

# HIPAA Compliance Check List

For Healthcare Information Management Service Providers

## Administrative Procedures to Guard Data Integrity, Confidentiality, and Availability

- Is your system regularly monitored and subject to internal audits?
- Are all access to your system tracked automatically?
- Does your system have built-in security procedures and measures to ensure the technical security of information?
- What level of industry certification to your systems experts maintain?
- Does your system have a contingency plan (e.g. a detailed backup plan) in effect to respond to system emergencies?
- What level of training do staff and business partners receive on security processes and procedures?
- What procedures or policies are in place for closing system access to terminated employees and customers no longer under contract?
- What monitoring is done of your system to prevent, detect, contain, and correct security breaches?
- What tests or audits do business partners who have access to medical records have to pass?
- Do you have documented policies and procedures for the manipulation, storage, dissemination, transmission, and disposal of health information?
- What procedures and policies exist for granting different levels of access to healthcare information for employees and customers?
- What measures are in place to ensure personnel security?

## Physical Safeguards to Guard Data Integrity, Confidentiality, and Availability

- Who is responsible within your organization for administering healthcare information security procedures?
- What procedures are in place to manage the receipt and removal of media within various center of operation?
- What controls are in place to prevent the unauthorized physical access to information?

## Technical Security Services to Guard Data Integrity, Confidentiality, and Availability

- How is access to data resources restricted?
- How is system activity monitored and recorded?
- How is authorization and access to data controlled?
- How is data authenticated?
- How is each system user authenticated?

## Technical Security Mechanisms to Guard Against Unauthorized Access to Data that is Transmitted over a Communications Network

- How are transactions encrypted?
- How are transactions tracked and audited?

Electronic Signatures

- Are electronic signatures used to authenticate each user's transactions?

Privacy Compliance Requirements

- What procedures are in place to determine access rights and privileges?
- What level of patient access to protected healthcare information (PHI) exists?
- Does the system provide for patients to submit amendments to their PHI?
- What policies exist to handle the destruction and/or de-identification of PHI when a customer contract terminates?
- How are disclosures of all PHI tracked and reported?
- What kind of data is used in the training of employees and business partners?
- How are third-party consents and authorizations obtained with this system?
- How are users notified of and updated on privacy practices?
- How is data privacy ensured?
- How are administrative requirements and updates managed or monitored?