Tuesday, October 26
2:30pm-4:00pm

710 - Data Security & Compliance

Dawn Haghighi
Assistant General Counsel
Princess Cruises

Lisa Murphy
Senior Associate General Counsel & Assistant Director
The Regence Group

Meredith Stone
Vice President General Counsel Americas
NACCO Materials Handling Group, Inc.

Session 710

Faculty Biographies

Dawn Haghighi

Dawn Haghighi is assistant general counsel for Princess Cruise Lines. She is also pro bono advisor to Rockefeller Pacific Trust advising on the advancement of national and international justice systems, with emphasis on transnational economic activities.

Her legal career encompasses senior management positions with responsibility for corporate matters, litigation and governance and compliance at several international corporations, including the Royal Bank of Scotland/Charter One Bank, NA and Nordstrom, Inc.

Ms. Haghighi is a frequent lecturer before corporate boards, foundations and professional organizations around the world. She is a member of the Pacific Council on International Policy and serves as a member of the board of directors of the Los Angeles Committee on Foreign Relations (officer), ACC's Southern California chapter, the Western Justice Center Foundation, the Princess Cruises Community Foundation and founding Director of the National US Hong Kong Business Association. She participated in the Salzburg Global Seminar (2010); she was selected through the UCLA Center for International Relations as a delegate to the Enhancing the Middle East's Economic Future IV Forum in Doha, Qatar (2009); she was invited as a delegate to the RAND Corporation China Reform Forum (2005, 2004), the First Sino-American Women's Conference (1991), and The PRC Supreme Peoples' Court International Arbitration and Mediation Forum (1990, 1992) and attended the White House Welcome Ceremony for the PRC Premier Wen Jibao (2003). In 2005, she was the recipient of ACC's Robert Townsend Member of the Year Award.

Lisa Murphy

Lisa T. Murphy has years of experience providing legal advice to health companies large and small. Currently she is senior associate general counsel & assistant director with The Regence Group in Portland, Oregon, which operates four BlueCross and/or BlueShield Plans in the Pacific Northwest and Intermountain regions.

Before joining Regence, she was a partner in the employee benefits practice group with Miller & Chevalier Chartered, a Washington, DC law firm. While at Miller & Chevalier, Ms. Murphy co-authored a book on HIPAA privacy compliance. She also worked as in-house counsel for the BlueCross and BlueShield Association.

Ms. Murphy frequently speaks and writes on legal issues relating to the health insurance industry. In addition to her work at Regence, Ms. Murphy is the chair of the Oregon Board of Bar Examiners and of the Oregon March of Dimes chapter.

Ms. Murphy graduated from the University of Oregon, cum laude, Phi Beta Kappa, and earned her law degree from Cornell Law School, cum laude.

Meredith Stone

Meredith B. Stone, vice president, general counsel Americas for NACCO Materials Handling Group, Inc. is responsible for the legal compliance of NMHG's Americas Division activities in North, South and Central America, including corporate transactions, litigation, import/export and government sales compliance, contractual commitments, as well as advising and counseling the corporation on employment law issues, and providing preventative legal training to employees.

Prior to joining NACCO Materials Handling Group, Inc., Ms. Stone was the vice president, general counsel and secretary of Konica Business Technologies, Inc., a general attorney for the Long Island Railroad Company in Jamaica, New York; an associate attorney with Levine & Robinson, P.C. in Mitchel Field, New York; and an assistant corporation counsel for the law department of the City of New York.

Ms. Stone is a member of the ABA, the New York State Bar Association, and the North Carolina Bar Association, where she is a council member of the Corporate Counsel Section and former chairperson of its membership committee and CLE Committee; she previously served as the Chairperson of the Small Law Department Committee of ACC and as president of ACC's Connecticut chapter.

She earned her bachelor of arts from the University of Vermont and JD, cum laude, from St. John's University School of Law in Jamaica, New York.

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

Data Security and Compliance

Dawn Haghighi
Assistant General Counsel & Privacy Officer
Princess Cruises

Lisa T. Murphy
Senior Associate General Counsel & Assistant Director
The Regence Group

Meredith B. Stone
Vice President General Counsel Americas
NACCO Materials Handling Group, Inc.

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

Federal Laws and Regulations: Sampling

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

Federal Laws and Regulations: Sampling

- GLBA
- HIPAA
- FCRA
- FACTA
- Identity Theft Red Flag Rules
- Affiliate Marketing
- Disclosure Identity Theft Red Flag Rules
- Affiliate Marketing Disclosure
- COPPA
- RFPA
- CAN –Spam
- ECPA
- TCPA

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

State Laws: US

- State Laws: Typically Consumer Centric Laws
- Trend: Expand the scope of law to cover not only businesses operating in the State to businesses collecting information about a State resident

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

State Laws: Sampling

- **SSN Laws:** Specific State Laws
- **California:** Shine the Light" Statute
- **Massachusetts:** Standards for the Protection of Personal Information of Residents of the Commonwealth
- **Nevada:** Restrictions on Transfer of Personal Information Through Electronic Transmission
- **Minnesota:** Access Device Security Breach

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

International Laws

- EU Data Protection Directives
- APEC Privacy Framework (Asia)
- Personal Information Protection Act (Japan)
- South America Privacy Initiatives
- Personal Information Protection and Electronic Documents Act (Canada)
- Federal Law for the Protection of Personal Data in Control of Private Persons (Mexico)
- Personal Data Protection Act (Taiwan)

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

Why Does this Matter to My Company?

- Employee Information
  - Social Security Number
  - Bank Account Information
  - Drivers License Information
  - Other Personally Identifiable Information
- Customer Information
  - Dealers, Distributors, Franchisees
    - Their Employees & Customers
- High Risk Areas
  - IT
  - HR
  - Payroll
  - Finance
  - Training

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

Why Does this Matter?

- Who Can Access your systems?
  - Suppliers?
  - Other Third Parties?
  - How do you share data with service providers to your company?
- International Operations
- Your Company's Website
  - Cookies
  - Data submitted by users
  - Your Privacy Policy – does it address how you secure and/or use the information?

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

Essential Elements of An Effective Privacy Program

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

Privacy Program: Common Elements

- Compliant with Applicable Laws and Regulations
- Privacy Policy and Notice(s)
- Designated Privacy Officer
- Privacy Committee
- Incident Response Plan
- Audit Procedures and Risk Based Assessments
- Training Programs
- Annual Review of Privacy Program
- Insurance Coverage

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

Drafting A Privacy Notice Best Practices

- Clear and Concise Sentences
- Plain Language
- Active Voice
- Accurately Reflects Company Practices

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

Scope of the Privacy Program

- Identify and define the type of information protected
- Identify the company or business unit that is covered
- Identify the standards for sharing, use, collection and disposal of the information

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

Definition of Personal Information

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

What Constitutes Personal Information

- General: Name plus PII
- Excludes: Encrypted, redacted or scrambled
- Expands Beyond PII: Data Points, such medical, mother's maiden name, telephone number etc.

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

Privacy and the Employer

- Privacy of employee medical information
- The case of the pregnant employee
  - Your employee Peggy is pregnant
  - Starts obtaining typical medical care
  - Participates in wellness program pregnancy module
  - Develops carpal tunnel syndrome
  - Takes time off to care for her sick mother
  - Develops complications and is put on bed rest
  - Moves to your Massachusetts office
- What do you need to worry about?

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

Privacy and the Employer

- No single privacy law
  - Addressed in specific employment laws
  - Common themes, but some landmines
- Key Laws
  - HIPAA privacy
  - FMLA
  - ADA
  - GINA
  - State privacy laws

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

Privacy and the Employer

- Wellness Program
  - Generally provided as part of health plan
    - Subject to HIPAA
  - Same rules apply depending on insured status
  - Pitfalls:
    - Reports
    - Health risk assessments and GINA
    - Using information for employment decisions

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

Privacy and the Employer

- FMLA and ADA Privacy Requirements
  - FMLA certifications separate from personnel file
    - Supervisors and managers may not access
    - Follow-up to certifications cannot be performed by direct supervisor
  - ADA
    - Results of medical exams must be kept in separate files
    - Available only to supervisors who need to know the restrictions and accommodations

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

Privacy and the Employer

- GINA
  - Cannot discriminate based on genetic information
  - Cannot intentionally gather genetic information
    - Health risk assessments
- Genetic information – broad definition
  - Individual or family member's genetic tests
  - Manifestation of disease in family member
- Must keep genetic information separate from personnel files

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

Privacy and the Employer

- HIPAA Privacy
  - Applies to medical information you hold as plan sponsor
  - Self-funded plan – significant compliance.
    - Goal: Firewall between plan sponsor employees and others.
    - Alert: ARRA breach notification requirements.
    - Business associate requirements with service providers
  - Insured plan – minimal compliance.
    - Goal: limit yourself to enrollment information.
    - Challenge: Large insured plans wanting data analysis.

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

Privacy and the Employer

- State privacy laws – Massachusetts example
  - Protects personal information (name, SSN, drivers license).
  - May apply to Massachusetts employees, even if data stored outside of Massachusetts
  - Breach notification requirement

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

Contracted Privacy Requirements

- ARRA/Recovery Act: privacy and security requirements extended to service providers of HIPAA covered entities
  - Since 2003, covered via contracts – business associate agreements
  - Now directly liable under HIPAA and subject to HHS and state AG enforcement
  - Required to terminate agreement or report to HHS if covered entity is violating HIPAA
- Proposed HHS rules go further and reach subcontractors of business associates

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

Contracted Privacy Requirements

- Are you a business associate?
  - Now critical to know, given liability
  - Do you use or disclose "protected health information" to perform services for a HIPAA covered entity?

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

Contracted Privacy Requirements

- HIPAA violations – most fines are now mandatory
- Fine, per violation:
  - $100 to $25,000 – did not know and would not have known the act or omission was a violation
  - $1,000 to $250,000 – violation due to reasonable cause
  - $10,000 to $250,000 – violation due to willful neglect, corrected within 30 days
  - $50,000 to $1.5 million – violation due to willful neglect, not corrected within 30 days.
- HHS keeps penalties for its enforcement budget.
- State AG enforcement authority

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

Contracted Privacy Requirements

- Typical contract negotiation hurdles
  - Indemnification
  - Breach notice costs
- Breach notice requirements
  - Must give notice to individuals when a breach occurs if risk of financial or reputational harm to individual
  - Notice to HHS annually of breaches impacting fewer than 500 individuals
  - If impacts more than 500, immediate notice to HHS and major media outlet

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

Cloud Computing - Data Security

- What Data is in the Cloud?
- Whose is it?
- Where is it hosted?
- How is it protected?
- Any copies (back up or other)?

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

Cloud Computing – Data Security Risks

- Plan for a Breach
  - Who is Responsible?
    - Types of harm
    - Damages available
    - Settlement value
    - Insurance coverage
    - Who manages breach notice/disclosure?
    - Who pays?

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

Company Accountability for the Privacy Program

- Privacy Officer
- Privacy Committee
- Management Involvement

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

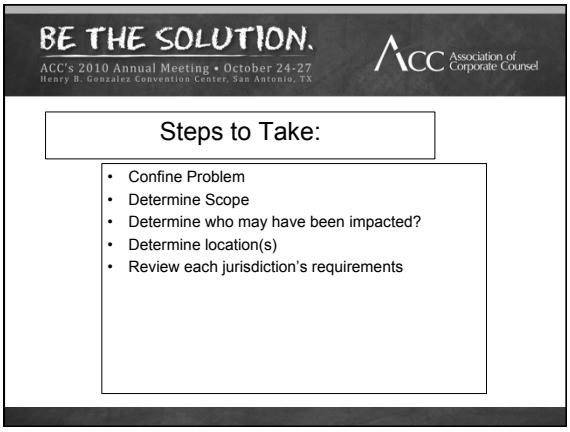
Key Departments

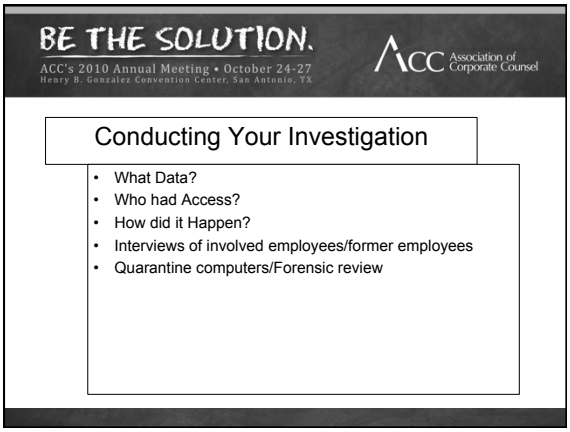
- Privacy
- Legal
- Compliance
- Risk Management
- Audit
- Sales
- Marketing
- Insurance
- Vendor Relationships
- IT
- MIS
- Facilities
- Human Resources
- Training
- Benefits/ Payroll

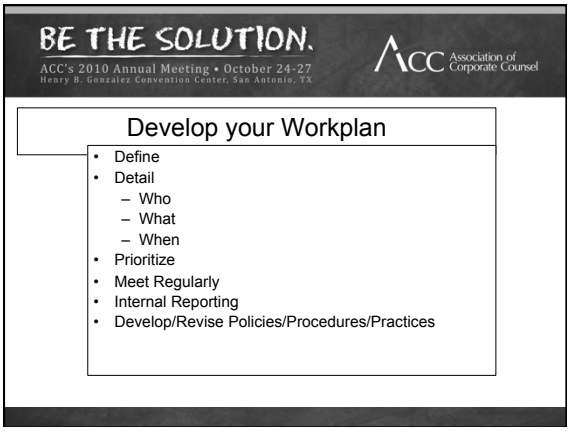
BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

After the Breach – What do you do?

- Don't Panic
- Act Quickly but not too quickly
- Team Approach
  - Legal
  - IT
  - HR
  - Public Relations/Investor Relations/Government Relations
  - Internal Audit







BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

Reporting Requirements

- 45 States & District of Columbia have breach notification laws
  - When to report
  - Who to tell
  - Form of report
- Penalties for violations of State Security Laws
- Don't Forget International Laws
  - Europe
  - Mexico
  - Canada (provincial)
  - Others

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

Who Else to Notify?

- Law Enforcement when appropriate
- Business Partners if effected
- Your insurer if appropriate
- Your Board of Directors/Committee
- Credit Reporting Agencies

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

Damage Control

- Public Statements
- Offering Credit Report Monitoring Services

To Whom It May Concern:

In accordance with the requirements of North Carolina G.S. §75-65, _____ is providing notice that it has notified _____ current and former employees of the company of a potential breach of security involving their social security numbers. A copy of a sample notice is enclosed. This notice also includes a description of the relevant circumstances. Notices were mailed to the affected individuals on or about _____. The Company has also notified the North Carolina Attorney General's Office, as required by law, and the other credit reporting agencies, _____ and _____.

Should you have any questions or require additional information, please feel free to contact me at the address below:

Name
title
Company name
Contact information

INTERNAL CORRESPONDENCE

From: **Date:**
To: All U.S. Employees

Subject: **Personally Identifiable Information Use at _____**

Adequate protection of personal information from inadvertent or inappropriate disclosure or use is very important to all of us. Accordingly, the Company has recently completed a review of how we use and maintain social security numbers and other personally identifiable information[1] relating to employees, ____ personnel and others. As a result of this review, we will be making changes in how we use and store such information and this requires action by each of you now and in the future.

The Company has determined the following:

1. The Company will not use social security numbers in data bases, hard copy documents, or otherwise to identify individuals, except as required by law.

2. If not required by law, all use of social security numbers should be phased out no later than _____.

3. As you know, all employees in the United States have been issued an employee ID number. If an identifying number will be used for an employee, the assigned employee ID number must be used.

4. If a non-employee needs to be identified other than by name (for example _____), a unique random number or other code must be assigned and maintained. Please contact _____ with any questions.

5. Unofficial physical records (convenience hard copies) that include personally identifiable information should be securely destroyed (shredded) once no longer needed for business purposes.

6. Active physical records that include personally identifiable information that are currently needed for business purposes must be maintained in a locked drawer or cabinet with access limited to only those who need to use the information for a business reason.

7. If a physical official record that include personally identifiable information is no longer needed for current business uses (for example a payroll change notice), it must be securely stored and destroyed in accordance with the Company's Physical Records Management Program. Questions should be addressed to _____.

---

[1] Personally identifiable information includes social security numbers, tax identifying numbers, bank account and credit card information.

8. Electronic records (e-records) that include personally identifiable information should be maintained in a secure electronic system, accessible only by those who need to know; access must be monitored and controlled, and may only be transmitted using a secure method approved by the IT Department, such as encryption. Please contact _____ to discuss the methods that are currently available for secure transmission of e-records.

9. When an e-record containing personally identifiable information is destroyed, it should be destroyed in such a manner as to ensure that it cannot be recovered or re-constituted.

What do you need to do now?

1. **By _____ all employees are required to review their paper files and either:**
   a. **Securely destroy convenience copies which contain personally identifiable information that are no longer needed for business purposes; or**
   b. **If the document is still needed for business purposes, it must be securely stored in a locked drawer or cabinet with access restricted to those who need to use the document and see its contents.**
   c. **Transfer inactive official records that contain personally identifiable information to the Records Center in accordance with _____. Ensure the records are identified as "Confidential" when completing the _____Form.**

2. **By _____, all employees are required to review their electronic files (e-records) and either:**
   a. **Delete e-records containing personally identifiable information if the data is no longer required for business purposes; or**
   b. **Modify e-records, such as spreadsheets or databases, to delete the personally identifiable information that is no longer needed for business purposes. If you need assistance, please _____.**
   c. **If, as part of your job responsibilities, you maintain and use data that contains personally identifiable information please notify _____ for additional instructions on how to secure these electronic files for use and transmission.**

3. **Department files (not maintained by one employee), both paper files and electronic drives, must be reviewed by each department as described above.**

What do you need to do moving forward?

1. Follow the guidelines in this memo when working with files containing sensitive information, including personally identifiable information and confidential and proprietary information.
2. If you have electronic files, these should be:

a. Saved and stored on your local personal network drive, not on the "C" or hard drive of your computer. Do not post any of these types of materials/information on a shared directory that does not have restricted access. Please submit questions _____.
b. Transmitted only when data is properly protected by a secure method approved by the IT Department, such as encryption.

3. If you have this type of information stored and you need to retain this data, please contact _____ for further direction.

Thank you in advance for your attention to this important initiative.

INTERNAL CORRESPONDENCE

From: [team members] **Date:**

Location: **To:** [senior management]

Cc:

Subject: **Personally Identifiable Information Use at _____**

The team reviewed all responses received from user departments in the U.S. to determine how and when social security numbers are used and maintained. During the course of this review, the scope was expanded to include retention of bank account and credit card information in the ____ system. The results of our findings and recommendations are summarized below.

Use of Personally Identifiable Information

Social security numbers are used at _____ for the following primary reasons:

1. Required by law (e.g., tax processing and reporting; workers compensation forms)

2. Used as an identifier for an employee.

3. Used as a contractor identifier (e.g., _____)

Personal bank account information and personal and corporate credit card information is maintained in the ___ system primarily for _____ purposes.

Team recommendations for immediate action:

1. Except as required by law, the company should not use social security numbers in data bases, hard copy documents, or otherwise to identify individuals.

2. If not required by law, all use of social security numbers should be phased out no later than _____. Appropriate steps to phase out use and retention of social security numbers will differ depending upon whether the information is in hard copy or electronic format.

3. If identifiers are required, employee ID numbers, or for non-employee's information - random numbers, should be assigned.

4. All convenience hard copies that include social security numbers should be securely destroyed (shredded).

5. All hard copy official records that include social security numbers or other personally identifiable information[1] should be stored in a safe and secure manner and when destruction is appropriate, in accordance with the company's global records management program, should be shredded.

6. All electronic official records that include social security numbers or other personally identifiable information should be maintained in a secure electronic system, accessed only by those who need to know; access to be monitored, password controlled, and if data must be provided electronically, the file should be encrypted. When destruction is appropriate, the electronic file should be destroyed in such a manner as to ensure that it cannot be recovered or re-constituted.

7. The _____ team should be directed to review the applicable policies and procedures to determine if any modifications are required to provide for secure retention and destruction of personally identifiable information such as social security numbers, bank account information, credit card information and other personally identifiable information of employees and others, addressing both hard copy and electronically stored information.

8. The _____ team should be directed to review security practices relating to requests to retrieve archived sensitive/confidential data and re-train _____ on the process.

9. All routine forms (e.g. HR forms) should be reviewed and modified to remove any request for a social security number and employee ID numbers substituted.

10. All employees should be advised to review their paper files by _____ and destroy copies of documents which contain social security numbers or other personally identifiable information as described in # 4 or 5 above.

11. All employees should be advised to review their electronic files and password protect any file which contains social security numbers or other personally identifiable information if the data is still required. This should also be completed by _____. When such a file is transmitted, it may only be transmitted with encryption.

12. A communication should be issued to all employees in _____ by _____, advising them of the required steps described in #s 10 & 11 above.

13. For all third party providers which require access to personally identifiable information, the contract should include appropriate confidentiality and processing obligations to secure this data from inadvertent or inappropriate disclosure.

[1] Defined for purposes of this memorandum to include social security numbers, tax identifying numbers, bank account and credit card information.

14. The ____ system contains social security numbers, other tax identifying numbers, bank account and credit card information for _____ which are available, in multiple copies of the ___ system, to multiple users on a global basis. The ___ team, by _____, is to review the security and use of personally identifiable information in the Company's ____ system and present a plan to appropriately suppress this data, limit access to those who have a business need to know and otherwise secure this data.

Summary

_____ uses and retains a significant amount of personally identifiable information in non-secure formats. Appropriate steps should be taken, within the short term (next __months) to securely destroy unnecessary information and to adopt security practices for information which has a valid business purpose. A longer-term solution for archived electronic records must be developed.

Attached to this memorandum is a list of appropriate business use of personally identifiable information, by function, with a recommendation of proper steps to be taken/instituted to safeguard this information from inadvertent disclosure. Further, for these functions, we recommend that the following occur:

1. Define which positions need access to personally identifiable information.
2. Limit access accordingly.
3. Train employees on proper use/retention of personally identifiable information if access is appropriate
4. Where possible, suppress access to personally identifiable information for those users who need to access a particular system or information but don't need access to the personally identifiable information in that system or information database.

Following your review of these recommendations, please contact us with any questions and directions on how the company wishes to proceed.

Title: Personally Identifiable Information Policy	Document Control Number:
Page 1 of 4 Document Author:	Effective Date: Revision No.

1.0 Objective

This Policy establishes how _____ uses, retains and destroys personally identifiable information.

2.0 Scope

This policy applies to U.S. and non-U.S. locations which access personally identifiable information relating to U.S. employees and/or U.S. customers, dealers, or other third parties.

For purposes of this policy, personally identifiable information includes social security numbers, tax identification numbers, bank account and credit card information.

3.0 General

3.1 The protection of personally identifiable information from inadvertent or inappropriate disclosure or use is important to _____.

3.2 This policy is intended to reduce the possibility of inadvertent or improper disclosure of personally identifiable information relating to ____'s employees, customers, dealers and other third parties with whom it does business.

4.0 Description

General:

4.1 U.S. Social Security numbers are not used by ____ to identify individuals except as required by law.

4.2 Employees are identified in ___ business systems in one of the following ways:

4.2.1 By name;
4.2.2 By a unique employee ID number that is assigned and maintained by the Human Resources Department; or
4.2.3 By a unique User ID that is assigned and maintained by the IT Department.

4.3 When non-employees are identified other than by name or a unique User ID (for example _____), a unique random number or other code is assigned and maintained.

4.4 Third parties requiring access to personally identifiable information maintained by the Company agree, in an executed contract, to appropriate confidentiality and processing obligations to secure the information from inadvertent or inappropriate disclosure.

4.5 Encryption software is installed on laptop computers used by employees who are required either to transmit personally identifiable information or to store such information on their

laptop hard drive

Electronic Records:

4.6 Official electronic records and data maintained in databases and other electronic systems (structured e-records) and which include social security numbers or other personally identifiable information as defined in this policy are managed so that:

4.6.1 They can be accessed only by persons with a business need to know;
4.6.2 Access is monitored and controlled;
4.6.3 Data and records are encrypted or otherwise secured in a manner approved by the IT Department for transmission; and
4.6.4 Electronic records destruction is conducted on a timely basis in accordance with the Company's Records Retention Schedule, in a manner designed so that it cannot be recovered.
4.6.5 The procedure described in _____ applicable to electronic back up media is understood to comply with the intent of this Policy.

4.7 Official and unofficial electronic records and data maintained by employees outside of structured systems (unstructured e-records) that contain personally identifiable information are managed so that:
4.7.1 They are stored securely either on a local personal network drive or on a network drive or Share Point site that is monitored and has access restricted only to those who have a substantial business need to know;
4.7.2 Data and records are encrypted or otherwise secured in a manner approved by the IT Department for transmission;
4.7.3 They are retained based on content for the period described in the Company's Records Retention Schedule.
4.7.4 If Official, they are deleted by the employee once the retention period is reached.
4.7.5 If Unofficial, they are deleted by the employee once they are no longer needed for business purposes.

4.8 Electronic records and data containing personally identifiable information are not stored on individual "C" or hard-drives, or on any transportable media, such as a CD Rom, PDA, laptop, thumb drive, etc or on any shared directory that does not have restricted access.

4.9 E-records containing personally identifiable information are only transmitted using encryption or other secure methods approved by the IT Department.

Physical Records:

4.10 Unofficial physical records that include personally identifiable information are securely destroyed once they are no longer needed for business purposes.

4.11 Active physical records, whether official or unofficial, that include personally identifiable information, are maintained in a locked drawer or cabinet with access limited to only those who need to use the information for a business reason.

4.12 Inactive official physical records that include personally identifiable information are securely stored and destroyed in accordance with the Company's Physical Records Management System.

5.0 Appendices

Appendix "A" – Definitions applicable to this Policy

APPENDIX "A"

Official Records - Official Records contain information that is required to be retained for business or legal reasons. Official Records provide evidence of ____ 's organization, business functions, policies, decisions, procedures, operations, and internal or external transactions, and reflect ____'s intent to preserve such information.

Unofficial Records - Records that are not required to be retained for business or legal reasons, formerly known as Working Papers. These may include: • Duplicates or convenience copies of official records. • Document drafts that have been superseded by approved, official versions or rejected. • Published literature, catalogs, and trade journals. This does not include published ____ product literature and catalogs. • Casual correspondence including records created to facilitate meetings or for internal communication. (Many e-mail messages fall under this category.) • Reference materials that have no on-going value. • Records that are either summarized in an Official Record or used as the basis for creating an Official Record. • Records created by employees solely for personal use that are retained on ____ computer systems or are physically located at a business site.

Active Records - Records related to current or in-process activities. These Records are typically referred to on a regular basis to respond to internal and external business requirements. Further definition of the Active period for certain record classifications is provided in the Records Retention Schedule.

Inactive Records - Records related to closed, completed, or obsolete processes or activities. Inactive Records are no longer routinely referenced but are retained in order to fulfill legal, operational, or other retention requirements.

Structured E-Records - Records that are controlled or maintained in data bases or other business applications, such as_____.

Unstructured E-Records – Records that are controlled by individual employees which are typically stored on local drives, shared drives, in Outlook, Microsoft Share Point, or in portable archive media, such as CD/DVD, USB and thumb drives, PDAs, etc.

Personally Identifiable Information ("PII") - For purposes of this policy, personally identifiable information includes social security numbers, tax identification numbers, bank account and credit card information.

Physical Records - Records retained in a physical format. They may take the form of paper, photos, or physical electronic storage media such as computer tape, video tape, USB drives, audio tape, microfilm, floppy disks, CD's, DVD's etc.

Date

Name
Address

Dear (first name):

Issue:

We wanted to bring to your attention a recent incident that affected certain personal information of _____ employees, including your information. This incident was brought to our attention recently, and we have taken steps to mitigate any results of this incident. While our investigation has revealed no reason whatsoever to believe that any improper activity has taken place in connection with your information, we cannot definitively rule out that possibility. As ensuring the ongoing confidentiality of company and employee information is important to _____. you will see in detail below what steps we are taking to protect your data going forward as well as making available to you a credit monitoring product that you can implement, at ____'s cost, to protect yourself in the unlikely event that these incidents result in any inappropriate action.

What Happened:

We learned that [describe what happened, what information was vulnerable and when this was discovered] We do not have any reason to believe that this personal information was used improperly by _____ nor do we have any reason to believe that there was any other improper use of this information. As soon as we learned of this development, immediate steps were taken to secure this information from any future use and review all procedures surrounding _____. However, because we have no means of ruling out the possibility of improper activity, we wanted to bring this situation to your attention.

Next Steps:

Although we have no reason to believe that there is any risk to you in connection with your personal information, because ____ places importance on the security of our employees' data and to the extent you have any ongoing concerns, we have arranged with _____ to help you protect your identity and credit information at no cost to you for one year from the time you enroll. This service is designed to determine if there has been any improper use of your information in connection with the credit system in our country.

Credit Monitoring Options:

To access this credit monitoring product, **within _____days of receipt of this letter**, the steps to follow are: [this information will come from your selected service provider]

Even if you are not interested in this credit monitoring product, you may wish to review your own credit report to evaluate whether any improper activity has taken place, whether connected to these incidents or to the wide range of other incidents that are reported in the media and otherwise involving companies across the country. More information is available at http://www.idtheftcenter.org/ or at http://www.ftc.gov/bcp/edu/microsites/idtheft//.

Additionally, whether or not you enroll in the _____program, you may choose to adopt an increased level of protection by placing a fraud alert on your credit file at Equifax, Experian or Trans Union, the credit reporting agencies

A fraud alert is a consumer statement added to your credit report. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. To place a fraud alert on your credit file, visit: www.fraudalerts.equifax.com or you may contact Equifax's auto fraud line at 1-877-478-7625, and follow the simple prompts. Once the fraud alert has been placed with Equifax, a notification will be sent to the other two credit reporting agencies, Experian and Trans Union, on your behalf.

In Summary:

It is unfortunate this has happened and we apologize for any inconvenience this may cause. In addition to having taken steps both to resolve this problem and to prevent further incidents of this nature, we see this as an excellent opportunity for both the Company and our employees to better educate ourselves in this important area, including taking proactive steps to understand identity theft and credit reporting. The Company has _____ to further secure your data when this occurred. We have completed this project to _____.

We hope you will take advantage of this opportunity to utilize the_____ system at no charge and thereafter, to consider what tools you may wish to employ in the future. If you have any questions about these incidents or the steps we have taken, please contact your local human resources department.

Sincerely,

Name
Senior Management Title

ACC ANNUAL MEETING - 2010
PROGRAM 710
SAMPLE

List of Process By Area where Personally Identifiable Information is required
Finance Process List

Business Process	Department that owns process	Key Contact	Data Format - how stored E=Electronic P=Paper B=Both	IT Application Name EXCEL, SAP, ACCESS, etc. if applicable.	How is application/data secured	Approved method of secured transmission when required	Title of employees with permission to access data	Comments	Date Complete
_____ Credit Card application									
_____ Expense Program									
Accounts Payable - Invoices Receipt									
Accounts Payable - W-9 forms (originals)									
Accounts Payable - W-9 forms (copies used for data entry)									
Accounts Payable - non-employee program spreadsheet: (1) used in lieu of W-9 forms for data entry of vendor info (2) used as invoice for cash/non-monetary prizes									
Accounts Payable - 1099s									
Outside Storage - archived copies									

List of Process By Area where Personally Identifiable Information and other confidential information is required
MISC process list

Business Process	Department that owns process	Key Contact	Data Format - how stored E=Electronic P=Paper B=Both	IT Application Name EXCEL, SAP, ACCESS,etc., if applicable.	How is application/data secured	Approved method of secured transmission when required	Title of employees with permission to access data	Comments	Date Complete
_____ Incentive Programs									
Corporate Officer/Director Appointments, Corporate Entity creation and related actions									
_____ Training Records									

ACC ANNUAL MEETING - 2010
PROGRAM 710
SAMPLE

List of Process By Area where Personally Identifiable Information and other confidential information is required
IT Process List

Business Process	Department that owns process	Key Contact	Data Format - how stored E=Electronic P=Paper B=Both	IT Application Name EXCEL, SAP, ACCESS, if applicable.	How is application/data secured	Approved method of secured transmission when required	Title of employees with permission to access data	Comments	Date Complete
___ IT databases including _____									
_____ database file backups									

SAMPLE

HIPAA PRIVACY AND EMPLOYERS – BASIC QUESTIONS AND ANSWERS

LISA T. MURPHY
Senior Associate General Counsel & Assistant Director
The Regence Group
Portland, Oregon

August 25, 2010

Contents

INTRODUCTION

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") included rules for "Administrative Simplification." The Administrative Simplification Rules create a uniform system for processing, retaining, and securing health care information by encouraging the use of electronic technology, mandating standardization of health-related transactions, and ensuring the security and privacy of health information. This paper focuses on the privacy provisions within HIPAA.

The privacy and security standards in HIPAA were amended by the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") which was part of the American Recovery and Reinvestment Act ("ARRA") of 2009. Congress has delegated responsibility for implementing and enforcing the Administrative Simplification provisions of HIPAA and the HITECH Act to the U.S. Department of Health and Human Services ("HHS").

Although employers are not "covered entities" under the Administrative Simplification Rules, every employer that offers health benefits or health services to its employees is affected by the Rules. This is because the Rules directly regulate most employer group health plans and certain health care providers (which may include some employers' on-site providers).

This paper provides basis information about an employer's compliance obligations, in a question-and-answer format.

I. WHAT IS PROTECTED BY HIPAA AND PENALTIES

What information is protected by the Privacy Rule?

The Privacy Rule does not protect all forms of health information – only health information that is "individually identifiable." In other words, it protects health information from which an individual can be identified, but only if that information is in the hands of a covered entity and only if the health information is held as part of a group health plan's records.

Health information is protected if:

- It is created or received by a provider, health plan, employer, or health care clearinghouse;
- It relates to the physical or mental health or condition of an individual, at any time, past, present or future (and includes information related to payment of health benefits);
- It identifies an individual or can be used to identify the individual; and
- It is in the possession or control of a covered entity (including a group health plan).

45 CFR §§ 160.103 (definitions of "health information," "individually identifiable information," and "protected health information").

"Protected health information," (often referred to "PHI") is the health information described above, *i.e.*, it is the health information that is subject to the Privacy Rule's protections.

Do state privacy laws also apply?

It depends. The Privacy Rule does not preempt all state privacy laws. State privacy laws that are "more stringent" are preserved. That is, a state privacy law that provides more privacy protections or greater individual rights than provided by the federal Privacy Rule will apply, unless that law is otherwise preempted by a different federal law, such as ERISA. Generally, state laws preempted by ERISA will remain preempted. 45 CFR § 160.203.

Accordingly, employers must determine whether and to what extent they must follow state law. This task may be particularly complicated for employers with employees in more than one state.

What about other federal laws that may require the disclosure of PHI?

Generally, nothing in HIPAA or the Privacy Rule exempts an employer from complying with other federal laws (*e.g.*, ERISA, ADA, FMLA) under the general rules of precedence applicable to federal law.

Generally, when may PHI be used or disclosed?

Group health plans may use or disclose PHI only if the use or disclosure is *permitted* or *required* by the Privacy Rule. 45 CFR § 164.502(a). In very general terms, a group health plan may use PHI internally or disclose it externally only under the limited circumstances and for the specific purposes permitted by the Privacy Rule. Otherwise, group health plans may use or disclose PHI only with the permission of the individual who is the subject of the PHI. Such permission must be given using a HIPAA compliant disclosure authorization.

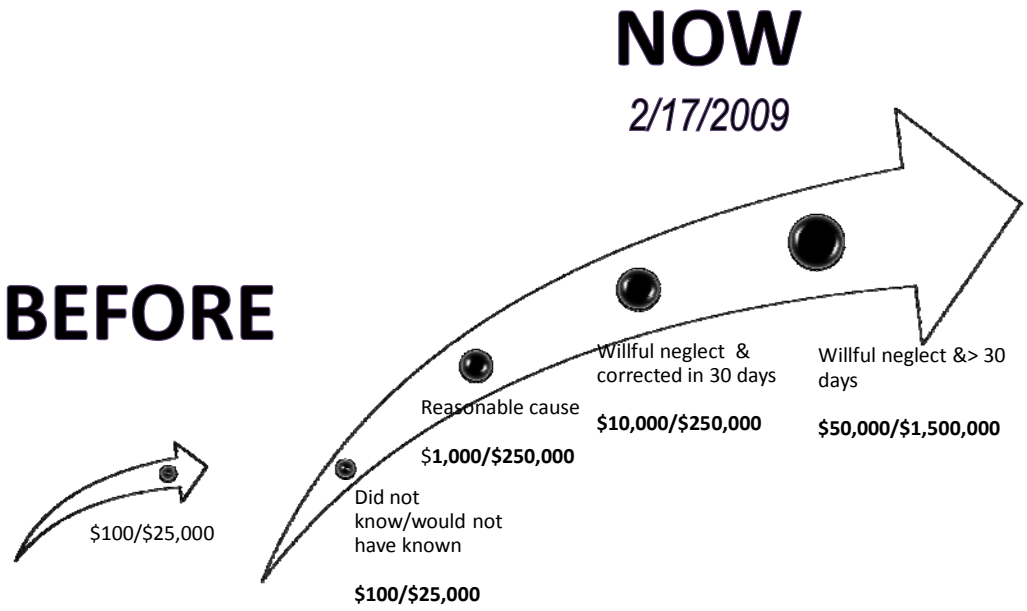
Are there any penalties for not complying with the Administrative Simplification Rules?

Yes. There are both civil and criminal penalties for noncompliance. When HIPAA was amended as part of ARRA, penalties were increased and made mandatory for most violations. Penalties are not in "tiers," based on the severity of the violation – and penalties are mandatory except for tier one violations:

- $100 to $25,000 per violation if did not know and would not have known the act or omission was a violation;
- $1,000 to $250,000 per violation if the violation was due to reasonable cause;

- $10,000 to $250,000 per violation if the violation was due to willful neglect, but it was corrected within 30 days;
- $50,000 to $1.5 million per violation if the violation was due to willful neglect and it was not corrected within 30 days.

These penalties are much more significant than those originally contained within HIPAA:



Also, under the penalty revisions, the HHS Office of Civil Rights ("OCR"), which enforces the HIPAA rules, OCR will be allowed to keep penalties for its enforcement budget.

The ARRA changes also added two additional dimensions of enforcement. First, it created authority for state attorneys general to enforce HIPAA requirements (but only if OCR has not already started an action). Although penalties for attorneys general actions are limited to $25,000 for all violations, they may seek injunctive relief and attorneys fees. Second, while HIPAA does not include a private right of action (as discussed in response to the next question), individuals harmed by "willful neglect" violations can be awarded a percentage of the civil monetary penalties beginning in 2012 (regulations are to be issued by February 2012).

Can a participant or beneficiary sue for alleged privacy violations?

Nothing in HIPAA, the HITECH Act, or the Privacy Rule provide a private right of action to an individual who claims his or her privacy rights have been violated. As noted above, however, state laws providing more stringent remedies are likely to apply. Those applicable state laws may provide private rights of action, and if they do, participants and beneficiaries may be able to invoke them.

In addition, if a group health plan incorporates its notice of privacy practices into its ERISA plan documents, a participant or beneficiary could have an ERISA claim based on a privacy violation. For this reason, employers may wish to keep their group health plan's notice of privacy practices separate from the plan documents.

II. IDENTIFYING AN EMPLOYER'S HIPAA COVERED ENTITIES

What is a HIPAA covered entity?

A covered entity is an entity required to comply with the Privacy Rule and all the other HIPAA Administrative Simplification provisions. If an entity is a covered entity for any purpose under HIPAA Administrative Simplification, it is a covered entity for all purposes under HIPAA Administrative Simplification – meaning it must comply with not only the Privacy Rule, but also the Electronic Transactions Rule and the Security. Compliance requirements for the latter two rules are beyond the scope of this paper.

There are three types of covered entities, two of which are relevant to employers: health plans (which include employer-sponsored group health plans) and health care providers (but only those who electronically transmit health information, generally to payors). 45 CFR § 160.103. The third type of covered entity, health care clearinghouses, is not relevant to this discussion.

Employers are not "covered entities" under the Privacy Rule. However, as discussed more below, employers that sponsor group health plans for their employees will be indirectly covered as the "plan sponsor." They also may be directly covered as a "hybrid entity" with respect to any on-site clinics or other facilities that are covered health care providers (if they electronically transmit health information).

A. COVERED HEALTH PLANS

What is a covered health plan?

Generally, a covered health plan is an individual or group plan that provides, or pays the cost of, *medical care*. 45 CFR § 160.103. Medical care is defined as amounts paid for:

- diagnosis, cure, mitigation, treatment, or prevention of disease, or amounts paid for the purpose of affecting any structure or function of the body,
- transportation primarily for and essential to the medical care listed above, and
- insurance covering the medical care and transportation costs listed above.

42 USC § 300gg-91(a)(2).

The Administrative Simplification Rules specifically lists a group health plan as a covered health plan for purposes of HIPAA compliance. 45 CFR § 160.103.

What is not considered a covered health plan?

Certain types of plans are specifically *excluded* from the definition of "health plan," even though these excluded plans can generate significant amounts of health information, and even though some of these plans are often combined with covered health plans in employer-provided welfare benefit packages. These plans are excluded because their primary purpose is not providing or paying for the cost of medical care and so they do not meet the basic definition of "health plan." The excluded types of plans are:

- AD&D coverage,
- short-term and long-term disability coverage,
- coverage issued as a supplement to liability coverage,
- liability insurance including general and automobile liability insurance,
- life insurance,
- workers' compensation coverage,
- automobile medical payment coverage,
- credit only insurance, and
- coverage for on-site medical clinics (although as noted, on-site medical clinics may be covered entities in their own right).

45 CFR § 160.103 (definition of "health plan"). In addition, stop loss and reinsurance plans are not covered health plans because they do not provide or pay for the cost of medical care. Rather, they insure health plans and providers against unexpected losses.

What group health plans have to comply with HIPAA?

As noted above, one of the types of covered health plans is a group health plan. It is further defined by the Administrative Simplification Rules as:

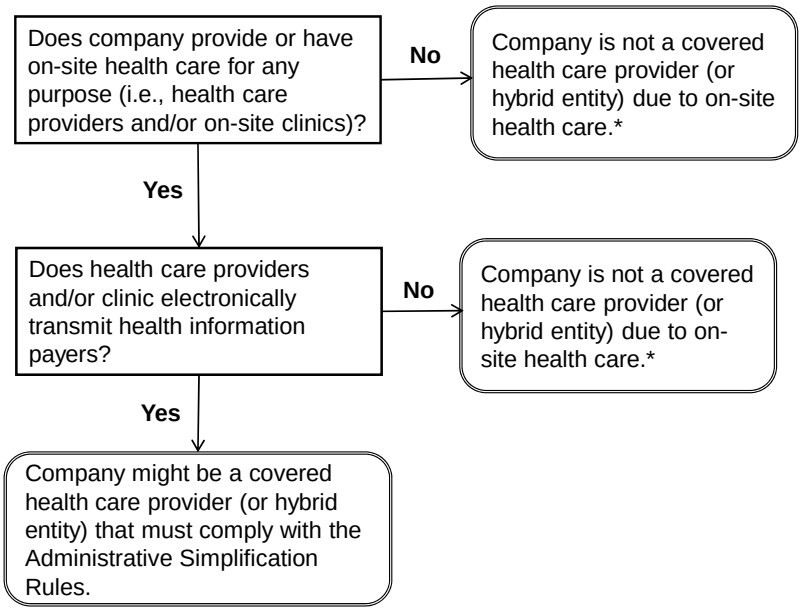
- an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA)),
- that is either insured or self-insured,
- that provides medical care, including items and services paid for as medical care to employees or their dependents directly or through insurance, reimbursement, or otherwise, and
- that
  - has 50 or more participants (as defined in section 3(7) of ERISA, 29 USC § 1002(7)); or

- is administered by an entity other than the employer that established and maintains the plan.

45 CFR § 160.103 (definition of "group health plan").

The only employer-sponsored group health plans that are not covered by this definition are those plans that are self-insured and self-administered and that have 49 or fewer participants (the "small/self-administered plan exception"). Only a small number of group health plans will meet the small/self-administered plan exception. For example, a plan with 30 participants that is fully-insured will not meet the exception because it is administered by an entity other than the employer. An example of a plan that would meet the exception is a self-insured, self-administered health flexible spending account ("health FSA") with 49 or fewer participants. Another example is a self-insured, self-administered "top hat" executive medical plan.

The following decision tree may be of assistance in determining whether a group health plan is a covered entity:



*However, company may have HIPAA Administrative Simplification compliance obligations because it offers a covered group health plan or because the company is a covered entity in and of itself (a health insurer, an HMO, a doctor's office, etc.).

Are health flexible spending accounts ("health FSA") group health plans?

A health flexible spending account ("health FSA") is a covered group health plan under the Administrative Simplification Rules. Most health FSAs are excluded from the requirements of Title I of HIPAA (*e.g.*, portability) by regulation. That regulation does not apply to the Administrative Simplification provisions, and therefore health FSAs are covered (unless they meet the small/self-administered plan exception described above).

Note that health FSAs are self-insured plans (funded by employee salary reduction amounts). As such, they are subject to full compliance under the Privacy Rule. This is the case even if all other health benefits provided by the employer are fully-insured.

Are plans not subject to ERISA required to comply with the Administrative Simplification Rules?

If a health plan otherwise meets the definition of a group health plan, it is covered by the Administrative Simplification Rules even if it is not also covered by ERISA. For example, church plans and government plans that meet the group health plan definition are subject to the Rules, even though they are exempted from ERISA.

What is an "organized health care arrangement" ("OHCA")?

An "organized health care arrangement" or "OHCA" is a new organizational entity created by the Privacy Rule. It is intended to allow separate legal entities that are expected to function as a single entity to, in fact, function as a single entity for various purposes under the Privacy Rule (usually simplicity of compliance). A key characteristic of an OHCA is that the people who receive services or benefits from it have an expectation that they are dealing with what is, in effect, a single entity. For example, if you purchase insurance, your employees probably do not make a distinction between your group health plan and the company insuring it and processing claims.

As it relates to group health plans, an OHCA can be any one of the following:

- A group health plan and its insurance issuer or HMO, but only with respect to PHI created or received by the insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in the group health plan.
- A group health plan and one or more other group health plans, each of which are maintained by the same plan sponsor.
- The group health plans described in the preceding bullet points and their insurance issuers or HMOs with respect to those group health plans, but only with respect to PHI created or received by the insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of the group health plans.

Many group health plans will be OHCAs. 45 CFR § 164.501 (definition of "organized health care arrangement").

What are the advantages to being an OHCA?

There are several advantages to being an OHCA:

- *Joint health care operations.* OHCA members may disclose information between and among themselves for purposes of joint health care operations. For instance, if a company wants to combine PHI from each of its group health plans

for purposes of data analysis, it may do so if those group health plans are an OHCA.

- *Joint privacy notice.* If a group health plan that is an OHCA is required to have a privacy notice, the notice can be a joint notice for all members of the OHCA. 45 CFR § 164.520(d).This is especially useful when the group health plan is insured – the insurer's notice satisfies the requirement for both entities.
- *Joint business associate agreements.* A business associate may provide services to an OHCA, but the business associate agreement must be signed by each member of the OHCA.

45 CFR § 160.103 (definition of "business associate"); 45 CFR § 164.501 (definition of "health care operations").

If an employer's group health plan (or plans) meet the definition of an OHCA, they will be one. It is not necessary to document that status. 45 CFR § 164.501 (definition of "organized health care arrangement").

B. COVERED HEALTH CARE PROVIDERS

What is a health care provider?

The term health care provider is defined broadly and includes:

- a provider of services as defined in section 1861(u) of the PHS Act, 42 USC § 1395x(u), including, for example, a hospital,
- a provider of medical or health services as defined in section 1861(s) of the PHS Act, 42 USC § 1395x(s), for example a physician, and
- any other person or organization who furnishes, bills, or pays, or is paid for health care in the normal course of business.

45 CFR § 160.103 (definition of "health care provider").

The last part of the definition in particular is meant to be functional – a person is a health care provider if the activities in which the person is engaged meet the definition of health care. The term "health care" is defined to mean care, services, or supplies related to the health of an individual, and includes, but is not limited to:

- preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual, or that affects the structure or function of the body; and
- sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

45 CFR § 160.103 (definition of "health care").

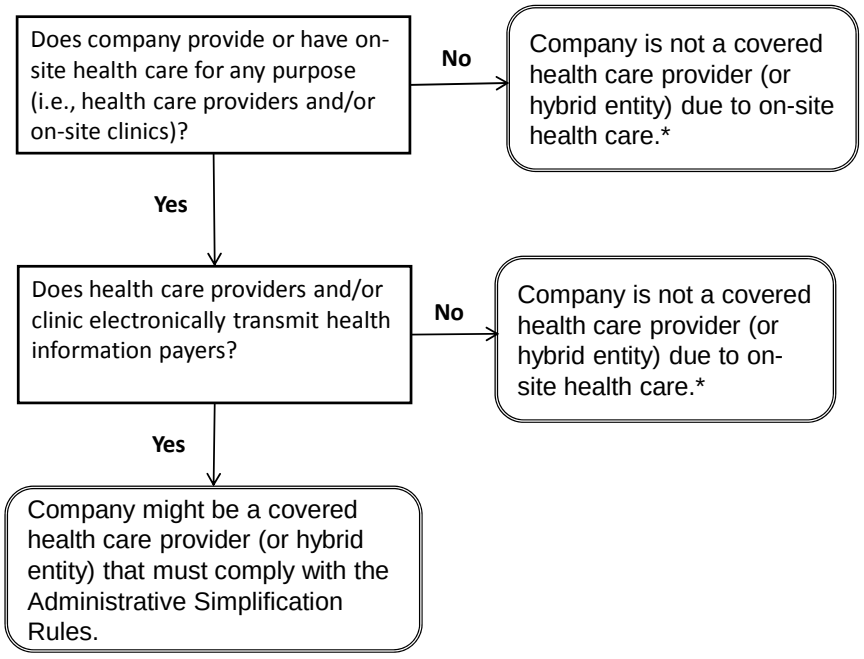
When are health care providers covered under the Administrative Simplification Rules?

Health care providers are "covered" and must comply with the Administrative Simplification Rules only if they (or someone on their behalf such as a billing service) transmit health information in electronic form to payors. 45 CFR § 160.103. These transactions are required to be in formats specific to the Electronic Transactions Rules, which are beyond the scope of this paper.

Are companies that have medical professionals who provide services on-site covered entities?

An employer that provides health care to its employees in kind will be a covered health care provider only if it transmits health information electronically to payors. Note that if such an employer were subject to ERISA, the provision of health care services to its employees could be treated as an ERISA welfare benefit plan and, if so, would be subject to ERISA's requirements including reporting and disclosure, as applicable. However, such services would **not** be treated as a group health plan under the Administrative Simplification Rules because of the exclusion of on-site medical clinics from the definition of covered health plans (see discussion above).

The following decision tree may be of assistance in determining whether an on-site clinic is covered under HIPAA:



*However, company may have HIPAA Administrative Simplification compliance obligations because it offers a covered group health plan or because the company is a covered entity in and of itself (a health insurer, an HMO, a doctor's office, etc.).

Are medical professionals who provide on-site services covered health care providers?

Yes, if, on their own behalf, they electronically transmit health information to payors. Such a professional would be acting on his or her own behalf if he or she was billing for his or her own services, and not for services on behalf of the employer.

What is a hybrid entity?

The Privacy Rule created the concept of a "hybrid entity" to help an entity that is partially a covered entity, and partially not, comply with the Privacy Rule. A hybrid entity is:

- a single legal entity,
- that is a covered entity,
- whose business activities include both covered and non-covered functions, and
- that designates the covered entity parts of itself as one or more health care components.

45 CFR § 164.504(a) (definition of "hybrid entity").

"Covered functions" are activities that would make the component a covered entity if it were a separate legal entity. 45 CFR § 164.501 (definition of "covered functions"). A prime example of a hybrid entity is a company with an on-site medical clinic that is considered a "covered provider" under the Administrative Simplification Rules. The on-site clinic is not a separate legal entity, but the company's activities involve covered and non-covered functions (*i.e.*, the company's core business, such as making widgets, and its clinic activities).

Hybrid entity status is voluntary. If elected, it enables an entity that has both covered and non-covered functions to limit its compliance with the Privacy Rule to only those components of its business designated as covered components. If hybrid entity status is not elected, such an entity would have to comply with the Privacy Rule with respect to all of its operations. The health care components of a hybrid entity must be documented. To the extent components are designated and documented, PHI may be shared between them in accordance with the Privacy Rule. Any disclosure to a non-designated or non-documented component can only occur to the extent and under the circumstances required by the Privacy Rule for disclosures to separate legal entities (*e.g.*, with the individual's written authorization). 45 CFR § 164.504(c)(3)(iii).

What compliance requirements apply to a hybrid entity?

A covered entity that is a hybrid entity must ensure that each covered component complies with the Privacy Rule. 45 CFR § 164.504(c).

Specifically, it must ensure that:

- the covered component does not disclose PHI to any other part of the hybrid entity if the disclosure would not be allowed to a separate legal entity,
- if the covered component discloses PHI to another component that it is permitted to treat as part of itself because the other component performs "business associate" types of activities for it, any further use or disclosure of such PHI by the other component is prohibited, and
- if a person is a member of the workforce of a covered component (or a component treated as the covered component, above), and a member of the workforce of another component, the person does not use or disclose PHI in a way prohibited by the Privacy Rule.

45 CFR § 164.504(b), (c)(2).

Notwithstanding its hybrid entity status, the entity responsible for compliance with the Administrative Simplification Rules generally, and with the Privacy Rule in particular, is the single legal entity. This compliance burden includes the creation of "firewalls" between covered and non-covered components where necessary to keep PHI from being improperly disclosed within the entity. The burden also includes responsibility for designating (and documenting) those parts of itself that are covered health care components. 45 CFR § 164.504(c)(3).

COMPLIANCE CHECKLIST

☑	COMPLIANCE STEP
☐	1. Determine whether your group health plans are subject to the Privacy Rule
☐	2. Determine whether your group health plans are an organized health care arrangement ("OHCA"). If so, decide if you want to treat them as an OHCA, including providing notice in your privacy notice.
☐	3. Determine whether you provide on-site health services to your employees.
☐	a. Consider on-site clinics.
☐	b. Consider other on-site health care providers.
☐	4. Determine whether your on-site clinics and/or health care providers electronically transmit information to payors. If so, they may be covered health care providers.

☑	COMPLIANCE STEP
☐	5. If you have any covered health care providers, determine if you wish to be a hybrid entity. If so:
☐	a. Identify and document your health care components and any support functions in non-health components (*e.g.*, legal department, audit department).
☐	b. Determine where firewalls or other safeguards will be necessary between your covered health care components (including its support functions) and any non-health care/non-support components.
☐	c. Implement the firewalls and safeguards.

III. GROUP HEALTH PLAN COMPLIANCE

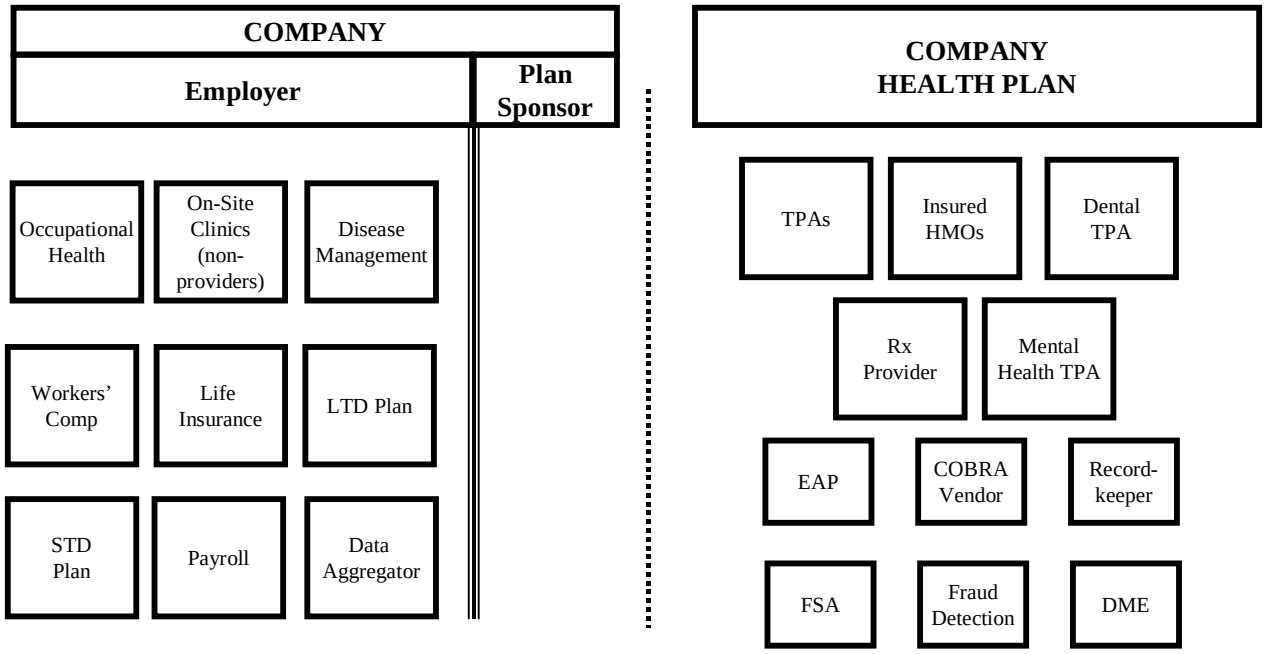
Group health plans are three-ring notebooks. How are they to comply with the Privacy Rule?

As discussed above, most group health plans are covered entities under the Privacy Rule and are expected to use and disclose PHI in accordance with the Privacy Rule like any other covered health plan. However, a group health plan is not like the other covered health plans in some critical ways. For example, it generally exists only in the form of plan documents and generally acts only through the actions of its sponsoring employer's employees.

To accommodate the special nature of group health plans, HHS created an analytical framework that attempts to balance two competing – and potentially conflicting – needs: (1) the need of the employer in its role as plan sponsor for information from its group health plan in order to carry out legitimate plan administration functions, and (2) the need to protect health information in the hands of the employer in its role as employer from being used improperly, *e.g.*, for employment-related purposes.

Under this framework, the group health plan is treated as being completely separate from the employer and the employer is, in effect, divided into two parts: the plan sponsor and the rest of the employer. It is easier to understand how a group health plan is regulated under the Privacy Rule if a company and its group health plan are viewed as two separate legal entities doing business at arm's length, and if the company itself is viewed as further divided into the plan sponsor (comprised of those people who act for and on behalf of the plan) and the rest of the company (comprised of everyone else). The following diagram is intended to show this framework in the context of a hypothetical company. On the far right are the various components that

might be part of a self-insured group health plan. On the left is the company, which is divided into two parts: the employer and the plan sponsor, divided by the bold line.



Generally, the Privacy Rule permits the group health plan to disclose PHI to the plan sponsor part of the employer for certain specified purposes such as plan administration, but only if the plan sponsor agrees to various conditions and restrictions. The Privacy Rule prohibits the disclosure of PHI from either the group health plan or the plan sponsor part of the employer to the rest of employer for any other purposes except to the extent that another covered health plan would be permitted to disclose PHI to an unrelated third party (*e.g.*, pursuant to a written authorization).

If the requirements of the Privacy Rule (*e.g.*, plan amendments) are satisfied for the hypothetical company depicted above, PHI can flow across the dotted line from the group health plan to the plan sponsor. PHI cannot flow across the bold line, however, without the authorization of the person whose information it is or without otherwise being permitted or required by the Privacy Rule.

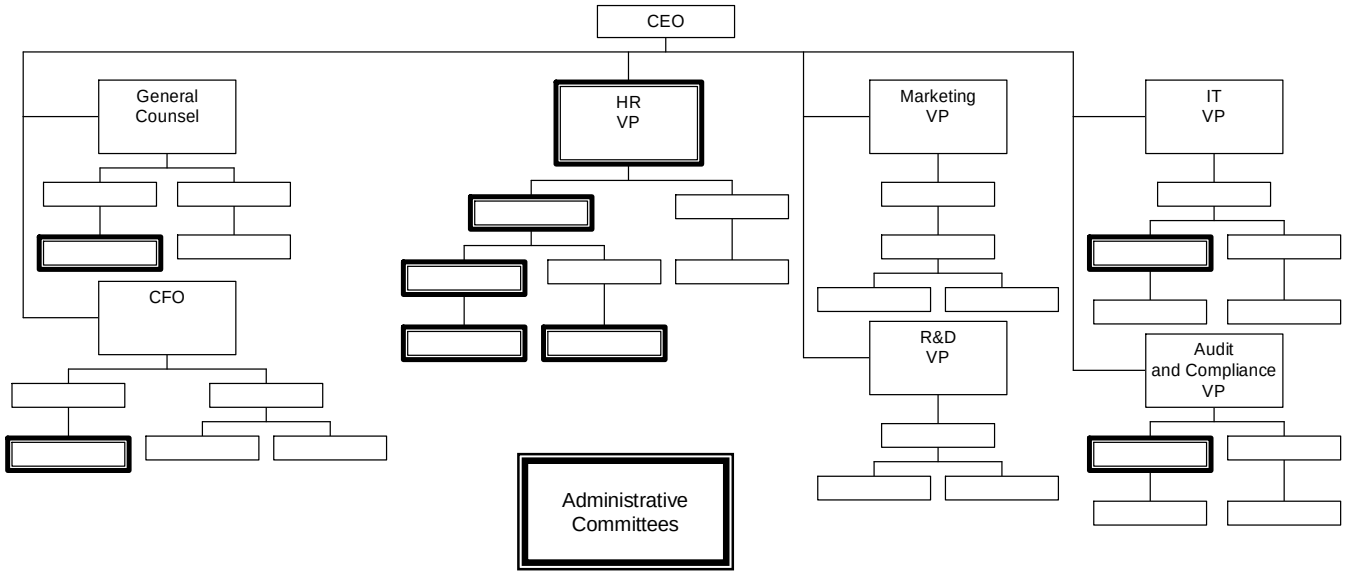
Can you explain the role of the plan sponsor in more detail?

The plan sponsor is defined by reference to ERISA. For single employer plans, this means the plan sponsor is the employer. As a conceptual matter, however, for purposes of the Privacy Rule, the plan sponsor will not be the entire employer. Rather it will be the group of employees who are involved in "plan administration functions," or who are responsible for "settlor functions" – either amending the plan or negotiating service provider contracts for the plan. 45 CFR § 164.103 (definition of "plan sponsor").

Who in a company is considered part of the plan sponsor?

Being a part of the plan sponsor is a matter of function. An employee who performs plan administration or settlor functions for the group health plan will be part of the plan sponsor no matter where in the organization he or she is located (*e.g.*, employees in legal and payroll might perform plan administration or settlor functions and be part of the plan sponsor). An employee who does not perform plan administration or settlor functions for the group health plan is part of the employer, not part of the plan sponsor, wherever he or she might be located in the organization (*e.g.*, employees in human resources who do not work on the group health plan).

The diagram below depicts who is part of the plan sponsor in the context of a hypothetical company. Individuals in boxes marked with a bold line are part of the plan sponsor. All other individuals are not.



What about employees that "wear two hats"?

If an employee "wears two hats" and spends part of his or her time performing plan administration functions, and part performing other functions (*e.g.*, working on other welfare benefit plans), that employee is part of the plan sponsor only to the extent that the employee performs plan administration functions. Additionally, a group health plan will have to take steps to keep such employees from improperly disclosing PHI from the group health plan to the other welfare plans, or to any other part of its company.

Who is the "workforce" of a group health plan?

The term "workforce" is defined in the Privacy Rule as employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. 45 CFR § 160.103 (definition of "workforce"). This definition is not directly

applicable to most group health plans because most such plans are contracts, not corporate entities, and have no employees, volunteers, or others under their direct control. However, HHS indicates that the analogous group for a group health plan is the group of individuals identified in the plan document as performing plan administration functions for the plan and having access to PHI (*i.e.*, the plan sponsor).

Generally, what must a group health plan do to comply with the Privacy Rule?

It first depends on whether the group health plan is self-funded or fully-insured. If it is self-funded, it must comply with all provisions in the Privacy Rule, including the following (not all of these are discussed in this paper):

- Limiting the uses and disclosures of PHI as permitted or required by the Privacy Rule;
- Enforcing individual rights with respect to PHI;
- Providing of a notice of privacy practices;
- Amending plan documents to permit disclosures and uses of PHI for purposes of plan administration;
- Satisfying other administrative requirements including the appointment of a privacy official, implementing safeguards, and training employees.

If, on the other hand, the group health is fully-insured (in other words, buys an insurance policy through an insurance company or an HMO), it has to comply with the provisions listed above only if it receives PHI. If it does not, then its insurer or HMO handles employee PHI and comply with HIPAA as directly-covered entities. Most insured group health plans will want to make sure they do not receive PHI.

Is information regarding the enrollment, disenrollment, and participation status of a participant or a beneficiary in a group health plan treated as PHI?

Although enrollment, disenrollment, and participation information is PHI, the Privacy Rule provides an exception permitting a group health plan, or HMO or insurer acting on its behalf, to disclose to the plan sponsor information on whether an individual is participating in the group health plan, or is enrolled in or has disenrolled from an insurance plan or HMO offered by the group health plan. 45 CFR § 164.504(f)(1)(iii). Receiving that information does not mean the group health plan has to comply with HIPAA's administrative provisions.

The information disclosed under this provision, however, is subject to the minimum necessary requirement and may not include medical information beyond that which is required to determine the enrollment, disenrollment, or participation in the plan.

Is health information held in a company's employment records considered PHI?

Employers themselves are not covered entities; accordingly, health information in their employment records is not subject to the Privacy Rule. If the employer is otherwise a

covered entity (such as a hospital, health insurance company, *etc.*), the Privacy Rule makes clear that information in the company's employment records is not subject to the Privacy Rule. 45 CFR § 164.501.

Employers should consider, each time they create, receive, or use a piece of health information about an employee, whether they are creating, receiving, or using the health information in their capacity as an employer or in their capacity as the plan sponsor of the group health plan. If the latter, then the information is subject to the protections in the Privacy Rule.

When receiving a piece of health information about an employee in its employer capacity, the employer also should determine whether the information came from the group health plan, and if it did, whether the disclosure was properly made.

COMPLIANCE CHECKLIST

☑	COMPLIANCE STEP
☐	1. Identify your group health plan.
☐	2. Identify your "plan sponsor" workforce.
☐	a. Identify (by individual and position) who in the HR Department provides services to the group health plan.
☐	b. Identify (by individual and position) who provides services to each group health plan in other parts of your organization.
☐	c. Identify your plan administrative committees.
☐	3. Determine whether your group health plan is fully-insured or self-insured. Remember to consider your health FSA, which typically is considered, self-insured.
☐	4. Determine whether you currently receive PHI from your group health plan. Consider whether you need to continue to receive PHI. For example, determine whether de-identified or summary health information would be sufficient.
☐	5. Determine whether aggregate information will satisfy your needs for information from the group health plan.
☐	6. Based on items 3-5, determine the compliance category into which your group health plan fits.

☑	COMPLIANCE STEP	
☐	7.	Identify the individuals in your plan sponsor workforce who have access to PHI.
☐	8.	Identify the individuals in your plan sponsor workforce who also provide services to another benefit plan or to the employer and will therefore wear "two hats."
☐	9.	Determine who (by name or position) will act for the plan sponsor (*e.g.*, signing the certification to the group health plan) and memorialize this determination.
☐	10.	Determine if your group health plan currently shares information with any other type of welfare plan or benefit (case management, disability management, data aggregation). If it does, consider how to re-organize this information flow to satisfy the Privacy Rule. (See discussion below.)

IV. ADMINISTRATIVE OBLIGATIONS

What are the administrative obligations imposed by the Privacy Rule?

The Privacy Rule imposes a plethora of administrative obligations on self-insured group health plans (and on fully-insured group health plans that receive PHI other than enrollment and disenrollment information). Except where noted specifically below, fully-insured group health plans (*i.e.,* group health plans providing all benefits through insured contracts or HMOs) that do not receive PHI – other than enrollment and disenrollment information – are exempt from many of the administrative requirements. 45 CFR § 164.530(k).

As discussed in more detail in the sections below, a group health plan that is subject to these requirements is obligated to:

- Designate a privacy official and a contact person
- Create privacy policies and procedures
- Educate plan sponsor personnel
- Safeguard PHI
- Implement a complaint process
- Impose sanctions
- Mitigate harm due to improper uses or disclosures of PHI
- Refrain from retaliation
- Not seek waivers of individual rights
- Document its compliance with the Privacy Rule

A. Privacy Official and Contact Person

Does every group health plan need to designate a privacy official and contact person?

No. Only self-insured group health plans and fully-insured group health plans receiving PHI must designate a privacy official and a contact person (or office). Group health plans do not need to hire new personnel to fill these positions; instead, these roles may be given to existing employees. A company offering more than one group health plan must designate a privacy official for each group health plan, but the same person can serve as the privacy official for each. 45 CFR § 164.530(a)(1), 164.530(k).

Fully-insured plans that do not create or receive PHI other than information regarding enrollment or disenrollment are not required to designate a privacy official or contact person. 45 CFR § 164.530(k).

What duties does the privacy official perform?

A group health plan's privacy official is responsible for developing and implementing the plan's policies and procedures under the Privacy Rule, and for the group health plan's compliance with the Privacy Rule generally. The privacy official also must oversee the plan's maintenance of and adherence to these policies. 45 CFR § 164.530(a)(1)(i). While many obligations are listed under the Privacy Official's job duties, as a legal matter, it is the group health plan, not the privacy official, ultimately responsible for meeting them.

What duties the contact person (or office) perform?

The group health plan's contact person is responsible for receiving complaints about the group health plan's privacy practices. This person is also responsible for providing more information about items described in the group health plan's notice of privacy practices. A group health plan must list its contact person (or office) in its notice of privacy practices. 45 CFR § 164.530(a)(1)(ii). The contact person or office will also be listed in any letters denying participant's or beneficiary's requests for access to or amendment of PHI.

The same person can be designated as a group health plan's privacy official and contact person, but they are not required to be the same person. Moreover, each of these positions can be combined, alone or together, with other duties. Whether an employer chooses to designate separate people to handle each responsibility will depend on the size of the group health plan.

B. Privacy Policies and Procedures

What are the requirements regarding privacy policies and procedures?

Group health plans must document their privacy policies and procedures to comply with the Privacy Rule's requirements. Documentation may be in written or in electronic form.

Certain privacy practices outlined in a group health plan's policies and procedures must be included in its notice of privacy practices. 45 CFR § 164.530(i)(1), (j)(i). The purpose of the policies and procedures is to ensure that group health plans do not make privacy decisions on an ad hoc basis. Written policies and procedures also facilitate workforce (*i.e.,* plan sponsor) training (see below).

The drafters of the Privacy Rule intended for covered entities, such as group health plans, to have the flexibility to design policies and procedures best suited to their businesses and information practices. Accordingly, the Rule does not require any standard format for the policies and procedures.

When should a group health plan revise its policies and procedures?

Permissible changes. A group health plan may revise its policies and procedures at any time, provided that the change does not affect the content of its privacy notice. If the change would affect the content of its privacy notice, the group health plan may not implement the change until it has issued a revised privacy notice. 45 CFR § 164.530(i)(4)(i), (i)(5)(i).

Required changes. A group health plan is required to revise its policies and procedures to comply with changes in the law. If such a change affects its privacy notice, it must revise and distribute its privacy notice before implementing the change. Such revisions and distribution must be accomplished promptly, however, because the Privacy Rule emphasizes that the group health plan is not excused from complying with the new law simply because it fails to quickly distribute its new privacy notice. 45 CFR § 164.530(i)(3).

Can revised policies and procedures apply retroactively?

A group health plan's changes to its privacy policies and procedures that result in a change in its privacy notice will apply prospectively only, unless the group health plan reserves the right in its privacy notice reserving the right to do so. 45 CFR § 164.530(i)(2). If the privacy notice does not reserve the right to apply policy changes retroactively, then the group health plan may apply those changes only to PHI created or received after the effective date of the notice. 45 CFR § 164.530(i)(4)(ii)(B). For ease of administration, group health plans probably will want to make sure their privacy notices reserve the right to make retroactive policy changes.

C. TRAINING OF PLAN SPONSOR PERSONNEL

What training requirements are imposed by the Rule and who must be trained?

A group health plan must train its "workforce" on its privacy policies and procedures so that those workforce members can carry out their jobs relating to the group health plan. Group health plans rarely have employees; instead, the group health plan is administered by the workforce of the plan sponsor. It is reasonable to assume that, in

the group health plan context, it is the plan sponsor workforce that should be trained in the group health plan's privacy policies and procedures. 45 CFR § 164.530(b)(1).

When must training occur?

A group health plan must train new workforce members within a reasonable time. It also must re-train its workforce within a reasonable time after any material changes to its policies or procedures. 45 CFR § 164.530(b)(B), (C).

Do I need to collect training certifications from workforce members?

No. The Rule requires the group health plan to document its training, but it does not require employees to sign a certification following training. Even though it is not required, consider having trained workforce members sign a certification acknowledging their training and duties with respect to maintaining the privacy of PHI. Such a step might emphasize to these employees the importance of complying with the group health plan's privacy policies and procedures.

D. SAFEGUARDING PHI

What safeguards should I create for PHI?

You must put in place administrative, technical, and physical safeguards to ensure the privacy of PHI. To meet the Privacy Rule's requirements, these safeguards must provide reasonable protections against any use or disclosure (intentional, unintentional, or incidental) of PHI that the Privacy Rule does not permit you to make. 45 CFR § 164.530(c). Safeguards must be appropriate and adequate for your operations. The Privacy Rule does not require that any specific technologies be used. The requirement is intended to be flexible and to allow implementation at a reasonable cost.

E. COMPLAINT PROCESS

What kind of complaint procedures must exist?

Group health plans must establish an internal complaint process with two key features. First, they must identify a contact person in their notice of privacy practices to whom complaints may be sent, as discussed above. Second, they must accept and document complaints about (1) the contents of their policies and procedures; (2) their compliance with their policies and procedures; or (3) their compliance with the Privacy Rule. The Rule does not require group health plans to respond to complaints within a given time frame. 45 CFR § 164.530(d)(1).

What can participants and beneficiaries do if they are unhappy with the results of a group health plan's complaint process?

Individuals have no appeal rights if they are not satisfied with the results of the complaint process. They can, however, take their complaints to HHS, which may give

group health plans an incentive to work to resolve the complaints internally – especially given the increased HIPAA penalties enacted by ARRA.

Are participants and beneficiaries required to exhaust the group health plan complaint procedures before complaining to HHS?

No. There is no requirement that participants and beneficiaries file a complaint with the group health plan, or wait until such complaint is resolved, before filing a complaint with HHS.

F. SANCTIONS

Are sanctions required for employees who violate the Privacy Rule?

Yes. Group health plans must have sanctions in place to apply when a workforce member (*i.e.*, a member of the plan sponsor) violates the group health plan's privacy policies and procedures or violates the Privacy Rule. 45 CFR § 164.530(e)(1).

What kinds of sanctions are required?

The type of sanction imposed for violations of a group health plan's policies and procedures or the Privacy Rule depends on the facts of each breach. Factors to consider would include whether the violation was intentional or unintentional, whether the violation indicated a pattern or practice of improper use or disclosure, *etc.* The actual sanction could range from a warning to termination. In essence, however, the group health plan will be able to determine appropriate sanctions at the time of violation.

G. MITIGATION OF HARM

What must a group health plan do if it learns that it has used or disclosed PHI improperly?

Group health plans must mitigate any harmful effect that is known to it that is caused by a use or disclosure of PHI that violates its privacy policies and procedures or that violates the Privacy Rule. This requirement also applies to improper uses or disclosures by the group health plan's *business associates*. 45 CFR § 164.530(f).

Are group health plans required to monitor business associates?

No. The Privacy Rule does not require group health plans to monitor their business associates. If a group health plan learns of a violation by its business associate, either through its own business dealings, through a complaint from a participant or beneficiary, or otherwise, then it is required to mitigate the harm.

H. Prohibitions on Undermining Privacy Rights

Who is protected from retaliation and intimidation?

Participants or beneficiaries are protected from retaliation or intimidation relating to the exercise of their individual rights, including the right to file a complaint with the group health plan or with HHS. 45 CFR § 164.530(g)(1). All persons, including any type of organization or group, are protected from retaliation or intimidation for filing a complaint with HHS, testifying or participating in an investigation, or opposing any acts violating the Privacy Rule. 45 CFR § 164.530(g)(2).

Fully-insured group health plans are not exempt from this requirement.

Can a group health plan require potential participants or beneficiaries to waive their Privacy Rule rights in order to enroll?

No. None of the rights in the Privacy Rule can be waived. It is a violation of the Rule for a group health plan to request waiver of any rights prior to enrolling a participant or beneficiary, or prior to paying for or providing health benefits. 45 CFR § 164.530(h).

Fully-insured group health plans are not exempt from this requirement.

I. Documentation Requirements

What are the documentation responsibilities?

A group health plan must maintain the following documents for six years:

- Its official policies and procedures with respect to PHI. 45 CFR § 164.530(j).
- Designation of its privacy official and contact person or office, if applicable. 45 CFR § 164.530(a)(2).
- All complaints received through the complaint procedures described above and the disposition of those complaints. 45 CFR § 164.530(d)(2).
- Any sanctions imposed on members of its workforce who violate its privacy policies and procedures, if any.
- Any changes to its privacy policies and procedures. 45 CFR § 164.530(i).

The group health plan may keep this documentation in either written or electronic form. 45 CFR §164.530(j)(2).

COMPLIANCE CHECKLIST

☑	COMPLIANCE STEP
☐	1. Determine which of your state's privacy laws are not preempted by ERISA, and then consider whether any of them apply by virtue of being "saved" by HIPAA.
☐	2. Determine who, under applicable state law, can be a "personal representative."
☐	3. If your group health plan is self-insured, or, if it is fully-insured and receives PHI, designate a privacy official and a contact person. Determine whether these will be separate positions and whether you will combine these functions with existing job duties.
☐	4. Develop a job description for your privacy official; consider identifying within your company who will be the privacy official, or, if necessary, hire a privacy official.
☐	5. Identify your group health plan contact person or office; determine if the contact person will be the same person as your privacy official.
☐	6. Draft your group health plan's official policies and procedures for complying with the Privacy Rule.
☐	7. Train your group health plan workforce (*i.e.*, your plan sponsor workforce) on the group health plan's privacy policies and procedures.
☐	a. Set up a system so that new employees receive training.
☐	b. Set up a system so that training re-occurs whenever the group health plan's policies and procedures are materially altered.
☐	8. Determine the steps you will take to safeguard PHI.
☐	9. Identify where group health plan data is stored, whether electronically or physically (*i.e.*, in paper form).

☑	COMPLIANCE STEP
☐	a. For paper records: i. Determine who should have access to the data; ii. Determine how access to the data will be limited (locked filing cabinets, locked offices, *etc.*). iii. Determine whether an access log (written statement of who accesses the data and when) is prudent.
☐	b. For oral communications: determine how to safeguard the disclosure of oral communications.
☐	10. Create procedures for receiving and handling complaints concerning the group health plan's privacy practices.
☐	11. Determine the sanctions process for group health plan workforce members (*i.e.,* plan sponsor workforce members) who violate the group health plan's privacy policies and procedures or the Privacy Rule.
☐	12. Determine where documentation required by the Rule will be kept and whether it will be in electronic or written form, or both.
☐	13. Review document retention policies to ensure Privacy Rule required documentation is retained for the appropriate period.

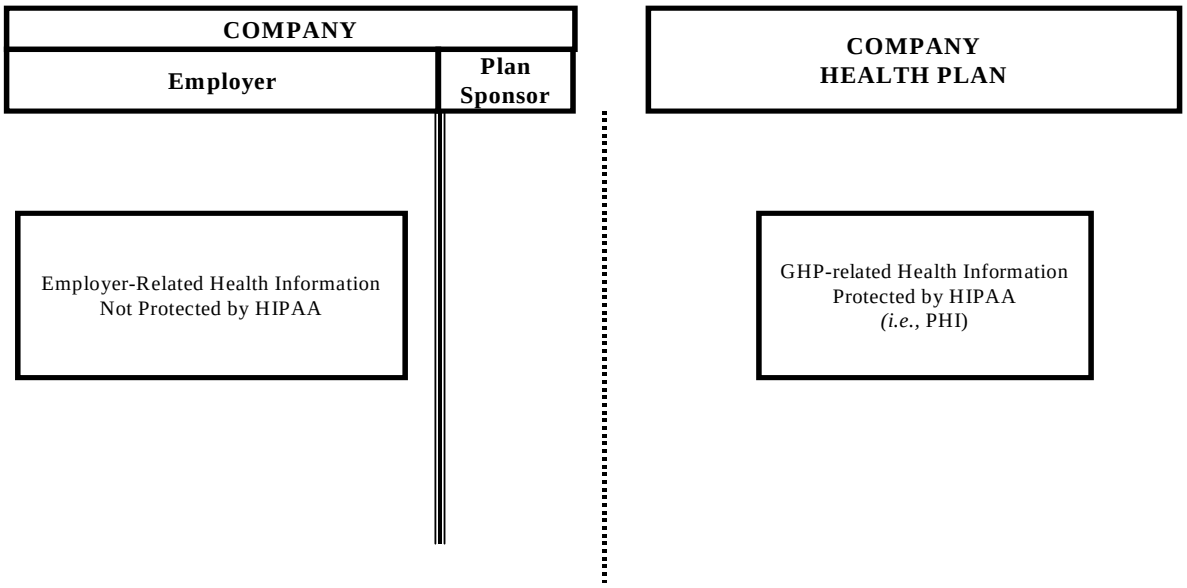
V. COMMON WORKPLACE ISSUES

Is all employee health information protected by the HIPAA Privacy Rule?

No. Only PHI held by covered entities is protected by the Privacy Rule. Information an employer receives in its capacity as employer, even if relating to an employee's medical condition, is not protected by the Privacy Rule. On the other hand, information held by an employer's group health plan or other covered entity ***is*** protected by the Privacy Rule. Similarly, if an employer has on-site covered health care providers, as discussed above, those covered providers will need to comply with the Privacy Rule.

The following diagram represents this concept in the context of a hypothetical company. On the far right is the group health plan. On the left is the company, which is divided into two parts: the employer (on the left of the bold line) and the plan sponsor (on the right of the bold line). Health information received by a company in its capacity as employer (*i.e.,* on the left side of the bold line) is not subject to the Privacy Rule. Health

information received by the company's group health plan, including the plan sponsor, (on the right side of the bold line) ***is*** subject to the Privacy Rule.



Most questions about whether employee health information is subject to the Privacy Rule can be resolved by considering this diagram and on which side of the bold line the health information is received or otherwise maintained. Section A, below, addresses common uses of information involving the group health plan and are governed by the Privacy Rule. Section B addresses common uses of health information that generally are not governed by the Privacy Rule because the information is received or maintained by the employer and not the group health plan.

A. GROUP HEALTH PLAN ISSUES

How does the Privacy Rule affect an employer's response to inquiries from participants or beneficiaries about another family member's status or benefits?

The Privacy Rule affects how a group health plan may respond to inquiries from one person about another person's status and benefits. It permits disclosures to individuals acting as the personal representative of participants and beneficiaries. It also permits, in certain circumstances, disclosures to family members or friends involved in a participant's or beneficiary's health care. Note, however, that participants and beneficiaries can limit access to their records by personal representatives, family members, and friends, by requesting restrictions or requesting that communications regarding their PHI be treated confidentially.

Personal representatives. Generally, a group health plan may disclose health information to the personal representative of a participant or beneficiary and should treat the personal representative the same as the participant or beneficiary (but only

with respect to PHI relevant to such personal representation). 45 CFR § 164.502(g)(1), (2).

There are two major exceptions to this rule:

- Certain disclosures to parents or guardians of non-emancipated minors. The Privacy Rule defers to state law with respect to the access of parents and guardians to the PHI of unemancipated minors. 45 CFR § 164.502(g)(3)(ii).
- In situations where the group health plan believes that it is not in the best interests of the participant or beneficiary to treat someone as his or her personal representative because:
  - The group health plan reasonably believes the participant or beneficiary has been or may be abused or neglected by the personal representative; or
  - The group health plan reasonably believes that the participant or beneficiary will be endangered if the personal representative is treated as such.

45 CFR § 164.502(g)(5). Personal representative status is determined under "applicable law," which most often is state law. For instance, state law governs parental rights, court-appointed guardianships, and powers of attorney. Generally, these laws are not preempted by ERISA.

Family members and friends. A group health plan may disclose to a participant's or beneficiary's family member, other relative, or close personal friend (or anyone else identified by the participant or beneficiary), PHI directly relevant to that person's involvement with the individual's care or payment related to the individual's care. This type of disclosure may be made in limited circumstances with the oral consent of the participant or beneficiary or with his or her implicit consent.

If the participant or beneficiary is present, the group health plan may make the disclosure if he or she agrees or, upon given an opportunity to object, the participant or beneficiary does not do so. 45 CFR § 164.510(b)(2)(i), (ii). If the participant or beneficiary is present, and if the group health plan reasonably infers from the circumstances that he or she does not object to the disclosure, then the disclosure is permitted. 45 CFR § 164.510(b)(2)(iii). Finally, if the participant or beneficiary is not present, a group health plan may nevertheless make a disclosure of PHI to the relative or close friend if:

- the disclosure is in the best interests of the individual; and
- the PHI disclosed is limited to that directly relevant to the person's involvement in the participant's or beneficiary's health care.

45 CFR § 164.510(b)(3). Note that disclosure under this provision requires the group health plan to exercise its discretion in determining whether a disclosure may be made to a family member or friend. Group health plans should carefully consider the circumstances in which they can respond to requests from family members about

another family member's status or benefits. For example, a group health plan should determine whether a non-participant spouse, who presumably is involved in his or her spouse's health care, should have access to all of a participant spouse's PHI or only to specified categories of information (*e.g.,* enrollment status and claims payment status).

Restrictions and confidential communications. Participants and beneficiaries can limit the disclosures discussed above by requesting that a group health plan provide communications of PHI by alternative means or at alternative locations, if the participant or beneficiary states that the disclosure of the information could endanger him or her. 45 CFR §164.522(b)(1)(ii).

Can an employer still advocate or troubleshoot for its employees in getting their claims paid?

Yes. Plan sponsors may still assist employees with their questions about unpaid claims, but in some instances may need to provide an authorization from the participant or beneficiary to the insurance issuer or HMO before that entity will disclose PHI.

If an employer wishes to receive PHI (and thus complies with all the HIPAA Administrative Simplification requirements), when it amends its plan documents, it can list employee advocacy as a permitted use. In this case, the group health plan or insurance issuer or HMO related to the group health plan may reveal the information to the plan sponsor in accordance with the plan amendment. No further authorization would be required.

If the plan sponsor does not otherwise receive PHI from the group health plan, and thus is not required to comply with all the HIPAA Administrative Simplification requirements, the insurance issuer or HMO will require written authorization from the employee.

Does the Privacy Rule impact a self-funded group's final review of denied claims?

A plan sponsor conducting the final review of denied claims for its group health plan must comply with both the Department of Labor Claims Review Regulation and the Privacy Rule. Certain aspects of the Department of Labor Claims Review Regulation will be affected by the Privacy Rule. Under the Claims Review Regulation, if the appeal of a denial involves a medical judgment, the named fiduciary must consult with a health care professional who was not involved in the initial denial. Some companies may need to contract with outside entities to provide this service. If so, those entities will be business associates of the group health plan and the group health plan must ensure that it complies with the Privacy Rule's business associate requirements.

Additionally, the Claims Review Regulation provides that when a claimant appeals a denied claim, he or she must be provided access to all documents, records, and other information relevant to his or her claim. A relevant document is one that was relied upon in making the determination, a document that was submitted (even if not relied upon), or one that demonstrates compliance with the administrative processes and safeguards required by the Claims Review Regulation. The Department of Labor has clarified that "relevant documents" do not include other claimants' appeal records or

appeal records from which a plan develops its criteria, guidelines, or policies used to demonstrate consistency in the claims review process. Accordingly, there is no conflict between this requirement and the Privacy Rule's limits on disclosures of PHI (*i.e.,* the Claims Review Regulation does not require disclosure of other participant or beneficiary PHI during the claims review process – something that if required, would conflict with the Privacy Rule). 29 CFR § 2560.503-1(h)(2).

Does the Privacy Rule impact a group health plan's compliance with the requirements of COBRA (e.g., COBRA notices, enrollment/disenrollment)?

COBRA requires that certain individuals who would otherwise lose coverage under the group health plan be allowed to continue coverage at their own expense for a limited period of time. COBRA compliance, therefore, largely involves enrollment information and activities.

The plan sponsor is acting on the individual's behalf when conducting enrollment activities, and therefore the information is not subject to the Privacy Rule. Similarly, the group health plan may give participation and enrollment information to the plan sponsor without it being considered a disclosure of PHI. Therefore, the Privacy Rule should have little impact on COBRA enrollment and disenrollment activities. Once the individual is enrolled in the group health plan, however, his or her PHI is subject to the Rule. 45 CFR § 164.504(f)(1)(iii).

Does the Privacy Rule affect a group health plan's compliance with Title I of HIPAA (e.g., certificates of creditable coverage)?

Under the portability provisions in HIPAA (Title I), participants and beneficiaries must be provided with certificates of creditable coverage upon leaving a group health plan. The certificates indicate how long the individual was covered under the group health plan and have the effect of shortening or avoiding any exclusionary period in a new health plan. Issuing the certificates of creditable coverage – even if they are considered PHI – should create no issue under the Privacy Rule, provided they are issued directly to the participant or beneficiary. It is the participant or beneficiary who then voluntarily discloses that PHI to another entity.

Does the Privacy Rule impact the use of a group health plan's case or disability management services?

Yes, provided the case or disability manager is part of the group health plan or is a business associate of the group health plan. If the case or disability manager is part of the group health plan (or contracts directly with the group health plan and thus is a business associate), then disclosures between the group health plan and the case or disability manager are permissible. The use of the PHI in that situation is considered "health care operations" and may occur without written authorization. In addition, the case or disability manager may obtain health information from other sources outside of the group health plan (*e.g.,* a long term disability plan) without raising Privacy Rule issues (because those other plans are not covered entities).

On the other hand, if the case or disability manager contracts with the employer (not the group health plan), then any disclosure from the group health plan to the case or disability manager would have to comply with the Privacy Rule. That is, it would not be permissible unless specifically allowed under the Rule or pursuant to written authorization from each participant or beneficiary. In summary, health information can flow from other plans (non-covered entities) into the group health plan for case or disability management purposes, but cannot flow in the other direction except as permitted under the Privacy Rule (*e.g.*, with written authorization). Because of this, group health plans might wish to ensure that their case or disability manager is housed in the group health plan.

Does the Privacy Rule impact the use of data aggregation services?

Generally, data aggregation is considered a "health care operation" and the use of the PHI by the group health plan or its business associate for purposes of data analysis or aggregation purposes is permitted. However, if the group health plan is fully insured and does not receive PHI, its insurance issuer or HMO will not disclose PHI to the plan's data aggregator. This is because the data aggregator is the agent of the plan – thus, the plan will receive PHI through its agent, and disclosing PHI to its agent is the same as disclosing the PHI to the plan. The plan is not compliant with the HIPAA Administrative Simplification provisions, and thus the disclosure to its agent is a HIPAA violation.

Does the Privacy Rule impact group health plan disclosures of PHI for purposes of workers' compensation?

Yes. Group health plans may disclose PHI "as authorized and to the extent necessary" to comply with workers' compensation laws without obtaining an authorization from the participant or beneficiary. Often the disclosure will be required by law, and the Privacy Rule permits disclosures required by another law to be made without obtaining an authorization. However, to encompass those workers' compensation laws that may be written as permissive, rather than mandatory, the Rule provides a specific provision independently permitting these disclosures. 45 CFR § 164.512(a), (*l*).

Under the special workers' compensation disclosure rule, a group health plan may disclose PHI regarding a participant or beneficiary to an entity responsible for payment of workers' compensation benefits to that individual. The group health plan also may disclose PHI to an agency responsible for administering or adjudicating an individual's claim for workers' compensation benefits. Any state or federal law that has the effect of providing benefits for work-related injuries or illness without regard to fault is, for purposes of the Privacy Rule, a workers' compensation law. This includes the Black Lung Benefits Act, the Federal Employees' Compensation Act, the Longshore and Harbor Workers' Compensation Act, and the Energy Employees' Occupational Illness Compensation Program Act. 45 CFR § 164.512(*l*).

When providing medical information to the workers' compensation payer or agency, group health plans cannot provide the entire medical history. Instead, in order to

comply with the Privacy Rule's minimum necessary requirement, they should provide only those parts of the medical history that relate to the injury at issue

B. EMPLOYER ISSUES

How does the Privacy Rule impact the use and disclosure of health information collected for purposes of drug testing, pre-employment physicals, and fitness for duty examinations?

Employers may require, or may be required by federal or state law, to have their employees undergo certain medical exams. For example, the U.S. Department of Transportation requires drug testing for all applicants employed in safety-sensitive positions.

This medical information, once received by the employer, is not subject to the Privacy Rule's protections. It is not received by the employer or its plan sponsor from the group health plan. Instead, it is received by the employer from a medical professional who conducted the exam at the employer's request. The medical professional is likely a covered entity under the Privacy Rule. This means that before the medical professional releases the information to the employer, the individual whose medical information is at issue must sign an authorization permitting the disclosure.

Because employees may refuse to voluntarily sign the authorizations (especially in drug-testing scenarios), employers may condition employment on the signing of an appropriate authorization form. Also, covered health care providers can condition their services on the signing of an appropriate authorization when the services are solely to create PHI to be disclosed to a third party (*e.g.*, an employer). 45 CFR § 164.508(b)(4)(iv).

Employers may not obtain medical information from the group health plan for purposes of determining fitness for duty. That information may be released only as permitted under the Privacy Rule. Absent a specific regulatory provision permitting the disclosure, an authorization would be needed from the individual before the PHI is disclosed.

May an employer require doctors' notes to establish the need for paid sick leave?

Nothing in the Privacy Rule affects an employer's policy of requiring an employee to present a note from a medical professional to establish that employee's entitlement to sick leave. Where these notes are given to an employer by the employee, an authorization is not required (as it is in the pre-employment physical, drug testing, *etc.*) because the disclosure is being made by the employee, not by a covered entity. The employer is receiving the information in its capacity as employer, not plan sponsor. Where the employer requires a communication directly from the medical professional, the analysis is the same as for drug testing, pre-employment physicals, *etc*., (see above).

May employers collect and report health information for OSHA/health surveillance purposes (e.g., exposure to toxic substances, work-place injuries)?

Many employers are required to collect and report medical information about their workforce members. For instance, under the Occupational Safety and Health Act ("OSHA"), employers must record work-related injuries if medical treatment is necessary. OSHA also requires monitoring of employees' exposure to certain substances. In order to obtain this information, employers typically use either private off-site medical providers or, if available, medical providers who are members of their workforce.

The Privacy Rule permits covered health care providers to disclose to employers PHI that is collected for the purpose of complying with OSHA, the Federal Mine Safety and Health Act, and similar state laws, without obtaining an individual authorization from employees. 45 CFR § 164.512(b)(v).

In order to make use of this exception to the authorization requirement, however, a covered health care provider must give written notice to each employee that his or her PHI will be disclosed to the employer. If the health care is provided at the employer's work-site, then the covered health care provider may comply with the distribution requirement by posting the notice in a prominent place where the health care is provided. 45 CFR § 164.512(b)(*v*)(D)(1).

Note that this rule applies to the providers offering the medical care to the extent that they are covered providers. It does not apply to the employers and it does not implicate the employer's group health plan. Information from the group health plan's records relating to a workplace injury or workplace monitoring cannot be disclosed unless required by law or pursuant to an individual authorization.

How does the Privacy Rule affect compliance with other federal employment laws (e.g., FMLA, ADA, Title VII, Rehab Act)?

Employers often receive medical information about their employees unrelated to their employer-sponsored health benefits. For instance, employers might need medical information to substantiate a requested accommodation under the Americans with Disabilities Act ("ADA") or requested leave under the Family Medical Leave Act ("FMLA"). The Privacy Rule should not affect an employer's ability to receive the necessary medical information.

Whenever an employer receives medical information relating to its FMLA, ADA, Title VII, *etc.*, compliance, it should ask whether it is receiving the information from an employee or medical provider in its role as employer, or instead, is receiving the information from the group health plan in its role as plan sponsor. If it is receiving the medical information in its role as employer, then the information is not protected by the Privacy Rule.

For example, an employer may need medical information from a medical professional establishing an employee's need for a reasonable accommodation under the ADA. The

Privacy Rule does not protect the information once it is in the hands of the employer. (Note, however, that it is protected under the ADA.)

The provider, of course, is subject to the Privacy Rule, and may not disclose the medical results to the employer without an authorization from the employee. Such an authorization will likely be freely given since the employee has an interest in receiving the ADA accommodation. Again, that medical information, once given to the employer, is not subject to the Privacy Rule's protections (but the medical professional disclosing the information will need an authorization from the individual to disclose the PHI to the employer).

The analysis is similar under the FMLA, where the employee may need to establish a medical need for family leave.

Does the Privacy Rule impact an employer who wishes to offer flu shots to its employees?

Yes, but if those flu shots are offered through an on-site clinic or provider that is a covered health care provider under the Administrative Simplification Rules, then the Privacy Rule applies. If, however, flu shots are offered by an employer and are unrelated to its group health plan (for example, through a contract with a local medical clinic), then, from the employer's perspective, that activity is not subject to the Privacy Rule because the employer is not a covered entity. The medical clinic, however, if it is a covered health care provider, would need to ensure that it complies with the Privacy Rule.

DATA SECURITY & COMPLIANCE – PROGRAM 710 – ACC ANNUAL MEETING 2010

ADDITIONAL RESOURCES

- Privacy Rights Clearinghouse: http://www.privacyrights.org/
- National Conference of State Legislatures: www.ncsl.org/default.aspx?tabid=13489
- Federal Trade Commission: http://ftc.gov/bcp/edu/microsites/idtheft/
- Federal Trade Commission Red Flags Rule:
    - Summary of Rule: http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm
    - FTC Red Flags Guide: http://www.ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml
- www.consumersunion.org - List of State Statutes
- ACC Docket –June 2010 - *New Privacy & Security Regulations Solutions*
- Practice Note, US Privacy and Data Security Law: Overview (www.practicallaw.com/6-501-4555)
- Directive 95/46/EC - European Union Directive on data protection
- Sarbanes−Oxley Act of 2002 (SOX), Pub. L. 107-204. This applies to public companies and contains provisions related to e-mail retention, data security and integrity, and oversight — all of which must be considered when outsourcing sensitive data to a cloud model.
- Payment Card Industry Data Security Standard (PCI DSS). This is a set of requirements for enhancing payment account data security, containing specific requirements related to security management, policies and procedures.
- Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191. This Act regulates the use and disclosure of protected health information.
- Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541, et seq. This Act requires federal agencies to develop and implement information security programs relevant to the agency's own operations.
- UK: The Information Commissioner's Office (ICO) 'Personal Information Online Code of Practice' providing organizations who operate online with good practice advice to assist them in complying with the Data Protection Act 1998 (DPA): http://www.ico.gov.uk/ebook/ebook.htm

Extras from ACC

We are providing you with an index of all our InfoPAKs, Leading Practices Profiles, QuickCounsels and Top Tens, by substantive areas. We have also indexed for you those resources that are applicable to Canada and Europe.

Click on the link to index above or visit http://www.acc.com/annualmeetingextras.

The resources listed are just the tip of the iceberg! We have many more, including ACC Docket articles, sample forms and policies, and webcasts at http://www.acc.com/LegalResources.