American Behavioral

ANNUAL HIPAA TRAINING 2019

What is HIPAA?

- The **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct of 1996 (HIPAA) is a federal law covering health care and health insurance industries.
- This training session focuses on the issues of protecting the privacy and security of health data, which HIPAA calls Protected Health Information (PHI).
- All associates are required by federal law to comply with HIPAA Regulations.

Covered Entities

In addition to our associates, other Covered Entities that we interact with must also comply with HIPAA requirements, including:

- Health plans, HMOs, government plans such as Medicare, Medicaid, and veterans health care programs;
- Providers (doctors, hospitals, labs, DME companies, etc.);
- Health care clearinghouses; and

Business Associates (BAs) that contract with a covered entity to help the covered entity carry out health care activities and functions must also comply.

Protected Health Information (PHI)

Any health information that is individually identifiable (including demographic information) that:

- Is created, received, transmitted, or maintained by our company and Covered Entities;
- Relates to or describes the past, present or future condition of an individual;
- Relates to or describes the past, present or future provision of care to an individual;
- Relates to payment for the provision of health care to an individual.

Examples of PHI:

- Claims
- Authorization information
- Explanation of Benefits (EOBs)
- Detailed Remittance Advices (DRAs)
- Photographs that can be used to identify a patient
- Medical records or notes
- Any health information that includes an individually identifiable data element (PHI Data Element)

PHI Data Elements

- Biometric identifiers (finger and voice)
- Account numbers, Medical Record numbers
- Full face photographic images and any comparable images
- Web locators (URLs); Internet Protocol (IP) address numbers
- Names, Dates of Birth, Admit/Discharge Dates, dates of death and all ages over 89; Email addresses, fax numbers, telephone numbers, postal address smaller than state
- Vehicle identifiers and serial numbers
- Social Security numbers; certificate/license numbers
- Health plan ID numbers; device identifiers and serial numbers

Personally Identifiable Information (PII)

Personally Identifiable Information (PII) is information used to distinguish or trace an individual's identity.

PII may be used alone or combined with other identifying information linked to a specific individual (date and place of birth, mother's maiden name, etc.).

YOU MUST PROTECT PII THE SAME AS PHI!

Information Sources to Protect

Verbal Communications including voicemail

Electronic Information (computer, cell phone, flash drives, etc.)

X-rays, Photographs, and Digital Images

Paper documents

How long should we protect PHI?

- PHI must be protected indefinitely—even after an employee terminates employment or a vendor's contract terminates
- HIPAA records must be retained according to the corporate policy which is at least 10 years.

WARNING!

- HIPAA Violations can result in federal, state, and criminal penalties, and civil suits.
- In addition to corporate disciplinary actions, you can be subject to misdemeanor charges and big fines!
- The Department of Health and Human Services through the Office for Civil Rights (OCR) can fine our company anywhere from $100 per violation up to $1.5 MILLION per calendar year.
- Criminal penalties for "wrongful disclosure" can include fines of $50,000 to $250,000 and up to 10 years in prison - - this applies to all employees!
- Individuals who fail to comply with HIPAA and protect information held by federal and state agencies may also be subject to penalties under The Privacy Act (5 U.S.C. 552a).
- Penalties can include misdemeanor charges and fines up to $5,000.

- Individuals that willfully access or disclose social security information for a reason other than a HIPAA permissible purpose may also be subject to the following penalties under the Internal Revenue Code (IRC) at 26 U.S.C.A. 7213, 7431, and 26 CFR 301.6103(n):
- Unauthorized disclosure – Imprisonment for up to 5 years, and/or a $5,000 fine
- Unauthorized access – Imprisonment for up to 1 year and/or a $1,000 fine
- Civil recourse – Minimum of $1,000 per unauthorized access/disclosure. Punitive damages may also apply!

NEWS

FOR IMMEDIATE RELEASE
April 24, 2017

Contact: HHS Press Office
202-690-6343
media@hhs.gov

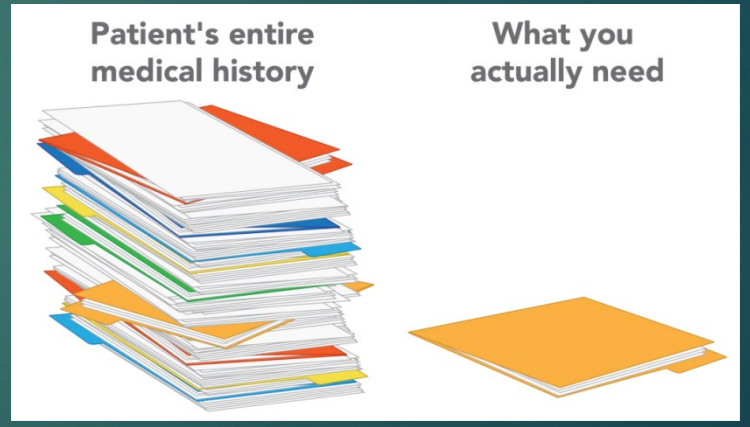
$2.5 million settlement shows that not understanding HIPAA requirements creates risk

The U.S. Department of Health and Human Services, Office for Civil Rights (OCR), has announced a Health Insurance Portability and Accountability Act of 1996 (HIPAA) settlement based on the impermissible disclosure of unsecured electronic protected health information (ePHI). CardioNet has agreed to settle potential noncompliance with the HIPAA Privacy and Security Rules by paying $2.5 million and implementing a corrective action plan. This settlement is the first involving a wireless health services provider, as CardioNet provides remote mobile monitoring of and rapid response to patients at risk for cardiac arrhythmias.

In January 2012, CardioNet reported to the HHS Office for Civil Rights (OCR) that a workforce member's laptop was stolen from a parked vehicle outside of the employee's home. The laptop contained the ePHI of 1,391 individuals. OCR's investigation into the impermissible disclosure revealed that CardioNet had an insufficient risk analysis and risk management processes in place at the time of the theft. Additionally, CardioNet's policies and procedures implementing the standards of the HIPAA Security Rule were in draft form and had not been implemented. Further, the Pennsylvania –based organization was unable to produce any final policies or procedures regarding the implementation of safeguards for ePHI, including those for mobile devices.

HIPAA Privacy Rule Essentials

- With few exceptions, Covered Entities can access, use, or disclose PHI for Treatment, Payment, or Health Care Operations (TPO).
- Do not discuss PHI with others who do not need to know the information to perform their job.
- Do not discuss PHI with family or friends.



What is TPO ?

- Treatment – provision, coordination, or management of health care for a patient.
  - A provider referring a patient to a specialist is an example of treatment.
- Payment – activities by a health plan to determine responsibilities for coverage under the health plan policy or activities by providers to obtain reimbursement for the provision of health care.
  - processing claims and prior authorization requests are examples of payment.
- Health Care Operations – certain administrative, financial, legal and quality improvement activities of our company necessary to run the business and to support our core TPO functions.

Who Can You Disclose PHI/PII To?

- Providers involved in the member's treatment
- Another HIPAA Covered Entity if the entity has or had a relationship with the member and the PHI is needed for a TPO function
- A Business Associate (BA) if the PHI is necessary for the BA to perform a function on our behalf.
- The Member who is the subject of the PHI
- To a parent covered on the same policy of a child age 13 or younger
- *Disclosures for a child age 14 or older requires the child's authorization*
- The Member's Power of Attorney (POA) or Legal Guardian
- PHI can be disclosed once proof has been obtained and SPECIFICALLY authorize health disclosures.
- The Member's appointed Personal Representative
- A completed Personal Representative Form provides a "blanket authorization" allowing us to share PHI indefinitely until the member revokes (in writing) the appointment or upon member's death.

Corporate policy for disclosing PHI on behalf of a member:

- A verbal authorization by the member to disclose PHI is permissible for the duration of one phone call.
- The *Patient Authorization for Use and/or Disclosure of Protected Health Information form # 27627159v1* must be completed and signed by the patient to disclose their PHI any further. This form is available from the Quality Department.
- The time period for which PHI is permitted to be disclosed is indicated on the form, otherwise it expires one year from the signed date.
- **Note: If an individual has *Power of Attorney* for a member then we are required to obtain a copy of the legal *Power of Attorney* form.**

EMERGENCY

- You can disclose PHI to a member's family/friends involved in the member's care in emergency situations where the member is temporarily incapacitated or unable to agree or object.

- Be sure to use good judgement and thoroughly document the situation in the system your department uses primarily

Long-Term Incapacity

In the event of a long term incapacitation of a member, PHI can be disclosed to family when:

- The disclosure is to the member's spouse, parent, sibling, or next of kin over the age of 19;
- The family member completes the required Personal Representative Attestation for Long-Term Incapacitated Members; AND
- Proof of long-term incapacity from a treating physician is provided with the Attestation (e.g. letter from the member's PCP/PMP confirming the member's incapacity).

Long-Term Incapacity Documentation

- Once all of the appropriate documentation is submitted, it provides "blanket authorization" for us to disclose to the next of kin listed on the Attestation.

- Always document the receipt of this documentation in the system your department uses primarily
- Talk to you supervisor if you have any questions.

Disclosing PHI

Only Use or Disclose the Minimum

- Do not disclose PHI to any individual unless you are sure they are authorized to receive it!
- HIPAA requires that employees only ask for, use, and disclose the minimum information necessary to accomplish the task.
- The only exceptions to this rule are disclosures involving:
  - Treatment of the member
  - Purposes the member has authorized in writing
  - Disclosures required by law
  - Sharing PHI with the member who is the subject of the PHI

- Before disclosing PHI, always ask for key identifiers about the member and validate the information against what is stored in our systems.
  - Member ID Number
  - Date of birth
  - Full Name;
  - Address and phone number

PHI RED FLAGS

- People can be very tricky when trying to get you to inappropriately disclose PHI. So use sound judgment!

- Be on the look out for these types of questions:
  - *"Was a pregnancy test performed during the visit or is the member pregnant?"*
  - *"Was the member screened for a sexually transmitted disease?"*
  - *"Did the blood test reveal AIDS or HIV?"*
  - *"Was the member diagnosed with a mental illness?"*
  - *"What is the diagnosis for the authorization provided or listed on the claim?"*

- Generally, these are the types of questions that should be discussed with their treating provider – not their health plan.

NEWS

FOR IMMEDIATE RELEASE
May 23, 2017

Contact: HHS Press Office
202-690-6343
media@hhs.gov

Careless handling of HIV information jeopardizes patient's privacy, costs entity $387k

St. Luke's-Roosevelt Hospital Center Inc. (St. Luke's) has paid the U.S. Department of Health and Human Services (HHS) $387,200 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule and agreed to implement a comprehensive corrective action plan. St. Luke's operates the Institute for Advanced Medicine, formerly Spencer Cox Center for Health (the Spencer Cox Center), which provides comprehensive health services to persons living with HIV or AIDS and other chronic diseases. St. Luke's is 1 of 7 hospitals that comprise the Mount Sinai Health System (MSHS).

In September 2014, the HHS Office for Civil Rights (OCR) received a complaint alleging that a staff member from the Spencer Cox Center impermissibly disclosed the complainant's protected health information (PHI) to the complainant's employer. This impermissible disclosure included sensitive information concerning HIV status, medical care, sexually transmitted diseases, medications, sexual orientation, mental health diagnosis, and physical abuse. OCR's subsequent investigation revealed that staff at the Spencer Cox Center impermissibly faxed the patient's PHI to his employer rather than sending it to the requested personal post office box. Additionally, OCR discovered that the Spencer Cox Center was responsible for a related breach of sensitive information that occurred nine months prior to the aforementioned incident but had not addressed the vulnerabilities in their compliance program to prevent impermissible disclosures.

When PHI gets personal

- Only look at records necessary needed to carry-out the functions of our TPO.
- Do not use your employee access to our systems (or to a provider's system) to look at your own records or the records of family and friends for personal reasons (even if you are the member's authorized representative).
- If you need PHI for personal reasons, you must follow the same procedures as other members – this means:
  - You must request access to PHI through the appropriate customer service department

Business Reasons for Accessing Your Own or Your Family's PHI

- In the very rare circumstances where your job requires you to access your own PHI, or the PHI for someone you are legally authorized to access, you must not take actions or make decisions that could create an unfair advantage over other members that are similarly situated (in other words, you must avoid a conflict of interest).

- You must never add, edit or delete any information to your own record or the record of another member that has authorized you to be his/her Personal Representative.

  - Example: A nurse in Health Services receives a request from a hospital to prior authorize her own surgery. The nurse must transfer the call to another authorized employee or to her supervisor to enter the authorization information

Transferring a Task to Protect PHI

If while performing your job responsibilities, a situation arises that would cause you to gain access to a family member's PHI that lives in your same household or that is covered under your same policy and the family member has not authorized in writing for you to have such access, you must transfer the task to another authorized employee or contact your supervisor for help.

- Example: An associate takes a call from a provider in the queue. The provider is checking the status of a claim on the associate's spouse, but the spouse has never legally authorized the associate to access their records. The associate must transfer the call to another authorized associate , or to their supervisor, to ensure that they do not obtain PHI for their spouse.

Security Rule Essentials

- The HIPAA Security Rule requires that we maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting PHI. This means we must:
  - Ensure the confidentiality, integrity and availability of PHI
  - Identify and protect against reasonably anticipated threats to security or integrity of the information

In-Office Safeguards

Don't leave PHI on printers, copiers, or fax machines for long periods of time.

Do not distribute any form of identifiable member information in a meeting (especially with others outside of the company) unless every single person needs to know the information.

At the end of the day, put away PHI (or at a minimum, turn PHI face down on your desk).

If identifiable member information must be shared in a meeting, collect the member information when the meeting is over, whenever possible.

Additional Safeguards

- Do not take pictures on your phone or camera in any area where PHI is located.
- Do not use FaceTime or other video applications where PHI can be seen by unauthorized people.
- NEVER, NEVER post any member information on social media.

Remote Office Safeguards

- Do not print any documents unless you are authorized to do so and have an approved document shredder
- Always Lock your computer when not at your desk
- Never share passwords
- Your computer must always be connected to the VPN
- Refer to the Remote Office Policy Manual for additional information

Off-Site Safeguards

Remember, you are responsible for PHI in your possession at all times!

- PHI can ONLY be taken off-site if approved by your supervisor and the President.
- Never leave PHI unattended in public locations or stored in plain sight in your automobile.
- Never store PHI at your home in your automobile for extended periods of time. Return PHI to the office the same or next business day when possible.
- Take extra precautions when working remotely so that unauthorized individuals cannot hear, see, or access PHI.
- This includes family members, friends, your dog, the general public and anyone not authorized to access PHI.

System Safeguards

- You are responsible for what happens under your login!
- Always lock your screen before leaving your workstation.
- Position your computer screen so PHI/PII is not visible to unauthorized individuals.
- Never share your password or login credentials with anyone.
- Try to use strong passwords whenever possible that contain alphanumeric characters, upper/lower case letters, symbols, numbers, etc.
- If helpful, write a password hint (not password) and store in a secure area – such as in your wallet.
- Do not download software to your computer
- Do not purchase software that requires storing, processing, or transmitting PHI/PII without approval

In-Office Physical Safeguards

- Do not give access to a secure area to someone you do not recognize
- Ensure visitors are escorted at all times
- Do not prop open doors to secure areas

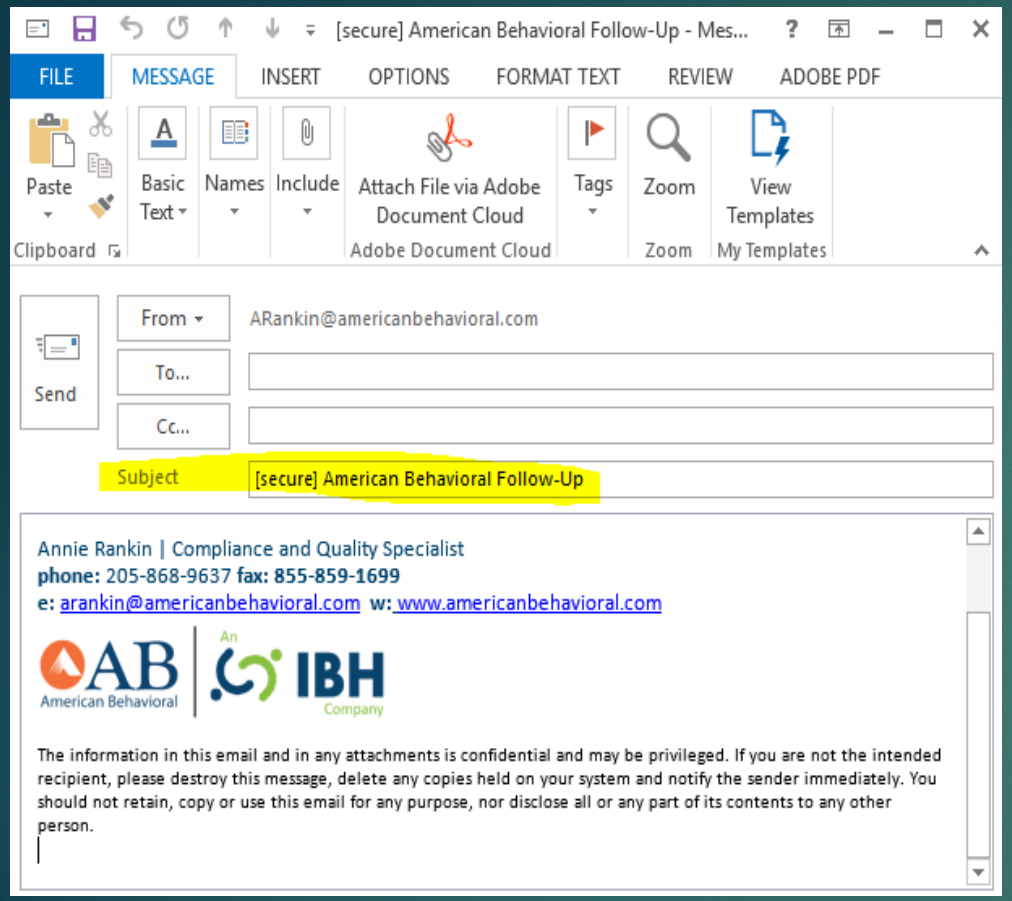
Fax Safeguards

- SLOW DOWN and be sure that you are faxing (or e-faxing) the correct recipient.
- Verify fax numbers before sending.
- Use a Corporate approved fax coversheet when sending faxes.
- READ confirmation sheets to verify that the fax was successful and accurate.
- Fax only the minimum information necessary.
- **Report any fax incidents to the Privacy Officer, Debbie Garvin**

Email Safeguards

- Be very careful to select the correct email recipient before hitting send!
- Never forward your email account or work emails to your personal email account. Business emails must remain within the corporate email systems.
- DO NOT OPEN any suspicious emails; report them to Parris Caldwell. Watch out for suspicious emails that ask you to click attachments, click a link, provide confidential information, or to reset your password.

E-Mail Safeguards



Encrypt all emails containing PHI/PII to any recipient outside of our company.

This can be done by typing "[encrypt]" or "[secure]" in the email subject line.
Do not include PHI in the subject line. Use generic subjects.

The Corporate Confidentiality Notice MUST appear at the bottom of all work emails!

Business Email Compromise (BEC)

Business Email Compromise (BEC)

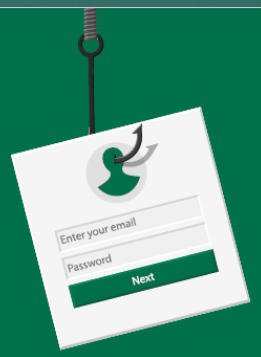
The Office for Civil Rights announced that Anthem, Inc. has agreed to pay $16 million for a breach, the largest in health data history, that exposed PHI of 79 million people. This breach was facilitated by a phishing email that at least one employee clicked on which provided hackers access to Anthem's network. A civil settlement of $115 million was approved to be split among the plaintiffs in the class-action lawsuit against Anthem.

Phishing emails remain the No. 1 threat companies face in terms of Information Security. Although there are many different approaches, the scammers typically try to impersonate an executive or use persuasive language in their phishing emails to trick recipients into such things as replying back with sensitive information, clicking on links to fake websites, or downloading attachments that contain malware (including ransomware).

On June 29, the FBI released its 2017 Internet Crime Report:

- **301,580** complaints made, exceeding $1.4 billion in losses
- **25,344** reports of phishing incidents, resulting in losses of **$29,703,421**
- Phishing and email scams continue to be a major concern

It's critical that our business associates (BAs) educate their employees on the dangers of phishing emails. Such attacks could not only compromise our BA's data, but could also impact Viva Health's data that is stored, transmitted, or accessed by our BAs.



What to watch for in phishing emails?

- Known sender name, but "mailto" doesn't match – example below:
  From: Lynn Murphree
  [mailto:admin@company-execs.com]
- Unknown sender
- Unexpected attachment
- Sender name in the address does not match the name in the email signature
- Poor grammar
- Sense of urgency
- Asking for sensitive information *(banking information, passwords, etc.)*

For additional information regarding cybersecurity education, please visit the Department of Health and Human Services' website at https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html.

Viva Health, Inc., | 417 20th Street North, Suite 1100, Birmingham, AL 35203 | www.VivaHealth.com/FDR

Saving PHI

- Only save PHI to a secure network drive (M: Drive)
  - Never the F: Drive as everyone in the company can see this.

- Do not save PHI to your hard drive as these files are NOT backed up and can be lost!!

Disposing of PHI

Never hand-shred paper documents or put PHI in a regular trash can.

In the office, place PHI in the designated Shred-It bins.

Transporting PHI

- The only Corporate approved methods for transporting electronic PHI (ePHI) are:
  - Encrypted email
  - Corporate Issued e-fax
- **If you have questions or concerns about transporting ePHI, please contact your supervisor the HIPAA Security Officer, Debbie Childress.**

Unapproved Personal Devices

- Employees are prohibited from using any printers or shredders for business unless it has been approved by Debbie Garvin and your department head.
- **Flash Drives are always prohibited.**

Computer Usage and the Internet

- Use of company devices (laptops, cell phones, etc.) should be used primarily for official business. This include internet usage.
- Be careful when going to websites that are not reputable or you are not familiar with.
- Malware can be put on your computer and the company network through such ways as:
  - Phishing email with a link or attachment
  - Downloading a document from a website
  - Clicking on a pop-up add on a website

NEWS

BULLETIN – July 10, 2015

HIPAA Settlement Highlights Importance of Safeguards When Using Internet Applications

St. Elizabeth's Medical Center (SEMC) has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security and Breach Notification Rules with the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR). SEMC will pay $218,400 and will adopt a robust corrective action plan to correct deficiencies in its HIPAA compliance program. SEMC is a tertiary care hospital located in Brighton, Massachusetts that offers both inpatient and outpatient services.

On November 16, 2012, OCR received a complaint alleging noncompliance with the HIPAA Rules by SEMC workforce members. Specifically, the complaint alleged that workforce members used an internet-based document sharing application to store documents containing electronic protected health information (ePHI) of at least 498 individuals without having analyzed the risks associated with such a practice. Additionally, OCR's investigation determined that SEMC failed to timely identify and respond to the known security incident, mitigate the harmful effects of the security incident, and document the security incident and its outcome. Separately, on August 25, 2014, SEMC submitted notification to HHS OCR regarding a breach of unsecured ePHI stored on a former SEMC workforce member's personal laptop and USB flash drive, affecting 595 individuals.

Incident Reporting

- It is your obligation to try and avoid a HIPAA incident in every possible way!

- If an incident or activity occurs that could possibly compromise PHI, you MUST report this immediately to:

- Your Supervisor;
- Privacy Officer;
  - Debbie Garvin
  - dgarvin@americanbehavioral.com
- Data Security Officer;
  - Debbie Childress
  - dchildress@americanbehavioral.com

Breaches

A HIPAA breach occurs when PHI is “acquired, accessed, used, or disclosed” in an unauthorized manner that compromises the security or privacy of the information.

Breaches

- HIPAA breaches can result from:
  - Accessing PHI without a work-related need to know
  - Sharing PHI with those not needing to know
  - Sending emails/faxes/mail to the wrong recipient
  - Loss or theft of records containing PHI
- Breaches occur when you do not take the required precautions when handling member information.

Breach Requirements

- If a HIPAA breach occurs, The Company must:
  - Notify impacted individuals within 60 days of discovery of the breach.
  - Report the breach to HHS in annual reporting (if less than 500 individuals impacted).
  - If the breach impacts 500 or more individuals, The Company must notify HHS immediately and the local media – and HHS posts the breach on their website.

Types of Incidents to Report

- Lost or stolen PHI
- Misdirected mail, emails, faxes, etc. containing PHI
- Lost or stolen electronic devices
- Unusual messages shown on your computer that make you question your system's security
- Suspicion of others misusing or abusing PHI
- ANY other incident/activity that compromises any member data!
- If you notice anything unusual about your computer, e.g. a suspicious pop-up, locked screen, any thing that doesn't look right – immediately report it to the Help Desk

Points of Contact

If you have any questions or concerns, we are here to help!

- The HIPAA resources are available to upon request from the Quality Department.

Debbie Garvin, Privacy Officer

- Email: dgarvin@americanbehavioral.com

Debbie Childress, Data Security Officer

- Email: dchildress@americanbehavioral.com