UHealth | MILLER SCHOOL OF MEDICINE

UNIVERSITY OF MIAMI HEALTH SYSTEM | UNIVERSITY OF MIAMI

UHealth HIPAA Self Assessment Checklist

Item #	*Item*	*Yes*	*No*	*Documentation/Observations*
1	Is the Notice of Privacy Practices (NPP) posted in the registration area?			
2	Does the site of service have a process for identifying and issuing patients who need to receive a Notice of Privacy Practices (NPP) and for collecting and documenting the patient's signed acknowledgement of receipt?			
3	Are documents containing PHI (e.g. appointment schedules, census lists, physician orders) visible to unauthorized individuals – including the public?			
4	Do sign-in sheets only contain minimum necessary information (i.e. no symptoms, chief complaint or diagnosis information)?			
5	Are patient charts & other sensitive information maintained/stored in a secure area?			
6	Can visitors in the waiting rooms overhear the registration process?			
7	Are visitors monitored or escorted through restricted areas?			
8	Are computer monitors and printers located in secure areas, and are they positioned so that visitors can't access or view the PHI on them?			
9	Computers left unattended are locked, password protected or logged off?			
10	Does the location have a whiteboard, patient tracker (electronic), or other posting mechanism that contains only the minimum amount of information necessary and is it located in a secure area (staff only or quasi-public area)?			
11	Are computer passwords kept confidential and not shared or posted (i.e. On a post-it note stuck on monitor)?			
12	Are materials removed from printers and fax machines in a timely manner?			
13	Is the HIPAA approved fax coversheet available and being used?			
14	Do staff members verify fax numbers prior to faxing information?			
15	Is there PHI discarded in the regular trash receptacle?			
16	Are recycle bins or other PHI disposal bins available and easily accessible by staff members?			
17	Are staff wearing name badges?			
18	Have all staff and faculty completed HIPAA training within the two year cycle?			
19	Are faculty/staff aware that they should only access PHI that they need to know to perform their work-related duties?			
20	Do faculty/staff know that they should not access the health information of their co-workers, supervisor, family or friends without a work related reason?			
21	Do faculty/staff know what to do when patients request their medical records?			
22	Do faculty/staff know what to do if patients request amendments to their medical records?			
23	Do faculty/staff know who the Chief Medical Compliance & HIPAA Privacy Officer and Chief Information & HIPAA Security Officer are?			
24	Do faculty/staff know where they should refer questions regarding patient privacy?			

UHealth UNIVERSITY OF MIAMI HEALTH SYSTEM | MILLER SCHOOL OF MEDICINE UNIVERSITY OF MIAMI

UHealth HIPAA Self Assessment Checklist Guidance

Item #	Item	Guidance	Review
1	Is the Notice of Privacy Practices (NPP) posted in the registration area?	***Notice should be conspicuously posted in registration areas.***	*Monthly*
2	Does the site of service have a process for identifying and issuing patients who need to receive a Notice of Privacy Practices (NPP) and for collecting and documenting the patient's signed acknowledgement of receipt?	***Observe staff.***	*Monthly*
3	Are documents containing PHI (e.g. appointment schedules, census lists, physician orders) visible to unauthorized individuals – including the public?	***Check work areas (registration desks, nurses' station) for PHI visible to unauthorized individuals. Use a "Confidential" cover page, place in drawers, or turn***	*Daily*
4	Do sign-in sheets only contain minimum necessary information (i.e. no symptoms, chief complaint or diagnosis information)?	***Sign-in sheets should not contain chief complaint, diagnosis or symptom information.***	*Daily*
5	Are patient charts & other sensitive information maintained/stored in a secure area?	***All charts should be maintained securely.***	*Daily*
6	Can visitors in the waiting rooms overhear the registration process?	***Observe dialogue/exchanges and identify need for staff to lower voices or move discussion to private area.***	*Monthly*
7	Are visitors monitored or escorted through restricted areas?	***Observe the area***	*Monthly*
8	Are computer monitors and printers located in secure areas, and are they positioned so that visitors can't access or view the PHI on them?	***Are they located in areas where visitors are left unattended? Are staff regularly present in those areas?***	*Monthly*
9	Computers left unattended are locked, password protected or logged off?	***Remind faculty/staff at meetings about risks.***	*Monthly*
10	Does the location have a whiteboard, patient tracker (electronic), or other posting mechanism that contains only the minimum amount of information necessary and is it located in a secure area (staff only or quasi-public area)?	***Review OR waiting rooms, ED triage areas, inpatient units.***	*Quarterly*
11	Are computer passwords kept confidential and not shared or posted (i.e. On a post-it note stuck on monitor)?	***Passwords should not be shared, posted, or written down where others may view/use.***	*Daily*
12	Are materials removed from printers and fax machines in a timely manner?	***Verify at the time of review. Is there a process where staff regularly removes output and distributes in a timely manner?***	*Daily*
13	Is the HIPAA approved fax coversheet available and being used?	***May be obtained from OHPS website*** ***Keep copies near fax machines.***	*Daily*
14	Do staff members verify fax numbers prior to faxing information?	***Remind faculty/staff about risks of sending PHI to the wrong destination & to verify fax numbers. Also, pre-programmed numbers should be checked monthly.***	*Monthly*
15	Is there PHI discarded in the regular trash receptacle?	***Check wastebaskets. PHI should be placed in locked confidential or shredding containers.***	*Daily*
16	Are recycle bins or other PHI disposal bins available and easily accessible by staff members?	***Contact Environmental Services at 305-243-1052 or via cell at 305-986-4996 to order containers or for a pick-up.***	*Daily*
17	Are staff wearing name badges?	***Walk around and assess.***	*Daily*
18	Have all staff and faculty completed HIPAA training within the two year cycle?	***Required to complete on a 2 year cycle; verify in ULearn system***	*Monthly*
19	Are faculty/staff aware that they should only access PHI that they need to know to perform their work-related duties?	***Emphasize during staff meetings.***	*Monthly*
20	Do faculty/staff know that they should not access the health information of their co-workers, supervisor, family or friends without a work related reason?	***Emphasize during staff meetings***	*Monthly*
21	Do faculty/staff know what to do when patients request their medical records?	***Direct patient to HIM Department to complete authorization form. Print out form from OHPS website.***	*Quarterly*
22	Do faculty/staff know what to do if patients request amendments to their medical records?	***Provide the patient with an Attachment 33 for completion. Completed form should be sent to OHPS.***	*Quarterly*
23	Do faculty/staff know who the Chief Medical Compliance Officer and Chief Information & HIPAA Security Officer are?	***Chief Medical Compliance & HIPAA Privacy Officer – Jennifer McCafferty, Chief Information & HIPAA Security Officer – Tim Ramsay***	*Quarterly*
24	Do faculty/staff know where they should refer questions regarding patient privacy?	***If cannot be answered by departmental supervisor, refer to OHPS 243-5000 or OHPS website***	*Quarterly*