

CHECKLIST 1: Mitigating Medical Practice and Office HIPAA Risks	YES	NO
Is my medical office, practice, clinic or healthcare organization a HIPAA-covered entity by virtue of being a medical office, clinic, outpatient care center or hospital?	<input type="radio"/>	<input type="radio"/>
Is my medical office, practice or healthcare organization a HIPAA-covered entity by virtue of being a nursing-home, extended care facility or Skilled Nursing Facility?	<input type="radio"/>	<input type="radio"/>
Is my office or healthcare organization a HIPAA-covered entity by virtue of being an insurance company, health maintenance organization (HMO), managed care organization (MCO), independent physician association (IPA), physician-hospital organization (PHO) or similar intermediary or third-party payor?	<input type="radio"/>	<input type="radio"/>
Is the system in my healthcare entity Protected Health Informatics (PHI) compatible?	<input type="radio"/>	<input type="radio"/>
Am I aware what is the permitted use and disclosure for PHI in my healthcare entity?	<input type="radio"/>	<input type="radio"/>
Is the PHI system public key informatics protected?	<input type="radio"/>	<input type="radio"/>
Is the PHI system private key informatics protected?	<input type="radio"/>	<input type="radio"/>
Do I know when systems entry authorization is needed?	<input type="radio"/>	<input type="radio"/>
Do I have a designated Privacy Officer who routinely audits HIPAA compliance?	<input type="radio"/>	<input type="radio"/>
Does the hospital have a detailed work and project plan to review action items?	<input type="radio"/>	<input type="radio"/>
Is there an assigned committee to address HIPAA-related issues?	<input type="radio"/>	<input type="radio"/>
Are regular meetings scheduled to discuss HIPAA-related issues, status, and/or resolutions?	<input type="radio"/>	<input type="radio"/>
Is there a contingency data backup plan, a disaster plan, or an emergency operation plan?	<input type="radio"/>	<input type="radio"/>
Has the backup plan or disaster plan been tested?	<input type="radio"/>	<input type="radio"/>
Is there a specific individual or organization assigned to oversee responsibility for security?	<input type="radio"/>	<input type="radio"/>
Does the hospital have a security configuration management plan?	<input type="radio"/>	<input type="radio"/>
Is there a security incident procedure and management plan?	<input type="radio"/>	<input type="radio"/>
Does the hospital utilize pre-programmed internal audits in their system to monitor security?	<input type="radio"/>	<input type="radio"/>
Is there a defined process to assure integrity for personnel security?	<input type="radio"/>	<input type="radio"/>
Is staff cleared for access on a need-to-know basis?	<input type="radio"/>	<input type="radio"/>
Do job descriptions define specific access needs?	<input type="radio"/>	<input type="radio"/>
Does the hospital routinely monitor each individual's access and compare it to the job description?	<input type="radio"/>	<input type="radio"/>
Does the hospital have a mandatory training program for all personnel including management?	<input type="radio"/>	<input type="radio"/>
Does the hospital provide information or training to staff on handling virus protection?	<input type="radio"/>	<input type="radio"/>

Are all virus protection software programs installed and routinely updated?	<input type="radio"/>	<input type="radio"/>
Is there a process for equipment control?	<input type="radio"/>	<input type="radio"/>
Is there a process for maintaining records?	<input type="radio"/>	<input type="radio"/>
Is there a process for visitor sign-in or escort?	<input type="radio"/>	<input type="radio"/>
Is there a process for testing and revision?	<input type="radio"/>	<input type="radio"/>
Is there a policy or guideline on proper work-station usage?	<input type="radio"/>	<input type="radio"/>
Are the work-stations monitors, and/or thin-clients secure?	<input type="radio"/>	<input type="radio"/>
Is there a technical security service?	<input type="radio"/>	<input type="radio"/>
Is there an audit control of system activity to identify potential suspected data access?	<input type="radio"/>	<input type="radio"/>
Is there an entity authentication process, such as user identification, PIN number, password or callback verification?	<input type="radio"/>	<input type="radio"/>
Is there a standard for electronic signature that is HIPAA compliant?	<input type="radio"/>	<input type="radio"/>
Does the hospital have a liability protection plan?	<input type="radio"/>	<input type="radio"/>
Can files be transferred via the Internet in a secure manner?	<input type="radio"/>	<input type="radio"/>
Is a protection process in place with wireless products to assure confidentiality and privacy?	<input type="radio"/>	<input type="radio"/>
Does the staff discuss protected health information with the patient within earshot of other patients, such as on the phone, in a reception area, or at the registration desk?	<input type="radio"/>	<input type="radio"/>
Has the staff left sensitive patient information on the answering machine?	<input type="radio"/>	<input type="radio"/>
Were faxes that included medical record data being forwarded to the correct recipient?	<input type="radio"/>	<input type="radio"/>
Does the staff make announcements in the waiting room that potentially include protected health information?	<input type="radio"/>	<input type="radio"/>
Is patient information being listed on whiteboards, x-ray boxes, computer screens or other areas that would have been visible to the public or others who don't need access to that information?	<input type="radio"/>	<input type="radio"/>
Are computer screens visible to the patient and are security measures in place to restrict access if the user walked away from the computer?	<input type="radio"/>	<input type="radio"/>
Is physical access to areas where medical records are kept restricted?	<input type="radio"/>	<input type="radio"/>
Is there a termination procedure and process to ensure individuals are removed from the access list, shared passwords, or user accounts?	<input type="radio"/>	<input type="radio"/>
Is there a process where all computers, laptops, or building cards are returned by a terminating employee?	<input type="radio"/>	<input type="radio"/>
Is there a procedure in place to ensure this process will be accomplished in a consistent manner?	<input type="radio"/>	<input type="radio"/>
Are new employees trained on HIPAA as part of their orientation?	<input type="radio"/>	<input type="radio"/>
Is a process in place for identifying the "correct" patient?	<input type="radio"/>	<input type="radio"/>

Do the patients ever carry their medical record from one location to another in the hospital?	<input type="radio"/>	<input type="radio"/>
Is it possible for a single person to breach security?	<input type="radio"/>	<input type="radio"/>
Are there internal security assessments on all networking devices?	<input type="radio"/>	<input type="radio"/>
Are there external security assessments on public facing systems?	<input type="radio"/>	<input type="radio"/>
Are all devices encrypted or do they have firewalls?	<input type="radio"/>	<input type="radio"/>
Is there "help desk" support for HIPAA?	<input type="radio"/>	<input type="radio"/>
Does anyone else, within the hospital, have access to and use of any employee's computer?	<input type="radio"/>	<input type="radio"/>
Can employees load personal CDs/DVDs onto their laptops?	<input type="radio"/>	<input type="radio"/>
Is there a system for monitoring private use of laptops?	<input type="radio"/>	<input type="radio"/>
Is a checklist for HIPAA included in the hospital's policies and procedures?	<input type="radio"/>	<input type="radio"/>
Does the computer system automatically log off if the desktop is unoccupied?	<input type="radio"/>	<input type="radio"/>
Do employees have a log off process when leaving their desktop?	<input type="radio"/>	<input type="radio"/>