Health Information Compliance Alert

Security Tool: Use This Checklist On Your Next Walkthrough

Are you overlooking these crucial security breaches?

Conduct a walkthrough to quickly and easily monitor your staff's HIPAA compliance.

This checklist, created by **Patricia Johnston**, a consultant with **Texas Health Resources** in Arlington, can help you catch violations and track problem areas.

For each item listed, check if observed or not, the number of occurrences, and add any comments.

Activity:

--Staff discusses confidential information in public areas.

--Conversations with patient/family regarding confidential information are held in public areas.

--Overhead and intercom announcements include confidential information.

--Phone conversations and dictation are in areas where confidential information can be overheard.

--Visitors in public areas can see computer monitors.

--Unattended computers are not logged out or protected with password-enabled screen savers.

--Computer passwords are shared or posted for unauthorized access.

--Documents, films and other media with confidential patient information are not concealed from public view.

--Whiteboards in public areas have more than the allowable information.

--Medical records are not stored or filed in such a way as to avoid observation by passersby.

--Confidential patient information is called out in the waiting room.

--Confidential information is left on an unattended fax machine in unsecured areas.

--Confidential information is left on an unattended printer in unsecured areas.

--Confidential information is left on an unattended copier in unsecured areas.

--Confidential information is found in trash, recycle bins or unsecured pre-shredding receptacles.

--Patient lists, such as scheduled procedures, are readily visible by patients or visitors.

--Contractors, vendors and other non-patient visitor third parties are not appropriately identified. Staff are not wearing name badges.

--Patient records not filed in locking storage cabinets or rooms that are locked when unattended.

--Security access mechanisms for buildings or departments are bypassed.

--When questioned, staff demonstrate lack of privacy awareness.