HIPAA Best Practices for Medical Practices

Notice of Privacy Practices	Every patient must be offered a copy of the entity's *Notice of Privacy Practices*. Best practice: Have a *Notice of Privacy Practices*; have the patient sign a form acknowledging that they were offered a copy, regardless if they chose to take and review it.
Posted Notice of Privacy Practices	The Office for Civil Rights requires that the Notice of Privacy Practices be posted in multiple locations where patients can find it, including the entity's website; in any waiting area; and printed copies available. Best practice: Have the notice posted on the website, in the waiting area, mailed to new patients, and available as a handout in the waiting area.
Privacy Policy	Every business that manages protected health information (PHI) should have a policy for their employees regarding permitted uses of PHI in the business, methods that secure PHI, and consequences for violations of the policy. Best practice: Have staff sign an acknowledgement that they have read and understand the business' Privacy Policy and what it requires of them.
Security Program	Entities must conduct a security assessment of their information systems that contain protected health information, identifying risks to the security of protected health information. Risks identified should be documented, along with the actions taken to mitigate the risk, or reasoning as to why the risk is not being addressed. Best practice: Conduct a risk assessment and categorize risks by the likelihood of occurrence; assure that prominent risks are being mitigated promptly.
Physical Security Practices	Entities can protect the security of PHI to assure its privacy by reviewing physical security of their facility. Any record storage area should be secured and out of access from the public. Best practice: Store records in locked offices; assure that PHI is not left in an exam room after a patient leaves; Transport printed PHI in locked briefcases; do not store PHI at home; lock workstations when stepping away from the computer record system.
Electronic Security Practices	Entities are expected to take 'reasonable' steps to maintain the security of electronic PHI, including encryption of PHI. Best practice: Do not allow users to share passwords; assign individual user accounts for access to medical records; send PHI electronically through encrypted communication channels; do not text PHI; evaluate the security settings of other applications to ensure that PHI is secured. Lesson: a practice in Arizona used a Google calendar to schedule patient appointments; this calendar was not set to private, and thus visible to other Google users. This resulted in a $100,000+ fine to the practice.