

PRIVACY AND SECURITY: REPORTING AND COMPLIANCE MANAGEMENT

April 21, 2010

Marti Arvin, JD, CCEP-F, CHC-F, CHRC, CIPP/GCPC
Chief Compliance Officer, UCLA Health Sciences

Monica Modi Dalwadi, CIA, CFE
Manager, Baker Tilly

Objectives

- Provide an orientation to key privacy concepts
- Discuss privacy in practical business terms
- Provide guidance on an effective governance structure and privacy program
- Discuss success factors in measuring the effectiveness of a privacy program
- Provide and promote an interactive presentation

Agenda

- Background and Key Privacy Concepts
- Governance and the Privacy Program
- Metrics and Reporting
- Closing Comments and Open Discussion

4

Background and Key Privacy Concepts

What Is Privacy?

- Privacy is defined as the rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information
 - Source: The AICPA's Generally Accepted Privacy Principles (GAPP)

Personally Identifiable Information (PII)

- Information that can be attributable and used to identify a specific individual
- May include, for instance:
 - Name
 - Social Security number
 - Street address
 - Phone number
 - Physical characteristics (e.g., face, eyes, fingerprints)
 - Driver's license number
 - Credit card number

Other Sensitive Information

- Some information is not PII, but is sensitive and should be treated with care
 - Age, gender, race, and/or ethnicity
 - Grades
 - Salary and/or job position
 - Criminal record
 - Purchase history
- Some sensitive information is also subject to regulatory/statutory requirements
 - Medical information

The Distinction Between Privacy and Security

- Privacy is concerned with enabling individuals to have a say over how their personal information is collected, used, retained, and disclosed
- Security is concerned with protecting information from inappropriate access, modification, or destruction
- You need security in order to achieve privacy

Privacy Benefits and Risks

Privacy Benefits	Privacy Risks
Brand protection	Negative publicity
Consumer confidence	Lost business
Customer loyalty	Damaged customer/employee relationship
Business partner trust	Legal liability and financial loss
Competitive differentiation	Regulatory or industry sanctions

Generally Accepted Privacy Principles (GAPP)

- Generally Accepted Privacy Principles (GAPP) promulgated by the American Institute of Certified Public Accountants (AICPA)
 - Principle 1: Management
 - Principle 2: Notice
 - Principle 3: Choice and Consent
 - Principle 4: Collection
 - Principle 5: Use and Retention
 - Principle 6: Access
 - Principle 7: Disclosure to Third Parties
 - Principle 8: Security for Privacy
 - Principle 9: Quality
 - Principle 10: Monitoring and Enforcement

Privacy in Higher Education

- An exceptional volume and variety of personal information (e.g., transcripts, financial aid, health centers, retail operations)
- Increased complexity and oversight challenges in a decentralized environment
- Subject to many privacy regulations due to
 - Breadth and nature of business operations
 - Students and alumni from many states

12

Governance and the Privacy Program

What Is Governance and Why Is It Important?

- The framework of processes, roles and responsibilities that links privacy resources, policies, processes, and information to an organization's strategic priorities and objectives
- Use of a steering committee or making privacy a standing agenda item for an existing committee
- Helpful to have a responsible executive to drive decision making and reconcile competing needs

Participant Poll

Who in your institution holds primary responsibility for privacy?

- a. Privacy office
- b. Compliance office
- c. General counsel's office
- d. Information technology
- e. Other
- f. It's a shared responsibility with no clear lead
- g. I don't know

Privacy Governance Challenges Inherent in Higher Education

- Numerous stakeholders
 - ▣ Chief Privacy Officer
 - ▣ General Counsel
 - ▣ Chief Compliance Officer
 - ▣ Chief Information Officer
 - ▣ Chief Information Security Officer
 - ▣ Human Resources
 - ▣ Admissions
 - ▣ Financial Aid
 - ▣ Registrar
 - ▣ Advancement
- Shared or undefined responsibilities
- Value of openness and sharing in the academic environment

Making Governance Work

- Clearly define governance roles and responsibilities
- Define the process and communication protocols for making privacy-related decisions
- Assign an individual to coordinate privacy efforts
- Provide a forum at which decision-makers discuss privacy matters
 - ▣ Dedicated steering committee
 - ▣ Agenda items within an existing forum

Making Governance Work (Continued)

- Include researchers' considerations
- Ensure there is a linkage between privacy and security programs
- Incorporate Internal Audit as part of the process
 - ▣ Transparency
 - ▣ Linkage with the audit committee and board of trustees
 - ▣ Monitoring

Risk Assessment

- The process of identifying and prioritizing internal and external privacy risks that may affect a university
- For most organizations, should be performed frequently
 - ▣ Periodic (e.g., annual) comprehensive risk assessment
 - ▣ Ongoing monitoring of new and emerging trends, laws, and threats
 - ▣ Privacy impact assessments (PIA) for business process and system changes
- Engage key business areas
 - ▣ Legal counsel, human resources, information security, marketing, customer service

Policy

- Policy is a foundation for all privacy activities
 - Consumer-facing
 - Internal
- Should cover the major areas in GAPP (e.g., notice, collection, use, retention)
- Consider an overarching policy supported by specific policies that apply to laws or business areas
- A website privacy policy is critical
 - Cookies and use of forms to collect information
- Many non-privacy policies have privacy implications (e.g., document retention, human resources)

Awareness

- Critical to the success of any privacy program, as the judgment of people on the front line and those who access data is critical
- Frequent, catchy reminders are more effective than infrequent big announcements
- Weave privacy messages into new hire training and logon banners of applications housing PII
- Focus on thematic principles and common sense, supplemented by specific regulatory or industry-specific information

Processes and Systems

- Weave privacy considerations into the fabric of the organization's processes and systems
- Areas with special privacy considerations include
 - Human resources
 - Face-to-face customer transactions (e.g., credit cards)
 - Online customer interactions
 - Records, filing
 - Credit and collections
 - System design (e.g., encryption, security, need-to-know access)
 - System development and change control
- Outsourcing warrants special consideration

22

Reporting and Metrics

Reporting Structure

- Immediate supervisor
- Leadership
- Colleagues
- Clients

Participant Poll

- How often do you generate reports to the following:
 - Supervisor
 - Other leadership
 - Colleagues
 - Clients
 - Other

Reports to the Immediate Supervisor

- The frequency and data elements of the reports to an immediate supervisor will vary
- Reports should be given on, at the least, a quarterly basis
- More frequent, informal reports may be appropriate
- These reports might be used to demonstrate the utilization of the resources in an office (e.g., number of issues received in the last quarter versus number closed by the aging report)

Reports to Leadership

- Many organizations present reports to leadership on, at the least, an annual basis
- Quarterly reporting is also fairly common
- These reports should be focused and consistent in structure
 - A 50 page report will not be read by leadership
 - Charts and graphs attract the audience's attention

Reports to Colleagues

- Reports may be provided at regular intervals, or as-needed for particular issues
- If the report is created at a regular interval, it should be consistent in structure
 - The audience will pay more attention to a report if they know where to look for information

Reports to Clients

- This program is generally designed to provide a service to the constituents of the organization
- When writing a report to the client, remember that this program is a service function
- Always preface bad news with good news
- Again, try to model a consistent structure for similar reports

What to Report

- Seven elements
- High level versus detailed
- Narrative versus graphic

Participant Poll

- How many structure reports using the seven elements?
- How many use another structure for your reports?
- If you use another structure, why?

Seven Elements

- All reports to leadership should be structured based on the seven elements
- If there is nothing to report for a particular area, leave the placeholder
 - For example, if no policy changes have been made in the last quarter, the Policies and Standards section of a quarterly report may note, “No changes in last quarter”

High Level versus Detailed

- A general rule of thumb is to lessen the level of detail in a report as the audience rises in levels of an organization
- Senior leaders and the board of directors will still require enough detail to understand the issues that are occurring under the program

Narrative versus Graphic

- A picture says a thousand words
- Visual depictions generally get more focus than a three page narrative of the same information
- It is often easier to visualize a trend versus reading a narrative about it

Consistency of Reports

- Timing
- Similar data elements
- Distinguish new factors

Timing of Reports

- There are some reports that will be provided on a regular basis
 - Board of directors reports
 - Committee reports
- Other reports, like audit reports, will follow the structure of the audit plan, but even these have timing issues
 - Ensure that it is clear what the timeframe is for the management response and the final report so that the audit does not drag on forever

Similar Data Elements

- Consistency of reports is critical
- Immediate supervisors, leadership members, clients, and colleagues will use these reports and pay attention to them if important data elements are easy to find
- Again, reports to leadership should follow the seven elements
- Audit reports may or may not follow the seven elements, but the structure should be consistent

Distinguishing New Factors

- Highlight any changes to the traditional reporting structure
- If the program had changes or if a significant issue was uncovered, this should be something the audience reading the report should be able to easily locate

Participant Poll

- What metrics do you measure?
- How do you track your metrics?
- What benchmarking measures do you use?
 - Internal
 - External

Creating Your Metrics

- This takes careful thought
- Talk to colleagues in the industry
- Beg, borrow, and steal ideas
- Think about this in the beginning
 - ▣ If data is not captures, reporting cannot occur
 - ▣ Think about what data should be reported
 - Garbage in, garbage out (GIGO)

Creating Your Metrics

- Think of the big picture when creating metrics
 - ▣ Is this capable of being added to the current structure?
 - ▣ Does the method for capturing metrics allow for consistency across the organization?

Participant Poll

What metrics do you use in your institutions to monitor the effectiveness of the privacy program?

Success on Ensuring the Right Information Gets to the Right People

- Maintain a skilled staff
- Use technology to leverage your data
- Be concise
- Don't speculate
- Know the information
- Be prepared to deliver bad news in the best light possible
- Offer solutions
- Push the issue if necessary

Contact Information

Marti Arvin

Chief Compliance Officer, UCLA Health Sciences

Email: marvin@mednet.ucla.edu

Phone: 310-794-6763

Monica Modi Dalwadi

Manager, Baker Tilly

(Formerly Beers + Cutler)

Email: monica.dalwadi@bakertilly.com

Phone: 703-923-8559