2016 Advisory Council on Employee Welfare and Pension Benefit Plans

Cybersecurity Considerations for Benefit Plans

June 7, 2016

Statement of Kathryn Bakich, Segal Consulting

Segal Consulting

About Segal

Nation's largest privately held/employee-owned benefits consulting firm

- Founded in 1939 (2014 was our 75th Anniversary)
- 100% employee-owned:
  - 22 offices in the U.S. and Canada
- Over 1,100 consulting and support staff including:
  - 150 credentialed actuaries
  - Technology consultants
  - MDs
  - PharmDs
  - RNs
  - Compliance assistance

Key Considerations for Plan Sponsors

- Understanding HIPAA/HITECH and related laws
- Knowing which programs are subject to HIPAA/HITECH, and when, particularly when changing benefit offerings
- Working with service providers, some of whom have limited understanding of privacy and security obligations
- Adapting to new electronic technology and using it to effectively manage plan benefits and employee communications

What is HIPAA?

- Health Insurance Portability and Accountability Act of 1996
- "Administrative Simplification"
- Compliance Deadlines
  - Privacy—April 14, 2003
  - EDI—October 16, 2003
  - Security—April 20, 2005
- Health Information Technology for Economic and Clinical Health (HITECH) Act
  - Includes requirement to notify participants and HHS when "unsecured" PHI is breached
- Enacted as part of the American Recovery and Reinvestment Act of 2009 (February 17, 2009)

HIPAA

HIPAA Privacy Rule

Protects all types of PHI:

- Electronic
- Written
- Oral

HIPAA Security Rule

- Applies to electronic PHI (ePHI) only
- ePHI = transmitted by electronic media or maintained on electronic media
- Examples:
  - Sent or received via e-mail
  - Stored on computer network
  - Stored on computer (including laptops, netbooks or tablets)
  - Stored on electronic media such as CDs, disks, flash drives, tapes or memory cards (including those in smartphones)

Basic Regulatory Framework Since 2003

Covered Entity: Group Health Plan

- Health plan sponsored by private sector employer
- Multiemployer fund providing health benefits
- Health plan sponsored by public sector employer

BA Agreement

Business Associate ("BA")

- Provides services to Group Health Plan
- Services require PHI
- Examples:
  - Benefit consultants
  - Actuaries
  - Attorneys
  - Auditors
  - TPAs
  - PBMs

Before and After HITECH

Before HITECH	After HITECH
• HIPAA Privacy: BA has ***contractual duty*** to use appropriate safeguards to prevent inappropriate use or disclosure of PHI • HIPAA Security: BA has ***contractual duty*** to implement safeguards • BA has contractual liability only	• HIPAA Privacy: BA has statutory duty to comply with BA Agreement • HIPAA Security Rule: **BA must comply with key requirements of Security Rule and must implement required safeguards** • BA subject to civil monetary penalties and criminal prosecutions & to HHS audits

Covered Entities

- Certain health care providers
- Health plans—such as:
  - ERISA-governed employee welfare benefit plans and multiemployer welfare plans (to the extent they provide health benefits)
  - State and local governmental health plans
  - Health insurers
  - HMOs
- Health care clearinghouses (help providers and plans exchange info electronically)

Not Covered Entities

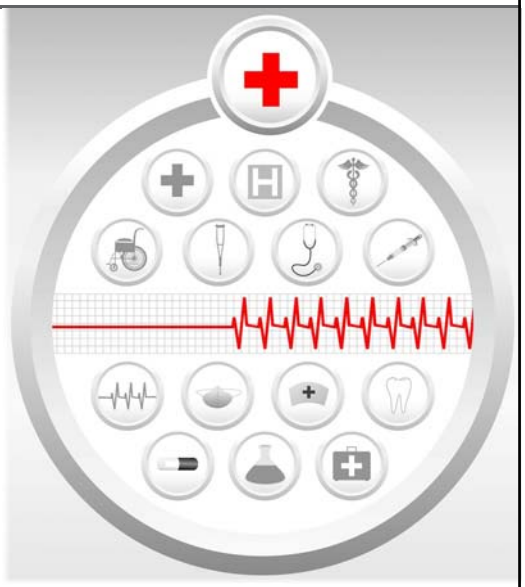
- TPAs, Flex Administrators, PBMs (BA)
- Systems vendors, copier services, storage services, etc. (BA)
- Employers
- Unions
- Pension plans
- Disability plans
- Medical stop-loss insurers
- Life, disability, or workers' compensation insurers

Group Health Plan vs. Plan Sponsor

- Covered Entity is the Group Health Plan (GHP)
- Plan sponsor of the GHP is not a Covered Entity
  - Employer for single employer plan
  - Board of Trustees for multiemployer plan
- HIPAA impacts disclosures to plan sponsors through regulations applicable to GHPs and other Covered Entities
- Enrollment information held by employer generally not considered PHI, but this can be confusing

Covered Benefits

- Medical, dental, vision, behavioral health, Rx
- Health Flexible Spending Arrangements (FSA); Health Reimbursement Arrangements (HRA)
- COBRA
- LTC benefits related to payment for health care
- EAPs that are group health plans providing behavioral health treatment
- Wellness programs



Not Covered Benefits

- Disability
- Life
- AD&D
- Workers' compensation
- Dependent care assistance
- Referral-only EAPs and EAPs that don't provide health care treatment
- Retirement/pension benefits

Human Resources Information Systems

- HRIS or HRM (human resources management) or HCM (human capital management) systems combine both regulated and unregulated functions
  - Provide software hosting & upkeep
  - Call Center – primary point of contact for employee questions
  - Payroll – tax updates, check printing, tax filing, money management & reconciliation, general ledger, leave accruals, EFT & positive pay
  - Provide employee & managerial self-service tools
  - Benefits administration – annual enrollment, ongoing enrollment & eligibility upkeep, family status changes, interfaces to carriers/vendors, bill payment & reconciliation, ongoing data maintenance
  - COBRA & FSA Administration
  - Leave administration
  - Employee advocacy
  - Affordable Care Act Employee Counting, Reporting Compliance

Plan Responsibilities

- Health plans must do three things to assure ongoing HIPAA/HITECH compliance:
  1. Periodic re-assessments,
  2. Update policies and procedures, and
  3. On-going staff training
- Non-health plans should also consider security assessments
- Have process in place to detect and report HITECH Breaches
- Monitor Business Associates
- Exchange data with Business Associates

Risk Assessment

- Complete a risk assessment:
  - Initial HIPAA Security Risk Assessment was likely completed several years ago
  - Risk assessment is an ongoing process as reflected in the HIPAA Security Rule's requirement to **periodically** re-evaluate protocols in response to environmental or operational changes affecting the security of ePHI
  - Periodically – every two or three years + whenever a new electronic technology is adopted or changed
- Risk assessment will review the application standard/implementation specification, make a factual finding, determine the risk to the e-PHI, and make recommendations

Risk Assessment

- The risk assessment should include:
  - All information systems and servers
  - Laptops
  - Mobile devices, wearables and robotics
  - Participant Portals
  - Cloud Storage Services
  - Social Media Presence
- Strongly consider encryption as the best line of protection

Policies, Procedures and Training

- Develop policies and procedures to protect PHI:
  - The Security Rule requires development of policies and procedures that reflect compliance with the Rule, and that are reasonable and appropriate for size and capability
  - Ensure policies address "hot ticket items" such as Bring Your Own Device (BYOD)

- Train staff on the Plan's policies and procedures:
  - The Security Rule requires a security awareness and training program for all workforce members. All training and retraining must be documented
  - As incidents occur, and they will, proper investigation should ensue to assure that any inconsistencies are remediated. Remediation can play an important part in HHS's review of an entity being investigated

Insurers

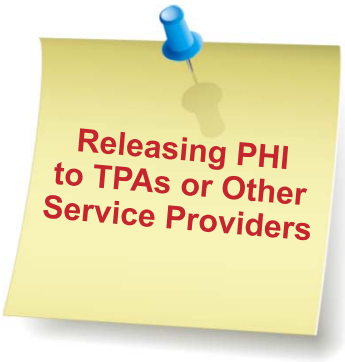
Releasing PHI to Insurers or HMOs

- PHI may be released to both the incumbent and prospective insurers and HMOs
- Insurer/HMO has legal duty to protect the information—even if they are not selected
- No need for confidentiality agreement or Business Associate Agreement

TPAs

Releasing PHI to TPAs or Other Service Providers, Including Insurers in ASO Role

- PHI may be released for bid purposes
- Privacy rules do not specifically address how service provider handles the PHI
- Best practice is to obtain confidentiality agreement

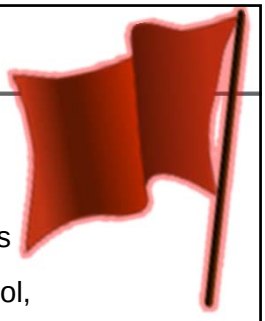


Stop-Loss Insurers

Releasing PHI to Stop-Loss Insurers

- PHI may be released for stop-loss purposes
- Privacy rules do not specifically address how stop-loss insurer handles the PHI
- Best practice is to obtain confidentiality agreement

HIPAA/HITECH
"Red Flag" Issues



- Inadequate encryption policies and procedures
- Poor access control and activity review
- Poor mobile device and laptop policies and controls
- Lack of IT governance—standards, inventory control, basic security procedures (patching, administrative lockdown, etc.)
- Inadequate disaster recovery procedures
- Insufficient IT policies and procedures
- Lack of advanced monitoring techniques—intrusion detection system/intrusion prevention system (IDS/IPS), log correlation, data loss prevention (DLP)
- Lack of a security officer

When Does a Plan Need a Risk Assessment...

- Changing health plan from insured to self-insured
  - A new privacy assessment, policies, and training is necessary
- Putting in a new electronic . . . server, cloud, database, website
  - A new security assessment is necessary
- The HR Office moved – what are the physical security issues for the new location?
  - A privacy and security assessment is necessary
- Developing a mobile health application
  - A security assessment and business associate agreements are necessary
- Giving HR staff . . . I-Pads, tablets, phones
  - A privacy assessment is necessary
- Adopting social media (interactive websites, Facebook, etc.)
  - A privacy and security assessment is necessary

And...

- Every two-three years
  - A periodic security assessment must be conducted every two-three years

Conducting a Risk Assessment

- Is there a HIPAA Security risk assessment?
  - Has it been updated periodically (every two-three years) and updated whenever new electronic technology or use of PHI is introduced?
- Are HIPAA Privacy and Security policies and procedures in writing?
  - Have they been updated since HITECH was enacted (2009)?
- Is the workforce trained on HIPAA and HITECH rules, and the entity's policies and procedures?
  - Is refresher training repeated regularly?
  - Are new employees trained prior to being allowed to handle PHI?
- Have plan participants received a HIPAA Privacy Notice, and reminders at least every three years?
  - Is the Notice on the plan's website?
- Does the entity review whether each service provider is a Business Associate?
  - Does it have their contact information?
  - Are all Business Associate agreements readily available?

Conducting a Risk Assessment

- Is there an inventory of all electronic devices, including computers, mobile devices such as laptops, phones, and tablets, copiers/scanners, etc.?
  - Are there policies and procedures for safeguarding electronic PHI, including policies for all electronic devices and policies for securing information through regular password changes and timely software updates?
- Has encryption been implemented for data in motion and at rest, and if not, is there a reasonable reason not to use encryption documented in a risk assessment?
- Has the entity developed new web or mobile applications?
  - If so, is the app developer a Business Associate and are appropriate security protections in place for the new apps, particularly during transition from one platform to the next?
- Are the entity's Privacy and Security Officers well trained on HIPAA and is there a process for reporting potential breaches and assessing whether they must be reported to HHS and/or the participant?

How to Distribute ERISA Required Disclosures

- ERISA required disclosures must be distributed in a way that is **"reasonably calculated to ensure actual receipt"**
  - Hand delivery
  - Mail
- To furnish the disclosure electronically, the plan must comply with the DOL's electronic safe harbor rules at 29 CFR 2520.104b-1(c)
  - Rules differ depending on whether the participant or beneficiary has access to the employer's electronic information as part of his/her job

DOL Rule for Electronic Distribution

For participants who can effectively access documents at any location where the participant is reasonably expected to perform his/her job duties and for whom accessing the employer's electronic system is an integral part of his/her job duties, electronic disclosure is permissible if:

- Delivery results in actual receipt of information
  - e.g., use return-receipt or notice of undelivered electronic mail features, conduct periodic reviews or surveys to confirm receipt of the transmitted information
- At the time a document is furnished electronically, must provide notice of the significance of the document and of the right to request and obtain a paper version of the document free of charge
- Must protect confidentiality

DOL Rule for Electronic Distribution

For participants *without* work-related computer access (e.g., employees on a leave of absence, retirees, COBRA qualified beneficiaries, etc.), electronic distribution is permissible only if the participant previously consented to electronic disclosures

- Consent must be provided in a manner that reasonably demonstrates the participant's ability to access information in the electronic form that will be used (e.g., provides electronic consent)

DOL Electronic Distribution Rules

Apply to:	Do Not Apply to:
SPDs, SMMs, SMRs, Special Enrollment Notices, WHCRA, EOB Forms, QMCSOs, QDROs, Claims and Appeals Notices	Medicare Part D Creditable Coverage
COBRA	HIPAA Privacy Notice
CHIPRA Notice	Employer/Plan reporting on Forms 1095, 1094
Summary of Benefits and Coverage	
Self-funded non-governmental plan HIPAA opt-out	

Electronic Reporting and Disclosure Obligations

- Employers have moved way beyond whether you can email someone an SPD
- Electronic communications are becoming more sophisticated and using social media
- Electronic reporting and disclosure obligations have not kept up, and are different for each type of disclosure

Thank you!