Workforce Onboarding and Termination Checklist & Audit

This form is to be used each time an employee is hired or terminated.

It should be used to periodically audit the onboarding and termination process and to help with the management of workers' access to ePHI.

The following items will be completed/reviewed for a potential/new employee:

- ☐ Written application
- ☐ Confirm education and/or professional credentials, if required for role
- ☐ Review of prior employment history
- ☐ Citizenship or resident alien status
- ☐ Criminal record check, if required by law
- ☐ Financial record check, if required by law or appropriate for role
- ☐ Interview
- ☐ Reference Check
- ☐ Other (e.g., OIG exclusion list):_____

The following items will be completed when employment ends. If employee will be terminated, deactivate access prior to notification.

- ☐ Deactivate access to network and systems with ePHI
- ☐ Deactivate and remove info from BYOD and remote access (if applicable)
- ☐ Deactivate work email address
- ☐ Deactivate any access/alarm codes to the physical building or restricted areas
- ☐ Obtain any keys to physical building and/or restricted areas
- ☐ Obtain badges allowing entry to physical building and/or restricted areas
- ☐ Retrieve any company owned items
  - ☐ Laptop
  - ☐ Tablet
  - ☐ Smart phone
  - ☐ Credit card(s)

EMPLOYEE NAME: _____ **TASK**	**DATE OR N/A**	**MANAGER, SUPERVISOR OR DESIGNEE INITIALS**	**COMMENTS**
ACCESS AND EQUIPMENT			
A unique user-ID and password is assigned for network access			
Depending on job responsibilities, a unique user-ID and password is assigned to each program with ePHI (see *Access Needed by Function* in the *Security Plan*)			
Email address assigned and account activated (if separate from network access)			
Name badge provided			
Key/badge provided for building access			
Unique alarm code assigned			
Mobile equipment assigned (tablet, laptop, phone)			
Bring Your Own Device Policy signed			
Device security set up/verified by IT support			
Working From Home/Remote Access Policy reviewed/signed			
TRAINING			
Initial training provided – Access the TMC online training			
Specific items reviewed: ☐ Chain of command ☐ Name of Privacy/Security Officers ☐ Sanctions Policy ☐ Minimum necessary standard ☐ Reasonable safeguards ☐ Password requirements ☐ Changing passwords ☐ Sharing passwords ☐ Email communications ☐ Voicemail usage ☐ Internet access/Workstation Use ☐ Social media and PHI ☐ Reporting privacy or security issues			
Any role related specifics (e.g., records release, incident response)			
OTHER			