Welcome to the TotalWellness *Privacy and Security* Annual Training

April 2024

TOTALWELLNESS

Privacy & Security Training Sections

- What is HIPAA & Why is it Important?
- HIPAA Definitions
- Participant Rights
- Privacy Rule Implementation
- Security Rule Implementation
- HIPAA Violations & Data Breaches
- Helpful Tips

Privacy & Security Training Resources

President & Privacy Officer

Alan Kohll
akohll@totalwellnesshealth.com

Compliance Committee Members

Kristina Macklin
kmacklin@totalwellnesshealth.com

Lisa Stovall
lstovall@totalwellnesshealth.com

Section 1

What is HIPAA &
Why is it Important?

TOTALWELLNESS

What is HIPAA?

- HIPAA is an acronym for the Health Insurance Portability & Accountability Act of 1996 (45 C.F.R. parts 160 & 164)

- HIPAA provides a framework for establishment of nationwide protection of participant confidentiality and security of electronic systems.

- HIPAA is comprised of the following:
    1. Privacy Rule
    2. Security Rule
    3. Electronic Data Exchange

Privacy Rule

Effective Date – The Privacy Rule went into effect on April 14, 2003.

Protection – The Privacy Rule refers to protection of an individual's health care data.

Definition – The Privacy Rule defines how patient information is used and disclosed.

Rights – The Privacy Rule gives participants privacy rights and more control over their own health information.

Outlines – The Privacy Rule outlines ways to safeguard Protected Health Information (PHI).

Security Rule (IT)

Effective Date – The Security Rule for IT regulations went into effect on April 21, 2005.

Protection means controlling:

1. Confidentiality of electronic Protected Health Information (ePHI)
2. Storage of electronic Protected Health Information (ePHI)
3. Access into electronic information

Electronic Data Exchange (EDI)

The EDI component of HIPAA defines the transfer format of electronic information between providers and payers and outlines standardization of coding, billing, and insurance.

We at TotalWellness need to be aware of the EDI component of HIPAA, but this component rarely affects us.

Why is HIPAA Important?

HIPAA is important because it shows a commitment to protecting privacy

- As an employee, you are obligated to comply with TotalWellness privacy and security policies and procedures
- Our participants are placing their trust in us to preserve the privacy of their sensitive and personal information
- Compliance is not an option, it is required
- If you choose not to follow the rules:
    1. You could be put at risk, including personal penalties and sanctions
    2. You could put TotalWellness at risk, including financial and reputational harm

HIPAA Regulations

HIPAA regulations require we protect our participants' PHI in all media including, but not limited to, PHI created, stored, or transmitted in/on the following media:

Verbal Discussions in person or over the phone
Written on paper including consent forms, participant handouts, applications, etc.
Computer Applications and Systems including our on-site data collection tool, scheduler, PCP tool, Aggregate tool, etc.
Computer Hardware/Equipment including computers, laptops, servers, cell phones, etc.

Why is HIPAA Training Important?

Anytime you encounter patient information or any PHI that is written, spoken or electronically stored, YOU become involved with some facet of the privacy and security regulations.

- TotalWellness wants to ensure that you know how to properly work with PHI
- TotalWellness wants you to take the confidentiality of participant information seriously
- TotalWellness is required by law to train you

It's not just about HIPAA – it's about doing the right thing!

Section 2
HIPAA Definitions

TOTALWELLNESS

What is Protected Health Information (PHI)

Protected Health Information (PHI) is individually identifiable health information that relates to a past, present or future:

- physical or mental health condition
- health care for that condition
- payment for that care

PHI must be protected if collected, stored, or used by a provider, health plan, clearinghouse or employer. Wellness programs, provided by TotalWellness, fall under the health plan.

PHI Includes:

- Service documentation (consent forms)
- Screening values/lab results
- Appointment dates/times
- Health history
- Participant identifiers

What are Participant Identifiers?

PHI includes information by which the identity of a participant can be determined with reasonable accuracy and speed either directly or by reference to other publicly available information.

Examples of Participant Identifiers:

- Names
- Social Security Numbers
- Birth dates
- Telephone numbers
- Email addresses

PHI is Not:

Aggregate data, statistics, or health information that's been stripped of identifiable pieces.

What are Uses and Disclosures?

Uses:

When we review or use PHI internally.

Example: When we utilize screening results to counsel an individual on their health.

Disclosures:

When we release or provide PHI to someone else.

Example: When we send participant's data to their health portal.

Participants must sign a consent form authorizing TotalWellness to use their data. The consent form will also include information about disclosing the participant's data, if applicable. Participants must always sign a consent form to receive services from TotalWellness.

What is Minimum Necessary?

Using or disclosing/releasing only the minimum necessary to accomplish a goal.

- The fewest possible people allowed access
- Access to the smallest amount of information possible
- Limit access to a “Need to Know” basis

Examples:

- Limiting access to the data scanning room
- Gathering limited information from participants
- Limiting access to the data storage room
- Transferring only the necessary data
  - IE. We don’t transfer or receive Social Security Numbers unless 100% necessary

Section 3
Participant Rights

TOTALWELLNESS

What are Participant's Rights under HIPAA?

1. The right to individual privacy.
2. The right to expect Health Care Providers (us) will protect these rights.

Notice of Privacy Practices

Our Notices of Privacy Practices summarizes how TotalWellness uses and discloses the participant's PHI. It also details the participant's rights with respect to their PHI.

The TotalWellness Notice of Privacy Practices is available on-site at each event and on our website at https://www.totalwellnesshealth.com/privacy-notice. When participants sign our consent form they acknowledge that they have had the opportunity to read our Notices of Privacy Practices.

Participant Actions

- Participants have the right to inspect and copy their PHI.
- Participants must complete a "Consent Form Copy Request" form to receive a copy of their consent form and results.

Section 4
Privacy Rule Implementation

TOTALWELLNESS

TotalWellness Responsibilities

Training. TotalWellness is responsible for training all internal employees and contractors on HIPAA policies and procedures.

Physical Security. TotalWellness is responsible for creating a secure physical atmosphere for data to be accessed and stored.

Maintain Records. TotalWellness must retain records that contain PHI for a specific duration.

Documentation. TotalWellness is required to document our privacy policies.

PHI Misuse

The following activities occurring in the absence of patient authorization are considered misuse of protected health information (PHI):

- Accessing
- Using
- Taking
- Possessing
- Releasing
- Editing
- Destructing

Examples

1. Jane participated in an on-site screening event. On the consent form Jane signed off that she was ok with sharing her information with her Health Management Company. Jane did not authorize the sharing of her information with her employer. It would be a misuse of PHI for TotalWellness to share Jane's information with her employer.

2. John had his cholesterol checked at an on-site event and his result was a cholesterol reading of 240 mg/dL. It would be a misuse of PHI for TotalWellness to change his cholesterol number to 140 mg/dL to make his company's aggregate report look better.

Privacy Violations

Type 1 – Inadvertent or Unintentional Disclosure

Inadvertent, unintentional or negligent act which violates the policy and may or may not result in PHI being disclosed.

Examples:

- Leaving completed consent forms results side up at on-site events – another participant may walk by and see the results.
- Leaving participant data exposed at your desk – a guest may walk by and be able to view the data.
- Accidentally counseling participant A with participant B's results.
- Sharing a contractor's birthdate with the wrong contractor.



Preventing Type 1 Privacy Violations

Be mindful of your actions, so you can actively prevent Type 1 – Accidental or Unintentional PHI Disclosure violations.

1. Always leave participant forms results side down at on-site events.
2. Do not leave data at your desk unattended. (IE. Lock your computer when you leave your desk, lock up paperwork containing PHI when you are not utilizing it, etc.)
3. At on-site events always verify the participant using 3 data points (first name, last name, date of birth) before sharing results.
4. Have contractors relay information to you, not the other way around. (IE. Instead of asking, is your birthdate xx/xx/xxxx, ask can you please verify your birthdate.)

Type 2 – Intentional Disclosure

Intentional act which violates the organization's policies pertaining to that PHI which may or may not result in actual harm to the participant or personal gain to the employee.

Examples

1. Paperwork is lost for an event and instead of notifying the client results are "made up" for all of the participants.

2. Participants do not authorize that data can be shared with their health plan, but the data is sent to the health plan anyway.

3. Contractor calls in and asks for information on another contractor and the information including date of birth and address are provided.

Preventing Type 2 Privacy Violations

TotalWellness has developed policies that outline expectations and consequences for intentionally disclosing PHI.

1. Abide by all set forth policies.
2. Do not share information with anyone other than the participant themselves.

When is it ok to share PHI?

- You may share a participant's PHI with the participant. You must verify who the participant is, verifying at least 3 data points, before sharing information.
- If the participant's consent form includes language that they "authorize the release of their information to…" TotalWellness can share the PHI with the organization identified in the consent, as long as the participant signs the consent form.



TotalWellness Privacy Policies

Privacy at Events

- Speak to participants in a secure area where it is unlikely PHI will be overheard.
- Speak to participants at a volume they can hear, but the rest of the room can't hear.
- Point to health screening results rather than saying them out loud.
- Only discuss an individual's health with that individual. This means don't discuss it with other contractors, other participants or the employer.
- When calling participants to the health education station or prior to entering data into an iPad, verify 3 participant data points (first name, last name, date of birth, and/or unique id) to ensure you have the correct participant.
- Keep forms and paperwork face down or covered when not in use.
- Don't allow companies to make copies of completed consent forms.
- Don't leave forms or health data unattended.
- Don't give any individual health data to the employer.
- Avoid visible, verbal or nonverbal cues as to what health data you might be discussing. For example, if you are shocked by a participant's numbers don't show it.

TotalWellness Privacy Policies

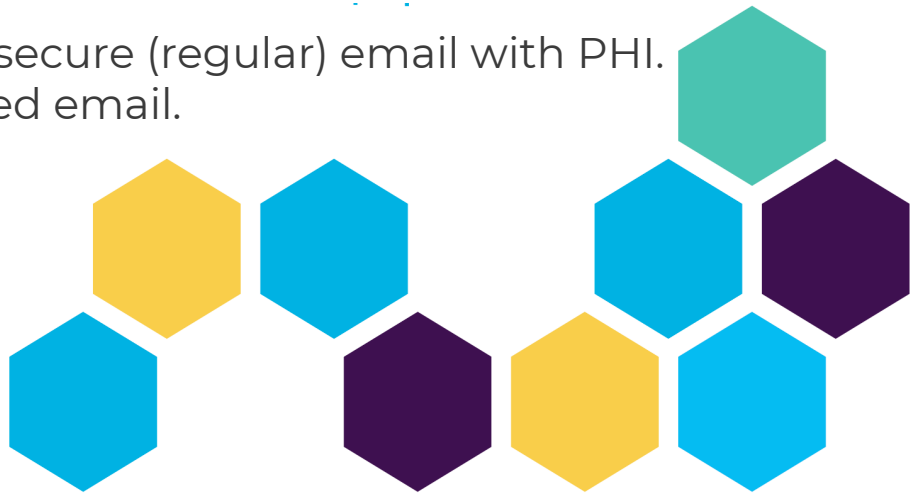
Privacy in the Office

- When speaking with participants on the phone about their data, speak to participants in a secure area. For example at your desk not out in the parking lot.
- When speaking with participants on the phone about their data, speak at a volume they can hear, but that others cannot easily overhear. For example don't yell into the phone, guests at TotalWellness may be able to hear you if you yell.
- Only discuss an individual's health with that individual. Ensure that the participant verifies 3 data points before discussing results with the individual.
    - Always make sure that the participant provides the information, not the other way around. For example ask what is your date of birth, not is your date of birth xx/xx/xxxx?
- Don't share individual results with the individual's employer.

TotalWellness Privacy Policies

Privacy in the Office, Continued.

- Keep consent forms and all paperwork containing PHI face down or covered when not in use.
- Do not leave PHI unattended. If you need to get up from your desk, lock up PHI. NOTE: All TotalWellness consent forms are considered PHI.
- All documents containing PHI should be shredded. Do not throw documents containing PHI in the regular trash.
- Only access areas that you are authorized to access.
- Use the Minimum Necessary rule when saving and storing data.
- Use email encryption when communicating about PHI. PHI data can include name, date of birth, unique ID, screening values, etc.
  - If in doubt, use encryption!
  - Clients may contact you using unsecure (regular) email with PHI. Always respond using an encrypted email.



Privacy Policies

Consent Request

Participants often request copies of their consent forms and/or results. We can provide participants with their information by following these steps.

1. Have the participant complete a Consent Copy Request Form.
2. Retrieve the participant's consent form from the secured area (Secured Room or Encrypted O Drive)
3. Verify the first name, last name, and signature match.
4. Send a copy of the consent form to the fax, physical address, or email address (use encryption) provided on the Consent Copy Request Form.

Section 5
Security Rule Implementation

TOTALWELLNESS

Security Rule

In general, the HIPAA Security Rule requires that TotalWellness do the following:

1. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic protected health information (ePHI) that is created, received, maintained, or transmitted.
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI.
3. Protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required under the Privacy Rule.
4. Ensure compliance with security by our workforce.

Applying the Security Rule

1

Administrative Safeguards

Policies and procedures are required and must be followed by employees to maintain security.

2

Technical Safeguards

Technical devices needed to maintain security.

- Assignment of different access levels.
- Badge/security code access.
- Computer logout/lock screens.

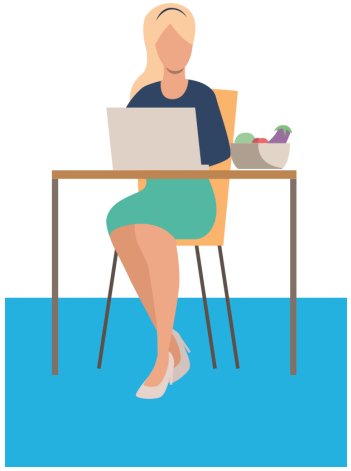
3

Physical Safeguards

Must have physical barriers and devices:

- Lock doors
- Monitor visitors
- Secure unattended computers

Security Procedures



Internet Use

- Access only trusted, approved sites
- Don’t download programs to your workstation

Email

- Keep email content professional
- Use work email for work purposes only
- Don’t open emails or attachments if you are suspicious of or don’t know the sender
  - If you receive a suspicious email notify DataServ.
- Don’t forward jokes
- Use email encryption when sending emails that contain PHI
- Verify email addresses before sending emails
- Include the TotalWellness confidentiality disclaimer on all emails
  - *Disclaimer: This email and any files transmitted with it are confidential. If you have received this email in error please notify the sender and then delete it immediately.*

Encryption

- Store files containing PHI on our encrypted Shared Drive or Operations Drive, do not store files containing PHI on your physical machine.

Security Procedures continued...

Set Secure Passwords

- Make your password as **long as possible**. Always use at least 8 characters in your password, at least two being numeric.
- **Use as many different characters as possible** when forming your password. Use numbers, special characters and mixed upper and lower-case letters.
- **Do not use personal information** in your password that someone else is likely to be able to figure out. Avoid things like your name, phone number, address, birthdate, etc.
- Do not use passwords that are **easy to spot while you're typing them in.** Passwords like 12345, qwerty, or nnnnnnn should be avoided.

Changing Passwords

- Update your passwords at least every 60-90 days.
- Do not use the same password for more than one application.
- Do not share your password with others.

Security Procedures continued…

Protecting Computer Systems & Equipment

- At your workstation, restrict viewing access from others.
- Lock your workstation when you get up from your desk
  - (Ctrl-Alt-Del or Shift-Control-Eject)
- Do not download your own software to your machine and do not delete the software installed by TotalWellness.
- If devices are lost, stolen or compromised, notify your supervisor immediately.
- Do not store PHI on mobile or removable devices unless you are authorized to do so.

Working with the Data

- Work with Aggregate Data instead of individual records.
- Strip identifiable information when possible.
- Ensure data subsets are independent of one another
  - When you access one person's PHI, you won't come across another person's PHI.

Section 6
HIPAA Violations
and Data Breaches

TOTALWELLNESS

HIPAA Violations

Incidental Violations

When PHI is accidentally overheard or seen by an unauthorized individual.

- If reasonable steps are taken to safeguard a participant's information and another individual happens to overhear or see PHI that you are using, you are not liable for the disclosure.
- Incidental disclosures are going to happen, even in the best circumstances.

Accidental Violations

Mistakes happen. You may mistakenly disclose PHI or provide confidential information to an unauthorized individual. If this happens you must:

1. Acknowledge the mistake and notify your supervisor.
2. Learn from the error and help revise procedures (when necessary) to prevent it from happening again.
3. Assist in correcting the error if requested by your supervisor. Don't cover up and try to make it "right" by yourself.

HIPAA Violations continued...

Intentional Violations

When an individual ignores the rules and carelessly or deliberately uses or discloses PHI or other confidential information. If you do this, you can expect the following:

- Disciplinary action, up to and including termination
- Civil and/or criminal charges

Examples of intentional violations of privacy include:

- Accessing PHI for purposes other than your assigned job responsibilities.
- Attempting to learn and use another person's access information.

Data Breaches

Data Breach

An impermissible use or disclosure that compromises the security or privacy of PHI.

- If PHI is put at risk of being accessed without authorization, the information has been breached.
- Breaches include lost consent forms, storing PHI data on an unencrypted machine, leaving data unattended and exposed in a public place, sending data to the wrong organization, etc.

Data breaches exclude situations in which:

- The PHI can’t be used to re-identify the individual
- The PHI wasn’t actually accessed
- The unauthorized individual won’t recall, use or disclose the PHI

Reporting HIPAA Violations & Data Breaches

Notify your supervisor immediately if you know of or suspect a HIPAA violation or data breach.

It is important to report HIPAA Violations and Data Breaches because:

1. TotalWellness may need to notify the affected individuals.
2. Violations and breaches need to be investigated, managed, and documented.
3. TotalWellness wants to prevent similar future violations and breaches.
4. Damages need to be kept to a minimum.
5. TotalWellness would like to minimize your personal risk.

Section 7
Helpful Tips

TOTALWELLNESS

Do’s and Don’ts

Do only share PHI data with those who need to know.
Don’t share PHI data with friends, family, neighbors, etc.

Do ensure you have the correct fax number, physical address, and/or email address prior to disclosing PHI and require that the information be submitted in a written format.
Don’t send PHI to a fax number or email address gathered over the phone.

Do secure your workstation by logging off, using strong passwords and keeping passwords confidential.
Don’t leave your workstation unlocked while unattended.

Do use a separate, unique password for each application.
Don’t share your usernames or passwords with others.

Do lock up all paperwork containing PHI (including consent forms) when not in use.
Don’t leave paperwork containing PHI unattended.

Do send encrypted emails when sending PHI.
Don’t send PHI using regular email.

Do's and Don'ts

Do use the minimum necessary rule.
Don't access or send unnecessary PHI.

Do keep PHI confidential.
Don't release PHI to the media or to anyone who offers you money for it.

Do turn over or cover paper PHI when coworkers approach you to discuss something other than PHI.
Don't leave PHI out for anyone to view.

Do pick up printed PHI as soon as possible from the printer and/or fax machines.
Don't leave documents containing PHI unattended on fax machines, printers, or copiers.

Do check fax machines often and remove faxes containing PHI immediately.
Don't leave faxes containing PHI on the fax machine for extended periods of time.

Do place papers containing PHI in the shred/recycling bin or shred using the shredder.
Don't throw papers containing PHI into the regular trash.

Do's and Don'ts

Do make sure all guests check in at the reception desk.
Don't allow unauthorized guests to follow you past the reception area.

Do delete files containing PHI from your machine.
Don't keep files containing PHI on your machine.

Do keep the doors to secure areas closed at all times (teal data processing room, back storage room, etc.)
Don't prop open doors to secure areas.

Do have individuals provide information to you to verify who they are (IE. date of birth)
Don't provide options for participants to say yes or no. (IE. is your birthdate xx/xx/xxxx or is your address 123 Main Street?)

Do abide by all TotalWellness Privacy and Security Policies and Procedures.
Don't ignore TotalWellness Privacy and Security Policies and Procedures.

Do report HIPAA violations and data breaches.
Don't cover up violations or breaches and try to make them "right" yourself.

Training Completion

In order to complete your HIPAA training we require that you complete a short quiz https://www.totalwellnesshealth.com/totalwellness-employee-hipaa-training/

Questions:

Contact Kristina Macklin at kmacklin@totalwellnesshealth.com or x101.

TOTALWELLNESS

Thank You!

TOTALWELLNESS