



HIPAA Compliance Checklist for Office Staff

This is an extra resource to go along with the original article:
[Is your office staff accidentally oversharing patient information?](#)

Make sure that office staff can check off these HIPAA compliance boxes if you want to avoid any violations around the office.

Front Desk

- Office staff uses electronic records for notes and other patient information
- Office staff utilizes online intake forms to minimize patient sharing on check-in
- Office staff protects patient information by speaking softly and, when appropriate, using non-public areas
- Office staff knows not to discuss personal patient stories or other information in front of other patients (and use break rooms or private rooms when necessary)
- Office staff does not post patient information to social media – practice or personal – without authorization

Workstation Use

- Workstations and computer monitors are positioned to prevent someone seeing the information
- Only authorized individuals can login or access personal patient information
- Office staff utilizes protected user IDs and passwords and don't share them
- Office staff doesn't share workstations while logged in
- User IDs and passwords are not posted on or near workstations
- Computer monitors are turned off when not in use and otherwise faced away from public areas or commonly used patient areas
- All computers are shut down after hours
- Laptops, PDAs and other portable equipment are physically secured
- Printers, photocopiers, or fax machines are always attended by office staff

Training

- Every staff member is provided annual HIPAA training and given a Notice of Privacy Practices
- A Notice of Privacy Practices is available to all patients
- Privacy information is documented and office staff has signed and affirmed they understand the repercussions of a violation
- Management, doctors and nurses have reviewed HIPAA policies and understand what constitutes a violation

IntakeQ

- New employees are given HIPAA training mat