

HIPAA Privacy & Security Compliance Rounds Checklist

The following elements are basic components for demonstrating compliance to HIPAA Privacy and Security Rules as well as organizational policies and procedures for safeguarding Protected Health Information.

Date:	Reviewer:	Location:	

Compliance Element	Yes	No	N/A	Comments	
General					
The Notice of Privacy Practices posted in public locations in					
the community.					
The Notice of Privacy Practices available on website.					
Compliance Hotline poster visible in public locations in					
community.					
There are no overhead paging/announcements of resident-					
specific health information.					
Telephone voice mail message volume is kept low/not					
audible to others.					
Phone conversations, speakerphone use, and dictation					
occur in areas where resident information is not overheard.					
Workstations and computer monitors are positioned in a					
manner that avoids access by public/others.					
Unattended computers are returned to the log-on screen					
(automatically or by user) or have password-enabled screen					
savers when not in use.					
Staff awareness of e-mail encryption.					
Staff are not posting or displaying computer log-ons or					
passwords in easily accessible areas.					
Staff are not observed sharing passwords.					
Staff are signing on/logging off computers correctly.					
Mailroom: no exposed PHI in open access mailboxes.					
Appropriate disposal processes for confidential information					
in place.					
PHI is shredded or discarded in secure container. There is					
no recycling of paper containing PHI (e.g., for notes,					
memos, etc.). Are documents stored in boxes under desks,					
on window sills or in other unlocked storage areas?					
Doors to non-public areas are kept closed.					
Health records are stored in a secure location.					
If using off-site facility for long-term storage of medical					
records, can manager retrieve any document from long-					
term storage within two working days?					
After-hours access by housekeeping/other staff is restricted					
and/or supervised.					
Resident Care Areas					
Staff discussions of residents are held in areas where					
conversation is not easily overheard.					
Conversations with resident/family & friends are held in					
areas where information is not easily overheard.					



HIPAA Privacy & Security Compliance Rounds Checklist

Compliance Element	Yes	No	N/A	Comments			
Steps are taken to ensure resident privacy when discussing							
care (semi-private room: curtains pulled, low voices used,							
etc.)							
Documents, charts, and other media containing resident							
health information are concealed from public access and							
view.							
Whiteboards contain minimum necessary resident							
information.							
Fax machines are located in secure areas out of public							
view/access. Any documents with PHI on faxes? Evidence of							
staff using cover sheets when transmitting faxes? Printers and copiers are located in secure areas out of							
public view/access. Any documents with PHI on the							
printers?							
Resident records that are being transported throughout the			1				
facility are not identifiable.							
Staff Conduct							
Staff members understand how to handle resident requests							
for access to health records.							
Staff members understand what resident information can							
be shared with family members and friends involved in the							
resident's care.							
Staff members understand the concept of minimum							
necessary/need-to-know access.							
Staff members can identify how and to whom privacy related complaints are to be made.							
Staff members are wearing ID badges.							
Staff know who to contact about a privacy complaint or							
breach of confidential information.							
IT/Data Storage							
IT equipment/hardware secured in locked/restricted area.							
Computer monitors are positioned in a manner that avoids							
access by public/others.							
Unattended computer screens are displaying logon screen							
or screen saver/no PHI.							
Use encryption for email and portable devices.							
			_				
Other Comments							