COMPLIANCE AND RISK MANAGEMENT: A LESSON FROM THE U.S. ATTORNEY’S OFFICE
Let's talk about a proactive vs. reactive approach to your business and organization.

Which would you prefer?

Proactive: Helps protect you from drowning.

Reactive: Thrown to you after you're already drowning.
I GET IT, SO WHAT DO I DO ABOUT IT?: SWORD AND SHIELD
A COMPREHENSIVE BEHAVIORAL HEALTH RISK MANAGEMENT PROGRAM
WHAT IS HIPAA?

The Health Insurance Portability and Accountability Act ("HIPAA") is a federal law that protects the privacy of protected health information ("PHI").

HIPAA is comprised of:

- Privacy Rule – Establishes national standards for the protection of health information, its use and disclosure, and individual rights and access to PHI.
- Security Rule – Establishes a national set of security standards for protecting certain health information that is held or transferred in electronic form.
WHAT IS PHI?

**PHI** is defined as “**individually identifiable health information**” that is:

- Transmitted by electronic media;
- Maintained in electronic media; or
- Transmitted or maintained in any other form or medium.

“**Individually identifiable health information**” is information relating to:

- An individual’s past, present or future physical or mental health;
- The provision of health care to the individual; or
- The past, present, or future payment for the provision of health care to an individual that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.
TO WHOM DOES HIPAA APPLY?

**Covered Entities (CE):**
- A health care provider that conducts certain transactions in electronic form;
- A healthcare clearinghouse; or
- A health plan
  - Examples: Physicians, hospitals, health care facilities

**Business Associates (BA):** Any individual or entity that receives PHI from a covered entity to assist the covered entity with its health care functions, including legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services
  - Examples: health care accounting firms, billing companies, BHCOE, etc.
AUTISM PROVIDERS AS COVERED ENTITIES

- All staff members that have access to a computer or electronic device which stores or transmits PHI are subject to HIPAA including:
  - Administrative staff with access to files containing PHI
  - Information Technology staff
AUTISM PROVIDERS’ SUBCONTRACTORS AS BUSINESS ASSOCIATES

- All Covered Entities that utilize third party vendors that will maintain, transmit, access or store PHI on their behalf must execute business associate agreements with those parties.
  - This includes copier services or document storage vendors.

- As a Covered Entity to a Business Associate an Autism Provider must ensure that its subcontractors are also compliant with HIPAA regulations.
ACCESS TO INFORMATION

- Never assume that you have a right to access PHI just because you work for an organization that handles PHI.

- An employee may access information based on his/her role and job responsibilities.

- Minimum Necessary:
  Staff members must only access the minimum amount of PHI necessary in order to perform his/her job function. Staff members may only access PHI if they have a valid reason for doing so (e.g. for work purposes).
Safeguards can be divided into three categories: administrative, technical and physical. The organization is required to safeguard all PHI in its possession.

<table>
<thead>
<tr>
<th>ADMINISTRATIVE</th>
<th>PHYSICAL</th>
<th>TECHNICAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Policies and Procedures</td>
<td>• Workstation security</td>
<td>• Password protection</td>
</tr>
<tr>
<td>• Staff training and education</td>
<td>• Locked File Cabinets</td>
<td>• Automatic logoff</td>
</tr>
<tr>
<td>• Defined employee access to ePHI</td>
<td>• Visitor sign-in and limited access</td>
<td>• Encryption and decryption mechanism</td>
</tr>
<tr>
<td>• Contingency plan in case of emergencies</td>
<td>• Chart locator records</td>
<td>• Identity authentication</td>
</tr>
<tr>
<td>• Assigned Security Officer</td>
<td>• Shred bins</td>
<td>• Backup data</td>
</tr>
<tr>
<td>• Business Associate Agreements</td>
<td></td>
<td>• Protocols regarding the introduction and removal of hardware and software from the Covered Entity network</td>
</tr>
</tbody>
</table>
BEST PRACTICES

- Passwords on Electronic Devices
- Lock Your Computer Screen
- Workstation Security
- Portable Device Security
- Data Management
- Anti-Virus Software
- Computer Security
- E-mail Security
PASSWORD BEST PRACTICES

- Use cryptic passwords that can’t be easily guessed.
- Protect your passwords – don’t write them down or share them!
- Use combinations of capitalization, numbers, and punctuation.
- Change your password on a regular basis.
LOCK YOUR COMPUTER SCREEN

- Use a password to start up your computer.
- Use a log off system which automatically logs off your computer after a period of inactivity.
WORKSTATION SECURITY

- Physically secure your area and PHI when it is unattended.
- Secure your files and portable equipment.
Fax Machines

Physical Fax Machine

- Fax machines must be located away from public and common areas, and accessible only by authorized persons.
- Reasonable care must be taken to assure that information reached authorized sources.
  - All fax documentation must be accompanied by a cover sheet.
  - When faxing PHI, double check that the fax number is correct.
TELEPHONES AND CELL PHONES

Physical

Cell Phone

- Text messaging is NOT a secure way of communicating PHI.
- Avoid sharing PHI over text.
  De-identify information as much as possible if communicating via text.

Telephone

- If possible, avoid sharing PHI over the telephone and share only the minimum necessary.
- Avoid leaving confidential information on voicemail messages.
  - Be aware of who has access to voicemails and answering machines.
- When using speakerphone, make reasonable efforts to minimize unauthorized access.
  - Close the door, lower the volume, consider using a handset.
LAPTOPS AND OTHER PORTABLE DEVICES

- Do not keep unencrypted confidential data on portable devices.

- **YOU MUST:**
  - Encrypt the data;
  - Password Protect the device; and
  - Use only a device that may be remotely wiped.

- Best Practice – Use a Device With a Non-Removable Hard Drive.
ANTI-VIRUS SOFTWARE

- Make sure your computer has up-to-date anti-virus software and all necessary security patches.
- Contact your system manager for any questions regarding computer security
Never install unknown or unsolicited programs on your computer to prevent:
- Viruses:
- Hacking; and
- Unauthorized disclosures.
EMAIL

- Practice safe e-mailing:
  - Don’t open, forward, or reply to suspicious e-mails.
  - Don’t open suspicious e-mail attachments or click on unknown website addresses.
  - Delete spam e-mails.
  - Don’t provide PHI to a third party without encryption.
  - Password-protect or encrypt documents containing PHI.
Physical Disposal and Destruction of PHI

- Records that have satisfied their legal, fiscal, administrative, and archival requirements may be properly destroyed.
  - PHI is no longer protected by HIPAA laws if the subject of the PHI has been deceased for over 50 years.
- Proper destruction of PHI ensures the confidentiality of the records and renders the information as no longer recognizable.
- Approved methods of record destruction include: shredding, burning, pulping, pulverizing, and magnetizing.
  - Paper PHI meant for shredding must be kept in locked containers.
  - Shredding is the best method to dispose of paper PHI.
E-PHI SECURITY ASSESSMENT

Technical

ePHI Security Assessment

HIPAA requires organizations to conduct an ePHI Security Assessment on an annual basis.

The Assessment list 28 security measures that are either required under HIPAA or addressable, depending on the technology available to the organization.

The organization must assess its implementation and effectiveness of each requires security measures and any other that they have implemented, and provide an explanation for any addressable measures that are not being implemented.
HIPAA TRAINING REQUIREMENTS

Required Education of the Workforce – The organization is required to provide training to all staff and volunteers on HIPAA rules and regulations.

- All staff members must be trained upon hire and then annually thereafter.
- Documentation of training should be maintained by the HIPAA Privacy Officer.
BREACHES, REPORTING, & PENALTIES

A Breach is -

1. Unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the organization.

2. Improper usage or disclosure of PHI by a vendor or staff member.

3. The impermissible use or disclosure of PHI (i.e. a violation of the HIPAA Privacy Rule) is presumed to be a breach unless the Covered Entity or Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised.
The organization must conduct a Risk Assessment for every potential breach. The Risk Assessment will measure the following things:

- The nature and extent of the PHI involved;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.
BREACHES, REPORTING, & PENALTIES

Breach Exclusions

**Internal** – Unintentional use of PHI by a workforce member or person acting under the authority of a Covered Entity or a Business Associate. *(Ex)* A nurse accidently accesses the chart for Mr. Jones instead of Mrs. Jones.

**External** – Inadvertent disclosure by a person who is allowed to access PHI at an organization to another person allowed to access PHI from the same entity. *(Ex)* A nurse accidently sends their QA consultant the wrong patient chart.

**Information that cannot be retained** – A disclosure of PHI where the organization believes that the party who accessed the information was not reasonably able to retain the information. *(Ex)* A visitor assisted a nurse in picking up a chart that was dropped on the floor.
BREACHES, REPORTING, & PENALTIES

Reporting Breaches

Once it has been determined that a breach has occurred, the organization must immediately notify the HIPAA Privacy Officer.

The HIPAA Privacy Officer is responsible for notifying the Administrator, Chief Compliance Officer and Legal.

The **Covered Entity** has an obligation to report breaches within the following time frames:

1. **California Department of Public Health (CDPH)** – The Covered Entity must report all breaches to CDPH within 15 business days.

2. **Office for Civil Rights (OCR)** – The Covered Entity must report breaches that affect over 500 individuals to OCR immediately. All other breaches must be reported within 60 calendar days of the end of the year in which the breach was discovered. Reporting will be done online.

3. **Notification to affected individuals** – The Covered Entity must provide written notification of a breach to the individuals whose information has been breached.
BREACHES, REPORTING, & PENALTIES

Breaches by Business Associates

• If a breach of unsecured PHI occurs at or by a Business Associate, the Business Associate must notify the Covered Entity immediately.

• Business Associates are directly liable for their breaches as long as the Covered Entity has executed a Business Associate Agreement with the third party.
## BREACHES, REPORTING, & PENALTIES

<table>
<thead>
<tr>
<th>HIPAA VIOLATION</th>
<th>PENALTY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual did not know that he/she violated HIPAA</td>
<td>$100 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation due to reasonable cause and not willful neglect</td>
<td>$1,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation due to willful neglect but violation is corrected within the required time period</td>
<td>$10,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation is due to willful neglect and is not corrected</td>
<td>At least $50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
</tbody>
</table>
COMPLYING WITH PRIVACY & SECURITY LAWS

- Why should all staff members make it a priority to abide by HIPAA?

We want to ensure that:
- We protect our client’s PHI;
- We demonstrate and promote the fact that our organization is a place clients can trust; and
- We want to follow the law.

Employees who violate any privacy or security law expose BHCOE to liability, as well as personal risk which may lead to termination of employment or criminal liability.
A SINGLE, ONGOING DIRECTIVE: DOCUMENT, DOCUMENT, DOCUMENT......

ASK ME WHAT HAPPENS IF YOU SPEND TIME AND RESOURCES ON RISK MANAGEMENT, BUT FAIL TO DOCUMENT IT!!!!
CONCLUSION: THE LEAST IMPORTANT PERSON IN THE ROOM
QUESTIONS

Nicholas Merkin
Chief Executive Officer
Compliagent
P. 310.996.8950 | F. 310.996.8955
nmerkin@compliagent.com
www.compliagent.com