PRIVACY AND SECURITY ISSUES FOR AGENTS, BROKERS & CONSULTANTS

Celebrating 25 years!

Jekyll Island Convention Center
August 20-21, 2015

Complex world

- Protecting information that you have about individuals is increasingly becoming a major issue
  - Identity Theft
  - HIPAA Privacy & Security
  - Other FTC rules

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

HIPAA Privacy & Security Rules

- Our focus, but ultimately most worried about:
  - Protecting against the misuse of information
  - Creating an environment where privacy and security is seen as being important

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Introduction to HIPAA

- Why do we need it?
  - Electronic transactions simplify the claims, enrollment, eligibility, and inquiry processes
  - Reduce (manage) the high cost of administering healthcare claims
  - Increase trust with privacy and security measures
  - Good business and confidentiality practices

What Is HIPAA?

- HIPAA is the Health Insurance Portability and Accountability Act of 1996, that regulates:
  - portability and continuity of health insurance
  - health information privacy
  - administration of health insurance

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Why is this suddenly a big deal?

- The Final Implementation deadline of September 23, 2014 for all Covered Entities, Business Associates and Subcontractors
  - Partial implementation date was 2013

- Significant breaches in the health insurance sector over the past twelve months

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Why is this suddenly a big deal?

- Enforcement Actions have ramped up over the last three years
  - Over 32M records improperly disclosed and millions in fines paid
  - Two agencies have suffered breaches this year with pending fines for lost computers
  - HHS has announced a new round of audits to occur in 2015 to focus further on compliance

Update on Breaches by Agencies

NFP - Maschino, Hudelson & Associates (Oklahoma): Password protected (not encrypted) laptop with PHI stolen from car containing 3,814 names (May 2014)

- Firm has notified each affected individual in writing, explained the situation and advised them on how to take advantage of the free credit monitoring and put a fraud alert on their files

Update on Breaches by BAs

DeLoach & Williamson (South Carolina): Auditor for SC State Health Insurance Pool had laptop with PHI stolen from car containing SSN, full name, dates of service of 3,438 individuals (December 2013)

- Pool notified affected individuals in writing

Update on Breaches by Agencies

Keystone Insurers Group (Indiana) provided greater than "minimally necessary" information about a client's 1,008 employees and dependents with potential clinic services providers (June 2012, discovered March 2014)

- Town provided information and published legal notice on the breach in the local newspaper

Update on Breaches

- Anthem: 80M
  - Subject to “sophisticated cyber attack” that impacted not only their customers but also those of numerous other Blue Plans
  - Recently discovered that this hacking had been going on for months, the question has now been raised as to why it took the company such a long time to uncover the hacking

Update on Breaches

- Premera (Blue Plans in WA, AK): 11M+
  - Information hacked goes back to 2002, includes members' names, dates of birth, Social Security numbers, mailing addresses, e-mail addresses, telephone numbers, member identification numbers, bank account information and claims information, including clinical information
  - “Individuals who do business with Premera, as well as Premera employees, also are likely to have been affected”

Update on Breaches

- Blue Cross Blue Shield of Michigan: 4/2015
  - Employees printed screen shots of more than 5,500 individuals' information and used it to access credit cards and gift cards; included $742,000 worth of merchandise from Sam's Club

Update on Breaches

- CareFirst (Blue Cross Blue Shield of Maryland): 5/2015
  - Sophisticated cyber attack of 1.1M member records

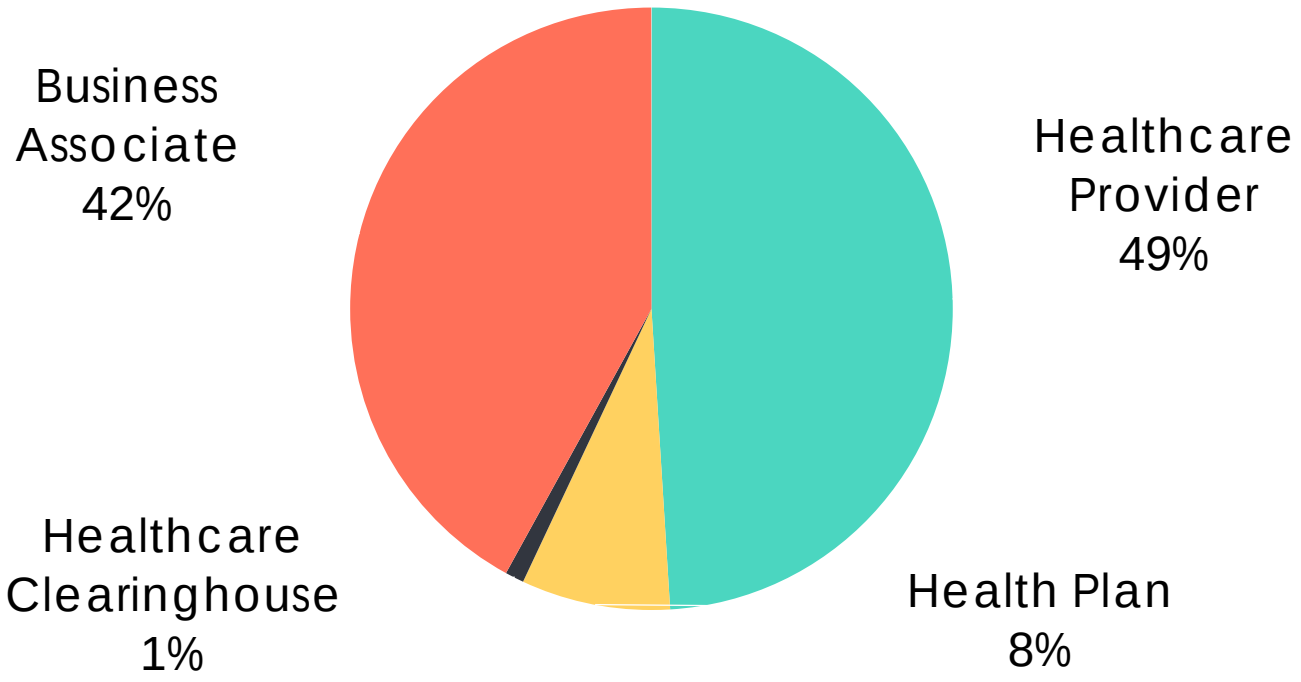
2014 health care data breaches

- 336 breaches, half impacting 500+ individuals
- Types:
  - 20% involved non-digital information
  - 12 stolen laptops or portable devices
  - Over 50% involved “insider actions” with nearly 500,000 records stolen or misused

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Individuals Affected By Breaches



Source: "Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance." 1 Jan. 2013. Web. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/compliancereport2011-2012.pdf

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

If I already have HIPAA policies and procedures in place am I okay?

No!

There are significant changes and you need to adopt new Policies and Procedures.

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

HIPAA PRIVACY

HIPAA Privacy Regulations

- General Rule:
  - Covered Entities, their Business Associates and their Subcontractors may not use or disclose an individual's protected health information without the authorization of the individual unless specifically required or allowed by the privacy regulation.
- Protects PHI in ANY form (oral, written, electronic)
- **Remember– Business Associates and Subcontractors now must meet all these regulations!**

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Protected Health Information

- Individually identifiable health information is that which can be linked to a particular person
- Specifically, this information can relate to:
  - The individual's past, present or future physical or mental health or condition,
  - The provision of health care to the individual, or,
  - The past, present, or future payment for the provision of health care to the individual.
- Common identifiers combined with health information include names, social security numbers, addresses, credit card number and birth dates

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Key HIPAA Terms

- **Covered Entity:** Healthcare provider, clearinghouse, health plans (insurance companies and employers)
- **Business Associate:** Person, group or organization that handles PHI on behalf of a Covered Entity (health insurance agents and brokers)
- **Subcontractor:** Person, group or organization that handles PHI on behalf of a Business Associate

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

HIPAA Only Applies to

Medical/Health

Dental

Vision

Long Term Care

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

HIPAA Does Not Apply to:

- Short-term and long-term disability
- AD&D (Accidental Death and Dismemberment)
- Life insurance
- Worker's Compensation
- Auto medical insurance
- Fitness-for-duty exams (DOT or OSHA exams)
- Drug testing
- Work-life benefits (on-site clinics; fitness center)
- Family Medical Leave Act (FMLA)
- Americans with Disabilities Act (ADA)

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Employers

- An employer is not a covered entity, but must sponsor an group health, dental and/or vision plan.
  - An ERISA group health plan is an employee welfare benefit plan that provides medical care to employees and/or their dependents/ spouse directly or through insurance, reimbursement or otherwise.
  - The group health plan is the covered entity, but the employer may need to comply with the HIPAA privacy rules as the plan sponsor or administrator.

- An employer may be a covered entity if it operates in the capacity of a health care provider (e.g., an employer may be a covered entity if it has an on-site health clinic for employees).

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Roles

- Think of the employer has having two different roles:

Employer

Plan Sponsor

Employer Role

- Employers do not need to comply with the HIPAA privacy rule when acting in the employer role—for example:
  - Requesting a doctor's note from an employee upon return from an absence consistent with policies or practices.
  - Obtaining medical information to administer leave programs such as FMLA, requests for ADA accommodation, workers' compensation, wellness programs and health benefits
  - Employee names and injury information on OSHA logs.
  - Information from medical providers related to drug tests and fitness-for-duty exams.

Employer Role

- More examples of employer role:
  - Employer corresponds with workers' compensation carriers and health care providers in the administration of a workers' compensation claim.
  - Employer shares summarized health information for purposes of amending plan benefits as long as all identifying information such as names, birth dates and Social Security numbers is removed.
  - Employer discloses information related to the birth of a child or health condition of an employee if the information comes from an employee and not from a group health plan.

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Plan Sponsor Role

- When the covered entity is the group health plan, an employer is obligated to comply with the HIPAA privacy rule in its role as the plan sponsor.
  - Participate in the administration of a group health plan.
  - Are active in the decision-making process of a group health plan.
  - Participate in the operation or control of the provisions of a group health plan.

Plan Sponsor Responsibilities

- Employers acting in a plan sponsor role need to:
  - Have written PHI procedures.
  - Limit uses and disclosures of PHI to the minimum necessary to accomplish the intended purpose.
  - Designate a privacy officer.
  - Require business associates to ensure confidentiality of PHI through written contracts or agreements.
  - Establish administrative, technical and physical safeguards to protect the privacy of PHI.

Plan Sponsor Responsibilities

- Employers acting in a plan sponsor role need to:
  - Train employees on the HIPAA privacy rule.
  - Provide a process for filing complaints.
  - Ensure that PHI is not used for making employment or benefits decisions, marketing or fundraising.

Plan Sponsor Responsibilities

- Business Associates (BA)
  - Person, group or organization that handles PHI on behalf of a Covered entity
  - Is not an employee and does not fall under direct supervision of the Covered Entity
  - Must ensure that they will protect PHI
  - Must ensure that any of their subcontractors will protect PHI
- Examples of BA
  - TPA that assists with claims processing
  - Cloud storage vendor
  - IT vendor
  - Shredding company

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Plan Sponsor Responsibilities

- Subcontractors of Business Associates
  - Person, group or organizations that handles PHI on behalf of a Business Associate
  - Is not an employee and does not fall under direct supervision of Business Associate
  - Must ensure that they will protect PHI
- Examples*
  - Cloud storage vendor
  - IT vendor
  - Shredding company

  - * Note: The same company can be a BA of a Covered Entity and a subcontractor of a BA

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

HIPAA SECURITY

Purpose of the Security Rule

- Protect electronic patient health information (PHI) in three ways:
  - Confidentiality – PHI concealed from people who do not have the right to see the information
  - Integrity – information has not been improperly changed or deleted
  - Availability – healthcare provider can access the information when it is needed
- As originally adopted, HIPAA Security Rule only applied to Covered Entities. Now applies to both Covered Entities and Bas.

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Why a Security Rule?

- Protecting PHI becomes more important as healthcare providers transition to Electronic Health Records
- Increasingly important with increased use of technology for data transmission
  - E-mails (transmission)
  - Electronic enrollments
  - Electronic storage of PHI

Three Security Rule Standards

Administrative Safeguards

Physical Safeguards

Technical Safeguards

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Description of the Security Rule

- Requires Covered Entities, Business Associates and Business Associate Subcontractors to protect electronic patient health information (ePHI) in three ways:
- Confidentiality
  - ePHI concealed from people who do not have the right to see the information
- Integrity
  - Information not improperly changed or deleted
- Availability
  - Information can be accessed whenever it is needed

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Risk Assessment

- Utilize a Risk Assessment tool
- Be thorough
- Conduct annually

What to Do to Comply?

- Appoint an Information Security Officer
- Form a team that includes technical people (this can be an outside contract who signs a Business Associate Agreement which means they have implemented HIPAA in their business)
- Create a set of Security Policies and Procedures
- Train your staff on HIPAA security and Policies and Procedures

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Protect your employees & business

- Follow the policies about what you put in emails and when you delete them
- Encrypt documents for storage and transmission (such as email) as directed
- Put a password protected time-out on all portable devices since they are frequently lost or stolen
- Require all personal computers to have encryption of all content on their hard drives or storage devices
- Report the loss of any equipment which might contain electronic Protected Health Information

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Specific Staff Expectations

- Manage passwords
  - Have staff members choose and remember
  - Change passwords regularly
  - Notify security officer if concerned that password is being improperly used by someone else
- Identify and keep out malicious software
- Use workstations properly
- Know sanction policies
- Learn and follow policies and procedures

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

How to Reduce Threats to Network

- Control access to your computers:
  - Limit use of external devices that might introduce viruses into the system: smartphones, mp3 players, tablet computing device, USB drives
  - Restrict family members or friends using the computers in off-site locations that could introduce viruses and expose to inadvertent ePHI disclosure
  - Implement strict controls on web surfing for personal enjoyment or downloading free programs or music from the Internet to office machines

Risk Assessment

- Conduct a risk assessment to determine areas where security concerns might exist
- Adopt policies and procedures that addresses potential risks
  - Who has access to network and data
  - What should be encrypted and when
  - Emphasize that every employee, especially management, is responsible for knowing and carrying out the relevant policies and procedures that affect the business

Train Everyone

- Need to know the law
- Need to know your specific Policies and Procedures for security and privacy
- Training needs to happen at least yearly
  - Refreshers during the year keep HIPAA on everyone's mind
  - Leave yourself exposed if there is no training

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

BREACH

What is a Breach?

An individual's protected health information that has been, or is reasonably believed by the Covered Entity or Business Associate to have been accessed, used, acquired or disclosed to an unauthorized person.

- Exceptions:
  - Unintentional access by employees or individuals acting under authority of covered entity or business associate if information is not used or disclosed by recipient or anyone else.
  - Inadvertent disclosure from one covered entity or business associate employee authorized to access PHI to a co-employee authorized to access PHI
  - Unauthorized access by an unauthorized person who cannot reasonably be able to retain the information disclosed.

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Breach

- These rules apply to Protected Health Information (PHI) in any format
  - ePHI (electronic PHI)
  - Paper
  - Tapes/CDs
- There is no breach if the PHI is kept in an "secured" format
  - If improperly acquired data was secured (encrypted or destroyed), then no breach notification is required

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

When There is a Breach

Any impermissible use or disclosure of PHI is presumed to be a breach, unless…

- CE/BA must demonstrate that there is a low probability that the PHI has been compromised
- Evaluated based on four factors
  - Nature and extent of the PHI involved
  - Who the unauthorized person who accessed or used the PHI or to whom the disclosure of PHI was made.
  - Whether the PHI was actually viewed or acquired
  - Extent to which the risk to the PHI has been mitigated

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

When There is a Breach

Notify without unreasonable delay and at least within 60 day timeframe

- 60 days begins to run from the date the covered entity or business associate or any employee, officer or other agent of the covered entity or business associate knew or reasonably should have known about the breach

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

How to Notify Clients of a Breach

- Send a written notice to the individual at the last known address by first-class or electronic mail.
- Post a conspicuous message on your Web site's home page about the breach
- Notify major print or broadcast media when:
  - insufficient or out-of-date contact information prevents direct contact of affected individual or
  - if a breach affects or is reasonably believed to affect more than 500 residents
- Call individuals whose unsecured health information was breached when there is an imminent threat of misuse.
- Notify HHS immediately for breaches involving more than 500 individuals and annually for all other breaches.

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

PENALTIES

Penalties

There are 4 categories for penalties

- Did Not Know
- Reasonable Cause
- Willful Neglect–Corrected
- Willful Neglect–Not Corrected

Penalties–Did Not Know

Fines for Did Not Know

- This is when you did not know or would not have known through exercise of reasonable discretion that the disclosure or breach was a violation of HIPAA Rules
  - The fines for this range from $100-$50,000 per violation for a maximum of 1.5 Million for identical violations in a calendar year
  - These fines may be reduced if you fix the issue within 30 days

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Penalties–Reasonable Cause

This is when you should have known what was going on, but you had a violation.

- Fines for this range from $1,000 to $50,000 per violation with a maximum of 1.5 million for such violations of an identical provision in a calendar year.
- These fines may be reduced if you fix the issue within 30 days

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Penalties–Willful Neglect Corrected

This is when you ignored the law, and you got caught, but you corrected the issue within 30 days.

- The Penalties for this range from $10,000 to $50,000 per violation with a maximum of 1.5 Million for all such violations of an identical provision in a calendar year

Penalties–Willful Neglect Not Corrected

This is when you ignored the law, you were caught, and you decided not to correct the issue.

- Penalties for this are $50,000 per violation with a cap of 1.5 Million for all such violations of an identical provision in a calendar year

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Criminal Penalties

- Criminal provisions apply to any individual, regardless of whether they are a covered entity including Business Associates, Subcontractors and their employees
- What is criminal?
  - Knowingly obtaining or disclosing PHI: Fine of up to $50,000 plus imprisonment up to one year
  - Offenses committed under false pretenses: Fine up to $100,000 plus up to five years in prison.
  - Offenses committed with the intent to sell, transfer, or use for commercial advantage, personal gain or malicious harm: Fines of $250,000, and imprisonment for up to ten years.

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

NOW WHAT?

The Most Obvious Mistakes Agencies Make

- Not completing both sets of Policies and Procedures
  - You must have Privacy and Security Policies and Procedures
- Putting a set of policies in a notebook and not competing or updating
- Not training staff on HIPAA and agency's P&P

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

How Can An Agency be Compliant with these HIPAA Rules?

- **TRAINING:** NAHU is now offering comprehensive online training for you and your staff
  - Satisfies the annual training requirement for agents as Business Associates
  - Also includes training on Gramm-Leach-Bliley (State Insurance Confidentiality laws) and PII (privacy of Marketplace information)

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

HIPAA Privacy/Security Certification

- Available through our Online Learning Institute - http://nahu.inreachce.com/
  - HIPAA Compliance Training 2.0
  - Cost:
    - $165.00 for NAHU members
    - $250 for non-members

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

QUESTIONS

RISK ASSESSMENT

What is a Meaningful Risk Assessment?

A meaningful Risk Assessment is a thorough audit of your practice's processes, including:

Administrative

Physical

Technical

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Why Do You Need to Conduct a Risk Assessment?

- Required by the HIPAA Law[1]
  - This is the first item for which an auditor will ask
  - This gives you an outline to develop your Privacy and Security Policies and Procedures
- Shows you where you may have security holes in your agency
- First step for protecting your business and clients!

1. (45 C.F.R. § 164.308(a)(1).) Risk analysis is one of four required implementation specifications that provide instructions to implement the Security Management Process standard. Section 164.308(a)(1)(ii)(A)

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Administrative Safeguards

- Privacy and Security Compliance Officers
- List of all workforce members, roles, and corresponding access
- A written disciplinary policy (sanction policy) in place for HIPAA violations
- HIPAA training program
- Business/Subcontractor Associate Agreements
- A plan for handling Breaches

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Physical Safeguards

- How do you secure your office(s)?
  - Locks, key cards, alarms, etc.
- Where and how are personnel records stored and secured?
- Do you have an inventory of your electronic assets?
- How do you dispose of paper records?
- What do you do with old media?
- Who has access to your office space?

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Technical Safeguards

- What is your encryption policy for
  - Computers
  - Emails
  - Electronic Files
- Can you audit who has been accessing records?
- Does each employee have their own unique password?
- Do you have
  - Data Backup Plan
  - Disaster Recovery Plan
  - Emergency Mode of Operation Plan

How Do You Complete a Risk Assessment?

- Do-It-Yourself package from Total HIPAA
  - 10-20 hours to complete
- Hire an outside vendor
  - Number of vendors who will conduct Turn-Key Assessment of agency
  - Look for someone who has experience working with health insurance agencies

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

How Often Should I Perform a Risk Assessment?

- Establish initial assessment
- Major changes in software or hardware
- No changes – revisit Assessment every 2-3 years
- When you've had a Breach

Who is Helping You With Security?

- Internal resource
  - First step - complete Privacy and Security training
- Outside vendor
  - Look for an IT vendor, not a teenager or friend
  - They must be HIPAA compliant
  - Review their policies and procedures
  - They must sign a subcontractor business associate agreement

The materials referenced here are subject to change, so frequent review of the source material is suggested.

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

What We Are Going to Cover

- Firewalls
- Virus Protection
- Mobile Devices
- Remote Access
- Voice Mail
- Portable Storage Devices
- Faxes
- Encrypting Email
- Data Encryption
- Password Protection
- Wi-Fi
- Website Security
- Backup
- Cloud Storage

Faxes

- Faxes are not a secure way to transmit information
  - Always use a cover sheet
  - Secure fax machine
  - Notify parties before sending faxes
  - Send test fax before sending actual document
  - If possible send information via more secure method
  - Make sure fax machine isn't saving any copies
- If you use online fax program, a Business Associate Agreement is required
  - Make sure they have a valid SSL license

Faxes with PHI sent to the wrong parties are considered a Breach and must be recorded and reported!

Email Encryption

- All PHI must be encrypted in transit, rest, and storage
- Review compliance plan
- 128-bit encryption or better
- Review for ease of use
- Business Associate Agreement is required with provider
- If you use a third party email provider, you must have a Subcontractor Business Associate Agreement

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Hard Drive Encryption (Free)

- For PC's use BitLocker
  - Windows 7 Enterprise and Ultimate
  - Windows 8.1
- For earlier PC Operating Systems
  - DiskCryptor
- Mac OS
  - FileVault2

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Password Protection

- First line of defense
- Make sure all devices have difficult passwords
  - 8+ characters with numbers, upper and lower case letters, and special symbols
- Require password changes frequently as described in your Policies and Procedures
- Make sure passwords are memorized or use password management software
- Password protect desktop, laptop, tablets and smart phones

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Wi-Fi

- Encrypt network using WPA2 with Advanced Encryption Standard (AES)
- If you allow guests to access Wi-Fi use a guest portal
- Do not use factory supplied password for router
- Consider limiting router power so network doesn't reach beyond your office

Website Security

- SSL/TLS License on site
- Force HTTPS on all pages to protect information
- Do not collect PHI through your website without proper protections
- Subcontractor BA Agreement with Web Host is required but not with transmission vendor (TWC, ATT, Verizon)

Backups

- Backups protect you from hard drive failures
- Backups need to be kept in a different secure location
  - Bank safety deposit box
  - Protect against theft, fire or flood
- Train multiple parties on how to perform a recovery of your computer systems
- Cloud – growing in popularity

Cloud Storage

- Review Cloud Storage Compliance Plan
- What level encryption do they use?
- Do they have access controls on data
- Audit trails?
- How do they get you back ups in the event of a failure?

Virus Protection - Things to Look For

- Email Scanning
- Download Protection
- Spyware and Malware Scans
- Speed
- Compatibility
- Privacy Policy
- Real-Time Information
- Heuristic Analysis
- Automatic Updates

Mobile Devices

- Wireless calls are secure
- Critical that the devices are encrypted and password protected
- All SD cards need to be encrypted
- Update operating systems
- Install virus protection
- Text messaging is not secure unless you use a secure text messaging service (BAA Required)
- Enable tracking for all devices

If staff is supplying their own electronic devices implement a BYOD policy

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Remote Access

- Ability to access files and systems from outside the office
  - Virtual Private Network
- Cloud based solutions dominate
  - HIPAA Compliant
    - ShareFile
    - Google Drive
    - Microsoft OneDrive
    - Box
  - Not HIPAA Compliant
    - DropBox and iCloud

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Voice Mail

- If voice mail is kept on computer as a part of your phone system you must physically secure the computer and encrypt the messages
- If a third party hosts your voice mail
  - Disable transcription service (Unless sent encrypted)
  - Disable emailing voice messages (Unless sent encrypted)

They must sign a Subcontractor Business Associate Agreement!

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Portable Storage Devices

- Establish a policy on use of
  - USB Drives
  - Tablets
  - Portable drives

- Require that the data stored on these be password protected and encrypted

Staff Compliance is Key

- Employees compliance will determine the success of controlling the Protected Health Information your agency manages
- Employees should be trained to follow your compliance plan, and retrained annually

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

BYOD

These devices...

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

The good, the bad, and the ugly

THE GOOD

- Good for productivity
- Saves you money

THE BAD

- You have limited control of the devices
- Distracting for employee

THE UGLY

- Employees can bring malware to work

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Why Should I have a policy in Place?

- Protects the agency
- Protects your clients
- Shows employees how important Privacy and Security are to you

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Acceptable use

- What apps are allowed or forbidden?
- Are certain websites restricted during business hours?
- Can employees access agency-owned resources?
  - Email
  - Contacts
  - Documents
  - Records

Employees shouldn’t share devices that can access the practice network with family members or friends.

Reimbursement

What **will** you reimburse?

What **won't** you reimburse?

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

What devices are allowed on your network

- First, create a detailed list of devices and the operating systems allowed.

- Next, you should determine:
  - Who will support connectivity issues?
  - Who will configure devices for network access?
  - How are you encrypting devices?

Password Changes

- Establish a set schedule (e.g., every 90 days)
- Clearly state this in your Policies and Procedures
- How should you enforce this?

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

Virus protection required on devices

- iPhone and iPad
- Android Devices
- Windows Devices
- Linux Based Systems

Tracking and remotely wiping devices

- Laptop PC's
- Android devices
- Windows Phones
- Apple Devices

Remote access

- What type of remote access is acceptable?
- How should employees access secure info?
- VPN
- Cloud File Sharing

Portable storage devices

- Do you allow these on your network?
  - Flash Drives
  - Removable Hard Drives
  - CD's and DVD's

Platform for mobile device management (MDM)

Supports Apple iOS, Android and Windows
Alphabetical order

AirWatch	Fiberlin MaaS360
AmTel MDM	IBM
Dialogs Smartman Device Mgt	MobileIron
Exitor DME	Symantec
Fancy Fon	Zenprise

http://www.zdnet.com/article/10-byod-mobile-device-management-suites-you-need-to-know/

GAHU Georgia Associations of Health Underwriters

FISHER & PHILLIPS LLP ATTORNEYS AT LAW Solutions at Work®

QUESTIONS