Workforce Onboarding and Termination Checklist & Audit

This form is for each new employee as well as to perform periodic audits of the office's onboarding and termination process.

To ensure PHI is protected at the highest level, this office will follow a consistent hiring, orientation and termination process.

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

- ☐ Written application
- ☐ Confirmation of educational history
- ☐ Review of prior employment history
- ☐ Skill set aligns with job requirements
- ☐ Verification of licensure/certification if needed for position
- ☐ Citizenship or resident alien status
- ☐ Criminal record check if required by law
- ☐ Financial record check if required by law
- ☐ Interview
- ☐ Reference Check
- ☐ Other:_____

The following items will be completed when an employee leaves the practice/business:

- ☐ Deactivate access to network and systems with ePHI
- ☐ 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)
  - ☐ Other: _____

Task	Date or N/A	Manager, Supervisor, or Designee Initials	Comment
Access and Equipment			
Unique user access assigned to the network assigned			
Depending on job responsibilities, unique user access assigned to each program with ePHI			
Email address assigned and account activated			
Name badge provided			
Key/badge provided for building access			
Unique code to deactivate alarm system assigned			
Mobile equipment assigned (tablet, laptop, phone)			
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 ☐ Set up of strong passwords ☐ Change of passwords ☐ Sharing of passwords ☐ Email communications ☐ Voice mail usage ☐ Internet access ☐ Social media and PHI ☐ Reporting privacy or security issues			
Any role related specifics (records release)			
Remote Access			
Review of policies for remote access			
For personal devices, security settings and malware protections appropriate			