GBS UNIVERSITY PRESENTS:

HIPAA & THE GROUP HEALTH PLANS- WHAT MUST A BROKER KNOW?

PRESENTED BY

KATHY THOMPSON

GBS Group Benefit Services

AmWINS Group, Inc.

AGENDA

- ✓ History
- ✓ Most Recent Fines and New Penalty Amounts
- ✓ Broker & Group Health Plan Responsibilities
- ✓ Business Associates
- ✓ Security
- ✓ Training

MAKING PHI SECURE AGAIN!

- **Provide information to the broker community to ensure the appropriate processes are in place for protecting their clients' PHI!**
- **There have been many 'breaches' of PHI over the past several years.**
  - ✓ **Fines and Jail time are being implemented**
  - ✓ **All parties have become lax in the protection of PHI during the normal course of the work-day**
  - ✓ **How does this effect the broker/consultant?**
    - **Email – using secured methods**
    - **Paperwork – who sees it, where is it stored/filed**

HISTORY OF IMPLEMENTATION OF PROTECTING PHI

- **HIPAA Privacy Regulations – April 2003**
- **HIPAA EDI Transaction Standards – October 2003**
- **HIPAA Security Regulations – April 2005**
- **HITECH (Health Information Technology for Economic & Clinical Health Act) - Enacted February 2009 but effective February 2010**
  - **✓Changes to implement stricter measures to protect PHI**
  - **✓Changes that now holds all Business Associates accountable – ie: broker/consultant**

Before/After Omnibus Rule

- **Before Omnibus**: BAs/Subcontractors regulated through Business Associate Agreements (BAAs)
- **After Omnibus**: BAs/Subcontractors are now regulated directly under HIPAA:
  - Comply with HIPAA Security Rule
  - Comply with a specific section of the HITECH Breach Notification Rule
  - Comply with all applicable provisions of the Privacy Rule
- **Substantially increased the magnitude of HIPAA enforcement risk and liability**

"I heard the new HIPAA Omnibus Rules are a whole lot tougher on business associates."

PENALTIES EFFECTIVE OCTOBER 11, 2018

Covered entity or business associate did not know and, by exercising reasonable diligence, would not have known that violation occurred:

Each Violation - $114 to $57,051

All such Violations of an identical provision within a calendar year - $1,711,533

Violation due to reasonable cause and not willful neglect:

Each Violation - $1,141 to $57,051

All such Violations of an identical provision within a calendar year - $1,711,533

PENALTIES EFFECTIVE OCTOBER 11, 2018

Violation due to willful neglect, and timely corrected (generally within 30 days after the covered entity or business associate knew or should have known):

Each Violation - $11,410 to $57,051

All such Violations of an identical provision within a calendar year - $1,711,533

Violation due to willful neglect but not timely corrected:

Each Violation - $57,051 to $1,711,533

All such Violations of an identical provision within a calendar year - $1,711,533

JAIL TIME FOR CRIMINAL PENALTIES

- **Tier 1 – Reasonable cause or no knowledge of violation – a maximum of 1 year**
- **Tier 2 – Obtaining PHI under false pretences – a maximum of 5 years**
- **Tier 3 – Obtaining PHI for personal gain or with malicious intent – a maximum of 10 years**

FINES IMPLEMENTED IN 2018

- **Fresenius Medical Care North America $3,500,000 – 5 breach reports of electronic PHI of 5 covered entities – failure to implement policies & procedures**
- **MD Anderson Cancer Center – Univ of TX $4,348,000 – June 2018 – 3 separate data breaches resulting in theft of information**
- **Anthem, Inc. $16,000,000 – the largest U.S. health data breach from a 'cyber attack' last October. During 2014 and 2015 the cyber attackers stole ePHI of almost 79 million individuals**
- **Cottage Health $3,000,000 – in 2017 breaches of unsecured electronic ePHI affecting over 62,500 individuals**

HOW CAN THE BROKER/CONSULTANT HELP THEIR CLIENTS THAT ARE “COVERED ENTITIES” WITH THE REQUIRED GROUP HEALTH PLAN RESPONSIBILITIES?

SHOULD THE BROKER/CONSULTANT ADOPT SOME OF THESE RESPONSIBILITIES?

GROUP HEALTH PLAN RESPONSIBILITIES

- **Privacy Rules**
  - ✓ **The Privacy Regulations control the internal uses and the external disclosures of Protected Health Information (PHI)**
  - ✓ **Covered entities and business associates may not use or disclose an individual's PHI except as permitted or required under the Privacy Regulations.**
  - ✓ **The Regulations (governed by OCR and DHHS) also:**
    - o **Create certain individual's rights – Notice of Privacy Practices**
    - o **Establish administrative requirements – Policies & Procedures**
    - o **Mandate that covered entities enter into contracts with their business associates (BAA – Business Associate Agreement)**

GROUP HEALTH PLAN RESPONSIBILITIES

- **Breach Notification Rules**
  - ✓ **Definition of a Breach**
    - o **Under the HITECH Act, a breach is defined as the "unauthorized" acquisition, access, use or disclosure of Protected health Information which compromises the security or privacy of the PHI"**
      - o **Breaches are treated as discovered**
      - o **Depending on the "size" of the breach, different parties are required to be notified**
      - o **Fines would be assessed based on the "size" and "severity" of the breach**

GROUP HEALTH PLAN RESPONSIBILITIES

- **Business Associate Agreement (BAA)**
  - ✓ **Brokers/Consultants**
  - ✓ **Covered Entities**
  - ✓ **Carriers – language normally in contracts**
  - ✓ **Third Party Administrators (TPA)**
  - ✓ **HITECH Act required changes to the agreement imposing direct compliance requirements to business partners other than covered entities.**

GROUP HEALTH PLAN RESPONSIBILITIES

Business Associate Agreement (BAA) continued

The failure to complete Business Associate Agreements (BAAs) with third party service suppliers can attract financial penalties for HIPAA noncompliance.

Several entities have been fined for not revising BAAs written before September 2014 when all existing contracts were made invalid by the Final Omnibus Rule.

In September 2016, the Care New England Health System was issued a fine for $400,000 for HIPAA noncompliance that included the failure to update a BAA originally completed in March 2005.

GROUP HEALTH PLAN RESPONSIBILITIES

- **Requirements based on activities of the Group Health Plan**
  - ✓ **Fully-insured vs. Self-insured**
    - o **Different guidelines (remember the carrier is a covered entity of the group health plan with fully-insured benefits)**
  - ✓ **Notice of Privacy Practices (carrier usually provides)**
  - ✓ **Business Associate Agreements**
  - ✓ **Authorization and Consent Forms**
  - ✓ **Training**

GROUP HEALTH PLAN RESPONSIBILITIES

- **Requirements based on activities of the Group Health Plan**
  - ✓ **Policies & Procedures for Privacy & Security**
  - ✓ **Risk Assessments**
  - ✓ **Employee Records vs. PHI (HR vs Group Health Plan Sponsor)**
  - ✓ **Right and need to know information**
  - ✓ **Minimum necessary – Limited Employer Access to PHI**
  - ✓ **Firewalls**
  - ✓ **Accounting Disclosures**

GROUP HEALTH PLAN RESPONSIBILITIES

- **Requirements based on activities of the Group Health Plan**
  - ✓ **Administrative Requirements**
  - ✓ **Breach Notifications**
  - ✓ **Complaints**
  - ✓ **Proper Documentation**

GROUP HEALTH PLAN RESPONSIBILITIES

- **Policies and Procedures**
  - ✓ **Covered Entities required to have**
  - ✓ **Self-insured group health plan sponsors required to have**
  - ✓ **Fully-insured large group health plan sponsors required to have**
  - ✓ **Why should P&P be required?**
    - o **To protect PHI for all employees participating in benefits**
    - o **To track complaints, requests for information and breaches**
    - o **DOL/OCR/DHHS audits**

BUSINESS ASSOCIATE AGREEMENTS

- **Who should have them?**
  - **Any employer sponsoring a group health plan – fully insured and self funded**
  - **Brokers/Agencies**
  - **TPAs**
  - **Carriers – including stop loss carriers**
  - **Networks**
  - **PBMs (Pharmacy Benefit Managers)**
  - **Vendors working with covered entities and other Business Associates**

BUSINESS ASSOCIATE AGREEMENTS

- **Compliance Requirements**
  - **Require BA that carry out covered entity's obligations under the Privacy Rule to comply with the same requirements**
  - **Require BA to comply with the Security Rule in handling PHI**
  - **Require BA to ensure that all subcontractors enter into a contract or arrangement to protect the security of the PHI**
  - **Require BA to report security incidents to covered entity as required by Section 164.410 of the breach notification rules**

BA = Business Associate

BUSINESS ASSOCIATE AGREEMENTS

- **Required language in a Business Associate Agreement**
  - **Obligations & Activities of Business Associate**
  - **Permitted Uses and Disclosures by Business Associate**
  - **Provisions for Covered Entity to inform Business Associate of Privacy Practices and Restrictions**
  - **Permissible Requests by Covered Entity**
  - **Term & Termination**
  - **Definitions (of terms used throughout the agreement)**

REVIEW OF OMNIBUS HIPAA/HITECH RULE

- **Overview of Significant Rules**
  - **Business Associate Obligations**
  - **Breach Notification Standards**
  - **Marketing of PHI**
  - **Notice of Privacy Practices**
  - **OCR Enforcement Mechanisms**

REVIEW OF OMNIBUS HIPAA/HITECH RULE

- **Business Associate Obligations**
  - **HITECH – Health Information Technology for Economic and Clinical Health Act – concentrated on Breach Regulations**
  - **Extends HIPAA obligations directly to Business Associates**
  - **Requires Business Associates to develop and implement policies and procedures to meet HIPAA Security Standards**
  - **Requires Business Associates to report any “breach” of unsecured PHI**

REVIEW OF OMNIBUS HIPAA/HITECH RULE

- **Business Associate Obligations**
  - **Imposes more obligations and extends liability to Business Associates**
  - **Business Associates can now be found liable for errors, breach of PHI and misuse of PHI under the guidelines**
  - **Business Associate Agreements was required to be HITECH compliant by September 22, 2014**

REVIEW OF OMNIBUS HIPAA/HITECH RULE

- **Breach Notification Standards**
  - **Administrative requirements remain the same**
  - **“Breach” is redefined**
    - **Unauthorized acquisition, access, use or disclosure of PHI that comprises the security or privacy of such information**
    - **Did the unauthorized action “compromise” the individual’s privacy/security where there was significant risk of harm to an individual?**
    - **Impact of the unauthorized act**

REVIEW OF OMNIBUS HIPAA/HITECH RULE

- **OCR Enforcement Mechanisms**
  - **OCR (Office of Civil Rights) increased its enforcement authority after realizing that voluntary compliance had not worked**
  - **OCR will investigate or initiate compliance reviews if preliminary review indicates possible violation due to willful neglect**
  - **OCR may proceed immediately to imposing penalties and may elect not to resolve complaint by informal means (before they would attempt to resolve)**

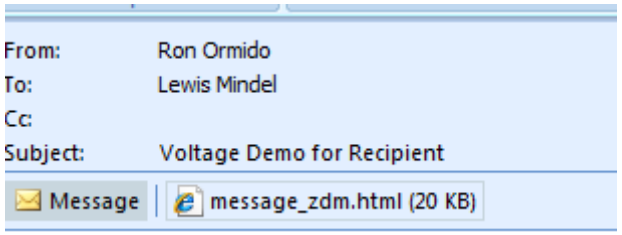
EMAIL SECURITY

EMAIL SECURITY - VOLTAGE

The Voltage SecureMail Usage Policy will provide guidelines in standardizing the proper usage for sending and receiving encrypted emails. These guidelines will not only represent the requirements and restrictions for handling of Protected Health Information (PHI) regulated by the privacy rule of the Health Insurance Portability and Accountability Act (HIPAA). It will provide a standard for integrating these procedures in properly transmitting electronic information for both internal and external recipients.

VOLTAGE REGISTRATION

How to receive Secure Emails



You will receive this email below that contains an attachment similar to the one next to it below. The attachment may be called “message_zdm.html”, simply double click on it.

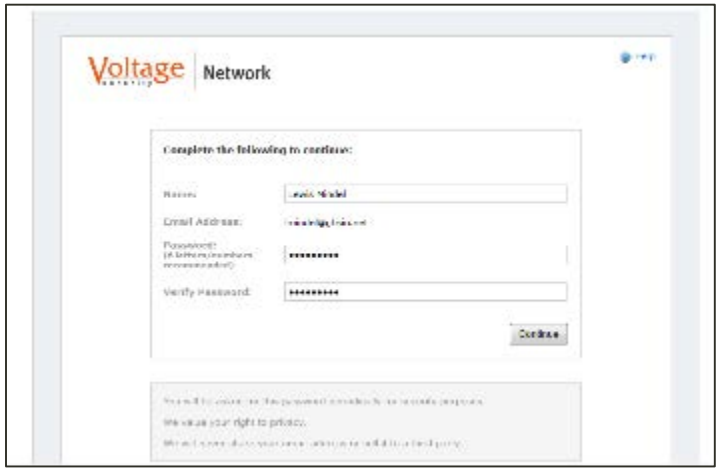
Once you click on the attachment, you will see the following screen, click on “Read Message”.

After you click on Read Message, this screen will appear to verify your Email Address, select it and select “View Message”.

VOLTAGE REGISTRATION

How to receive Secure Emails

Now you are going to be asked for a password which you will use for the secure emails in the future. Please do not keep it view of others or tell anyone your password. Select Continue.



After Continue, you should receive a temporary email, please check it and continue.

After you click on Read Message, this screen will appear to verify your Email Address, select it and select “View Message”.

TRAINING

- **Who should be trained?**
  - ✓ **Employer/Group Health Plan**
    - **Management**
    - **Employees or Staff having access to PHI**
      - **Enrollment or claims**
  - ✓ **Brokers/Agencies**
    - **All staff members working with client information**

TRAINING FREQUENCY

- **At least once a year**
- **Each new employee that would be working with PHI**
- **More often if misuse of PHI**
- **Document the training, who attended and get signatures**

TRAINING SESSION MATERIALS

- **Based on the employees' responsibilities**
- **Tailored to department working with PHI**
- **Reasonable Safeguards should be discussed and processes put in place**
- **Review of penalties and fines**
- **Sharing Policies & Procedures as allowed**


Knock Knock!
-Who's there?
HIPAA!
-HIPAA who?
I can't tell you that.
someecards
user card