

FREE CHECKLIST FOR KANSAS CITY PRACTICES

The HIPAA IT Checklist

32 technical safeguards every medical, dental, and behavioral health practice should be able to check off before its next risk assessment. Written for practice owners and office managers, not IT people.

How to use this

Work through each section with whoever handles your IT. Every unchecked box is either a finding waiting to happen in a risk assessment or a gap an attacker can use. Most practices find 6 to 12 gaps on the first pass.

Access control

Who can get to patient information, and how you know it was really them.

☐ **Every staff member has their own login**

No shared front desk accounts, no shared EHR logins. HIPAA requires unique user identification, and shared accounts make audit logs meaningless.

☐ **Multi-factor authentication is on for email**

Email is where most breaches start. MFA on Microsoft 365 or Google Workspace closes the single biggest hole.

☐ **Multi-factor authentication is on for the EHR and remote access**

If staff can reach patient data from home, that path needs the same protection as email.

☐ **Accounts are removed the day someone leaves**

A written offboarding step, not a reminder. Former employees with working logins are a common audit finding.

☐ **Staff only see what their role needs**

Billing does not need clinical notes. Front desk does not need admin rights. Minimum necessary access is a HIPAA requirement.

☐ **Workstations lock automatically**

Screens lock after 5 to 10 minutes of inactivity, and faster in patient-facing areas.

☐ **Nobody uses an administrator account for daily work**

Admin rights are reserved for IT tasks. Malware that lands on an admin account owns the whole machine.

☐ **Passwords are long, unique, and stored in a password manager**

A practice-wide password manager is cheaper than one incident and ends the sticky note problem.

Why it matters: Access control is the first thing an OCR investigator looks at after a breach. The questions are simple: who could reach this data, and can you prove it?

Devices and data protection

What happens to patient information if a laptop walks out the door.

☐ **Every laptop and desktop is encrypted**

BitLocker on Windows, FileVault on Mac, and you can prove it was on. A lost encrypted laptop is usually not a reportable breach. A lost unencrypted one is.

☐ **Phones and tablets that touch practice email are managed**

A PIN, encryption, and the ability to wipe the device remotely if it is lost.

☐ **Endpoint protection is installed and monitored on every machine**

Modern endpoint detection, not just consumer antivirus, and someone actually looks at the alerts.

☐ **Operating systems and software are patched within 30 days**

Windows, browsers, the EHR client, and imaging software. Unpatched systems are the most common way ransomware gets in.

☐ **Old equipment is wiped before disposal**

Computers, copiers, and imaging devices store patient data. Keep a disposal log with serial numbers.

☐ **Patient data is not stored on personal devices or personal cloud accounts**

No patient spreadsheets in personal Dropbox, no texting photos from a personal phone.

☐ **Email containing PHI is encrypted**

Microsoft 365 and Google Workspace can encrypt automatically when a message contains patient information. Turn it on.

☐ **Faxing and patient messaging go through a HIPAA compliant service with a BAA**

Consumer fax apps and standard texting do not qualify.

Quick test: Pick one laptop at random and ask IT to show you the encryption status screen. If they cannot show it in five minutes, assume it is off.

Backups, network, and vendors

Can you recover, and who else holds your data.

☐ **Backups run daily and a test restore has been done in the last 90 days**

A backup nobody has restored from is a hope, not a backup. Write down how long the restore took.

☐ **One backup copy is offsite or cloud based and cannot be deleted by ransomware**

Immutable or offline copies are what let a practice say no to a ransom demand.

☐ **Microsoft 365 or Google Workspace is backed up separately**

Microsoft and Google do not back up your mailboxes and files for you in a way that survives deletion or ransomware.

☐ **Guest Wi-Fi is separate from the practice network**

Patients in the waiting room should never share a network with the EHR server or imaging equipment.

☐ **A business-grade firewall is in place and updated**

The modem the internet provider gave you is not a firewall.

☐ **Remote access uses a VPN or a managed remote tool, not an open port**

Remote desktop exposed to the internet is the number one ransomware entry point for small practices.

☐ **Every vendor that touches PHI has a signed Business Associate Agreement**

EHR, billing, IT provider, cloud storage, fax, transcription, shredding, and the answering service. Keep the signed copies in one folder.

☐ **Your IT provider will sign a BAA and can describe their own security controls**

If they hesitate on either, that is your answer.

Common gap: Practices often have a BAA with the EHR vendor and nobody else. The list of business associates is usually two to three times longer than the office manager expects.

Monitoring, training, and documentation

What an auditor asks for, and what you need the day something goes wrong.

☐ **A written security risk assessment exists and is less than a year old**

Required by the Security Rule and the first document OCR requests.

☐ **Audit logs are on for the EHR and email**

You can see who opened which record and when.

☐ **Someone reviews security alerts and logs**

Alerts that go to an inbox nobody checks do not count.

☐ **Staff complete security awareness training yearly, with a record kept**

Phishing recognition is the most valuable hour of training a practice can buy.

☐ **A written incident response plan names who to call**

IT provider, attorney, cyber insurer, and the decision maker, with phone numbers.

☐ **Cyber insurance is in place and its security requirements are met**

Many policies now require MFA and backups. An unmet requirement can void a claim.

☐ **There is a current inventory of every device, account, and vendor**

You cannot protect what you have not listed.

☐ **Policies and procedures are written down and reviewed yearly**

Access, device use, incident response, and sanctions.

0 to 4 unchecked

You are in good shape. Keep the risk assessment current.

5 to 12 unchecked

Typical for a practice without dedicated IT. Fix MFA, encryption, and backups first.

13 or more

You are carrying real breach risk. Start with a professional risk assessment.

Want a second set of eyes?

Inovura runs a free IT assessment for Kansas City practices. We go through this list with you, verify what is actually in place, and give you a written gap report mapped to the HIPAA Security Rule.

inovurallc.com/healthcare-it-support-kansas-city

Inovura LLC, Olathe, Kansas. (913) 302-4578. rithik@inovurallc.com

This checklist covers common technical safeguards and is not legal advice or a substitute for a formal risk assessment. Requirements depend on your practice and state law.