HIPAA RISK ASSESSMENT AUDIT

Philadelphia VA Medical Center

Service Area: _____ **Date:** _____

---

45 C.F.R. § 164.530: Safeguards. A covered entity must have in place appropriate administrative, technical and physical safeguards to protect the privacy of PHI (Protected Health Information).

	Y	N	NA	Recommended Solution(s)
ORAL COMMUNICATIONS				
Have you witnessed any of your staff discussing confidential Protected Health Information (PHI) among themselves in public areas? **If Yes, explain why it occurs and give recommended improvements/safeguards.**				
Are visitors, other staff or patients able to hear medical discussions? **If Yes, explain why it occurs and give recommended improvements/safeguards.**				
Have conversations with the patient and/or his/her family, which may include protected health information, been held in public areas? **If Yes, explain why it occurs and give recommended improvements/safeguards.**				
Can phone conversations, which may be relaying protected health information, be easily overheard in public areas? **If Yes, explain why it occurs and give recommended improvements/safeguards.**				
Is dictation completed in an area where protected health information can be overheard? **If Yes, explain why it occurs and give recommended improvements/safeguards.**				
Except for the patient's name, is protected health information ever called out into the waiting area(s)? **If Yes, explain why it occurs and give recommended improvements/safeguards.**				
When retrieving voice mail messages, is the answering machine volume turned down so messages being listened to cannot be overheard by others? **If No, explain why it occurs and give recommended improvements/safeguards.**				
Are voicemail passwords unique – not set to default settings or the last four digits of the phone number? **If No, explain why it occurs and give recommended improvements/safeguards.**				

PROTECTING CONFIDENTIALITY OF ELECTRONIC PHI				
Workstations	Y	N	NA	Recommended Solution(s)
Are workstation monitors in public areas positioned in a way to avoid observation by visitors? **If No, explain why it occurs and give recommended improvements/safeguards.**				
Are screens on unattended workstations returned to the logon screen or have a password-enabled screen saver? **If No, explain why it occurs and give recommended improvements/safeguards.**				
Are workstations turned off after business hours? **If No, explain why it occurs and give recommended improvements/safeguards.**				
Do staff protect their IDs and passwords and never share them? **If No, explain why it occurs and give recommended improvements/safeguards.**				
Do staff share workstations while logged in? **If Yes, explain why it occurs and give recommended improvements/safeguards.**				
Are passwords in plain sight or under mousepads? **If Yes, explain why it occurs and give recommended improvements/safeguards.**				
If asked, do staff refuse to give you their passwords or ID's? **If No, explain why it occurs and give recommended improvements/safeguards.**				
Do workforce members in your area store electronic reports, spreadsheets or databases containing protected health information on workstations? **If Yes, explain why it occurs and give recommended improvements/safeguards.**				
If applicable, are laptops and personal digital assistants (PDAs) stored in locked areas? **If No, explain why it occurs and give recommended improvements/safeguards.**				
Have you ever noticed anyone in your service area using personal computers not belonging or registered with the Philadelphia VA Medical Center? **If Yes, explain why it occurs and give recommended improvements/safeguards.**				
Does your service area frequently do inventory to ensure that all of the equipment can be accounted for? **If No, explain why it occurs and give recommended improvements/safeguards.**				

Electronic Mail	Y	N	NA	Recommended Solution(s)
Do workforce members in your service area use e-mail to transmit protected health information? **If Yes, explain why it occurs and give recommended improvements/safeguards.**				
Do workforce members in your area conduct business communications containing protected health information using an e-mail account not provided by the United States Department of Veterans Affairs (i.e. hotmail, yahoo or MSN)? **If Yes, explain why it occurs and give recommended improvements/safeguards.**				
Do business e-mails from your service area include a confidentiality notice? **If No, explain why it occurs and give recommended improvements/safeguards.**				
Fax Machines				
Is it common to find protected health information unattended on fax machines in your service area? **If Yes, explain why it occurs and give recommended improvements/safeguards.**				
Are fax machines in enclosed areas to which only authorized personnel have access? **If No, explain why it occurs and give recommended improvements/safeguards.**				
Are network printers in enclosed areas to which only authorized personnel have access? **If No, explain why it occurs and give recommended improvements/safeguards.**				
Do staff immediately retrieve papers that contain confidential information from printers and fax machines? **If No, explain why it occurs and give recommended improvements/safeguards.**				
Are faxes sent with cover sheets containing a confidentiality statement? **If No, explain why it occurs and give recommended improvements/safeguards.**				
For faxes containing protected health information, are the cover sheets saved or a log kept of who they're sent to and when? **If No, explain why it occurs and give recommended improvements/safeguards.**				
If your fax machine is in a public area, is it placed in a "sleep" mode during non-work hours? **If No, explain why it occurs and give recommended improvements/safeguards.**				

	Y	N	NA	Recommended Solution(s)
Do you routinely notify the intended recipient <u>before</u> sending confidential information? **If No, explain why it occurs and give recommended improvements/safeguards.**				
Do you confirm receipt of fax <u>after</u> transmission? **If No, explain why it occurs and give recommended improvements/safeguards.**				
Are copy machines in enclosed areas to which only authorized personnel have access? **If No, explain why it occurs and give recommended improvements/safeguards.**				
Do staff always remove originals and copies before leaving the copy machine? **If No, explain why it occurs and give recommended improvements/safeguards.**				
PROTECTING CONFIDENTIALITY OF PAPER PHI				
Are documents with protected health information placed face down or otherwise concealed to avoid casual observation in public areas, chart holders or at nurse's stations? **If No, explain why it occurs and give recommended improvements/safeguards.**				
Are paper records, reports and other types of paperwork containing protected health information distributed among staff in a concealed way to avoid casual observation by unauthorized personnel and/or visitors? **If No, explain why it occurs and give recommended improvements/safeguards.**				
Are documents with protected health information, that are being sent to another location, placed in a sealed envelope to avoid casual observation during delivery? **If No, explain why it occurs and give recommended improvements/safeguards.**				
Are paper records and medical charts stored or filed in such a way as to avoid observation by patients or visitors, or casual access by unauthorized staff? **If No, explain why it occurs and give recommended improvements/safeguards.**				
For units that are not staffed 24 hours, are patient records filed in locked storage cabinets or rooms that are locked? **If No, explain why it occurs and give recommended improvements/safeguards.**				

	Y	N	NA	Recommended Solution(s)
Do white boards include only non-confidential patient-specific information? **If No, explain why it occurs and give recommended improvements/safeguards.**				
Is there protected health information requested on sign-in sheets? **If Yes, explain why it occurs and give recommended improvements/safeguards.**				
Are patient lists and/or sign-in sheets, including scheduled procedures, with information beyond room assignments readily visible by patients or visitors? **If Yes, explain why it occurs and give recommended improvements/safeguards.**				
Are medical records or other protected health information removed from the facility for transport or any other purposes? **If so, under what circumstances? AND** **What precautions are taken to safeguard the information?**				
Disposal of Paper PHI				
Does your service area have a secured recycling bin (one with a locked top) to dispose of protected health information, if it is in a public area? **If No, explain why it occurs and give recommended improvements/safeguards. OR** **Go to the next question.**				
Does your area have a paper shredder to dispose of protected health information? **If No, explain why it occurs and give recommended improvements/safeguards.**				
Do staff, researchers and residents in your area remove/delete files, reports, databases or e-mails from their workstations with protected health information before transferring the workstation to another person for their use? **If No, explain why it occurs and give recommended improvements/safeguards.**				
Is shredding equipment located in an area that is secure from unauthorized personnel or visitors? **If No, explain why it occurs and give recommended improvements/safeguards.**				
Is confidential patient information discarded in regular wastebaskets? **If Yes, explain why it occurs and give recommended improvements/safeguards.**				
Are films and other images properly discarded in a confidential manner as to avoid the disclosure of protected health information? **If No, explain why it occurs and give recommended improvements/safeguards.**				

OTHER	Y	N	NA	Recommended Solution(s)
Are the doors in your service area locked during extended periods of time when all employees are absent (i.e. all staff meetings, after hours)? **If No, explain why it occurs and give recommended improvements/safeguards.**				
Are visitors and patients given detailed directions or escorted to ensure they do not access staff areas, dictating rooms, chart storage, etc.? **If No, explain why it occurs and give recommended improvements/safeguards.**				
Are those individuals not recognized in restricted areas challenged for identification? **If No, explain why it occurs and give recommended improvements/safeguards.**				
Do authorized staff who have access to protected health information use only the minimum amount necessary to accomplish their duties? **If No, explain why it occurs and give recommended improvements/safeguards.**				
Do any unauthorized personnel have keys and/or access to secured areas? **If Yes, explain why it occurs and give recommended improvements/safeguards.**				
Can you account for all keys and/or electronic access cards to secured areas? **If No, explain why it occurs and give recommended improvements/safeguards.**				
Does your service area have a detailed checklist of items to be returned or accesses removed upon an employee's termination (i.e. ID's to various computing systems, departmental keys, ID badges, computing equipment)? **If No, explain why and give recommended improvements/safeguards.**				

If you have any questions regarding the survey, feel free to contact the Philadelphia VA Medical Center Privacy Officer, Timothy H. Graham, directly at 215.823.6270.