



Building Security Reminders

Physical Security

Policies are in place prescribing the physical safety and security of devices.

All workforce members understand and agree to abide by physical access policies and procedures.

Is key and door card access frequently audited?

All devices containing Protected Health Information (PHI) are inventoried and can be accounted for.

Computers are protected from environmental hazards.

Physical access to secure areas is limited to authorized individuals.

Computers running Electronic Health Records (EHR) systems are shielded from unauthorized viewing.

Equipment located in high-traffic or less secure areas are physically secured.

Are entrances and exits that lead to locations with ePHI secured?

Do you know who is responsible for inventory management and its maintenance?

Do you manage access to and use of your facility or facilities that house information systems and ePHI?

Do you have physical protections in place to manage facility security risks?

Is physical access restricted to any equipment that has ePHI?

Do you validate a person's access to facilities (including workforce members and visitors) based on their role or function?

Do you maintain records of physical changes, upgrades, and modifications to your facility?

Does your practice have a contingency plan in the event of an emergency?

IT Security

Does each workforce member have a unique user identifier?

Are common sense precautions taken, such as using a unique password, not writing passwords down and leaving them in areas that are visible or accessible to others?

Is the automatic lock or log-off feature activated on all workstations with access to ePHI?

During the on-boarding process are detailed job descriptions used to determine ePHI levels of access?

During the off-boarding process is access removed when a workforce member leaves?

Is PHI access frequently audited?

Shredding

Are records containing PHI that are scheduled for destruction or disposal secured against unauthorized access until such destruction or disposal is complete?

Do you keep a destruction log with all the required information and signatures?

If using an outside vendor to destroy or dispose of records, do you have a business associate agreement with the required information?

Is PHI destroyed or disposed of using the acceptable methods of destruction or disposal?