

HIPAA PHYSICAL SAFEGUARDS MEASUREMENT TOOL
To Assess Physical Safeguards for Protecting the Privacy of Health Information

Directions: Use one worksheet for each office, building, or “campus”. Read and answer each question. Use the score key at the end to determine your overall compliance with HIPAA’s physical safeguards for protecting the privacy of **protected health information (PHI)**.

1. Can you name all the places where PHI is located in your office (or building or campus)?
 No Yes
2. When a person walks through the office (or building or campus), is PHI visible (i.e., on white boards, desks, by photocopy or fax machines, or on computer screens)?
 No Yes
3. Is PHI stored in a secure location?
 No Yes

If yes, check all that you can clearly define:

- Is the location lockable?
- Who has access?
- How is access monitored during business hours?
- How is access managed outside of business hours?
- Are there sign-out logs for PHI?
- How promptly is PHI stored?
- Who is responsible for storing?
- Is the location of PHI waiting to be stored secure?

4. Is the location of PHI locked?
 No Yes

If yes, check all that you can clearly define:

- When is the location locked?
- Who has keys/pass codes?
- How many keys are there?
- Where are keys located?
- Are keys marked “Do not duplicate?”
- How are keys returned when a staff member terminates employment?
- Are there policies and procedures regarding locks and keys?

5. Do staff members maintain PHI at their workstation?

No Yes

If yes, check all that you can clearly define:

Are workstations lockable?

Who else has access to the workstations?

What happens to the medical record/PHI when it is no longer needed?

Are there policies and procedures regarding staff members maintaining PHI at their workstations?

6. (If applicable) Does direct care staff maintain PHI in travel charts when they are off the premises?

No Yes

If yes, check all that you can clearly define:

How is the PHI protected?

Is it visible inside vehicles?

What happens if it gets lost?

What happens when the PHI is no longer needed (i.e. when a patient is discharged or dies)?

Are there policies and procedures regarding travel charts or the protection of PHI off premises?

7. Is PHI placed in staff mailboxes for later retrieval?

No Yes

If yes, check all that you can clearly define:

Is the mailroom or mailbox locked?

What happens if the staff member is on vacation?

Does the staff member who distributes the mail have access to PHI while distributing mail or anywhere in the mailroom?

Is mail opened (i.e., to determine which mailbox it goes in, to date/time stamp)?

8a. Do you receive PHI by fax machine?

No Yes

If yes, check all that you can clearly define:

How many fax machines receive PHI and where are they located?

Are they located in secure areas?

Who has access to receiving and distributing faxes?

8b. Do you send PHI by fax machine?

No Yes

If yes, check all that you can clearly define:

How are you certain that it is sent to and received by the correct recipient?

Do you have a confidentiality statement on your fax coversheets with directions specifying what to do if the fax has been misdirected?

Do you have policies and procedures regarding sending and receiving PHI by fax?

9. Do you shred PHI that is no longer needed?

No Yes

If yes, check all that you can clearly define:

Who is responsible for shredding?

How do you shred (outside company or in-house)?

Is PHI that is waiting to be shredded kept in secure areas?

Is the shredder always in good working order?

What happens when it is not?

10. Are management documents (e.g., census reports, case conference agendas) created which contain PHI?

No Yes

If yes, check all that you can clearly define:

Who prepares and receives these documents?

What happens to these documents when they are no longer needed?

Are copies of these documents safeguarded by the recipients?

11. Do you have multiple service sites?

No Yes

If yes, check all that you can clearly define:

Is PHI transferred between sites? How?

How is the PHI safeguarded during transfer?

12. Do you maintain PHI in off-site storage?

No Yes

If yes, check all that you can clearly define:

Who has access to it?

When and how is it transferred to and from off-site storage?

Are you certain that the PHI maintained in off-site storage is adequately safeguarded?

Do you have a contract with the off-site storage provider that includes provisions for the safeguarding of PHI?

13. Do people (e.g., on-call staff, support groups, community groups, cleaning services) have access to your offices outside of normal business hours?
 No Yes

If yes, check all that you can clearly define:

- Who are those persons?
 Do they also have access to PHI?
 How do you train them on privacy practices?

14. Do you maintain PHI on computers?
 No Yes

If yes, check all that you can clearly define:

- Are minimum requirements followed for access to PHI on computers?
 Are computer screens visible to casual observers?
 Are passwords used to access PHI on computers?
 Are passwords shared amongst staff members?
 Are there appropriate login and logout procedures?
 Do staff logout when they are not at their computers?
 Are role-based access restrictions built into the computer software?
 Does the software automatically “tag” PHI with a code for each user and when they accessed the PHI?
 Does HR or IS remove/deactivate former employees’ user names and passwords to prevent unauthorized further or future use? How soon after the employee leaves does this process take place?
 Is remote access (from the employee’s home computer) allowed?
 Is PHI sent or received by email?

SCORE KEY

Count the number of questions that you answered “yes” and write that number here: _____

Count the number of items that you checked under the headings “*If yes, check all that you can clearly define:*” and write that number here: _____

Add the two numbers together for your total score and write that number here: _____

COMPARE YOUR TOTAL TO THESE SCORES

68 or higher ... your physical safeguards for PHI are excellent!

40 to 67 ... you need to re-think some physical safeguards for PHI.

39 or less ... PHI is not well protected.