUCATION – AWARENESS AND TRAINING

- Who should be trained?
  - HITECH’s new definition of "workforce“ includes "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate."

WORKFORCE EDUCATION - BEST PRACTICES

- AHIMA recommends the following best practice guidance regarding Privacy and Security training procedures:
  - General training must be provided for all workforce members, including contract workers, as a part of new hire orientation, before the first day of work in the staff member's actual department.
  - Annual training is required of all staff.
  - Make training your mantra—it may be your best privacy asset.
  - Develop an enduring program that perpetuates itself and becomes part of the culture of your organization.

WORKFORCE EDUCATION - BEST PRACTICES

- AHIMA recommends the following best practice guidance regarding Privacy and Security training procedures:
  - Privacy and security training programs should include education (knowledge and understanding), training (how-to), and ongoing awareness. They should cover PHI in all forms including verbal, written, and electronic, and they should establish timelines for training new employees according to date of hire.
  - Develop a responsive communication process to address questions that arise after training and in an ongoing manner.

WORKFORCE EDUCATION - BEST PRACTICES

- AHIMA recommends the following best practice guidance regarding Privacy and Security training procedures:

  - Develop a reference repository of up-to-date policies and procedures.
  - Develop a process for evaluating training program effectiveness, reliability, and validity.
  - Develop a verification process to ensure that users have completed security awareness training before receiving access to electronic PHI.

RISK ASSESSMENTS

- Emerging technologies and Electronic Health Record systems – new set of privacy and security risks
- Identify where your data is stored
- Security risk assessments are more mature – several standardized frameworks are in place
- Privacy can leverage the tools and the frameworks developed by security industry
- Combined risk assessments are very effective

NEW PRODUCT/SERVICE &TECHNOLOGY REVIEW

- Holistic approach and coverage for privacy and security risks
- Prioritization of risks and remediation
- Security Amendments and Business Associate Agreements should be aligned to provide strong administrative controls

INCIDENT MANAGEMENT & BREACH INVESTIGATIONS

- Complex State Privacy Laws and Notifications
- Incident vs Breach
- Critical area for the teams to work together

INCIDENT MANAGEMENT & BREACH INVESTIGATIONS

- Requires thorough and detailed investigations before declaring an incident as a breach

- Security technologies can provide significant information to determine the impact

DATA LEAKAGE PREVENTION (DLP) AND MONITORING

SECURITY OR PRIVACY TOOL

- Data Leakage Prevention software is not just a Security tool. It offers opportunities for Privacy to assess the movement of PHI and PII within an organization. Data provided by DLP can assist Privacy in key areas such as:
  - Risk Assessments
  - Education
  - Policy Development
  - Incident Response

DATA LEAKAGE PREVENTION (DLP) AND MONITORING

- The additional benefit is the opportunity for Security and Privacy to work collaboratively in response to any high severity activity identified within the DLP system.

SUPPLIER RISK ASSESSMENT

- Majority of applications in Healthcare – COTS applications; third party applications
- Medical Device Vendors
- Application Service Providers

SUPPLIER RISK ASSESSMENT

- Significant growth of suppliers and partners – Business Intelligence

- Most of the partners have access to protected health information (PHI)

- Integration will help determine where the significant data risks are and high risk suppliers

SUMMARY

- Integration of privacy and security is integral to your data protection program.
- Assess your organization risks to identify potential opportunities.
- Hold your Business Associated accountable.
- Education is your first line of defense.
- As technologies advance, understand the risks and benefits; identify necessary controls

Questions?