



HEALTHCARE IT & CYBERSECURITY CHECKLIST

How Confident Are You That Your Practice Is Protected and Prepared?

A practical checklist for healthcare leaders to identify potential gaps in cybersecurity, backups, clinical applications, and IT accountability.



REDUCE
RISK



IMPROVE
RELIABILITY



SUPPORT
YOUR TEAM



PROTECT
PATIENT TRUST



KEEP CARE
MOVING

Healthcare IT and Cybersecurity Checklist

How confident are you that your practice is protected and prepared?

Your practice depends on technology to support patient care, scheduling, billing, and communication. Use this checklist to identify potential gaps, reduce disruptions, and discuss priorities with your IT team or technology provider.

How to use this checklist

Check Yes, No, or Not Sure for each question. Pay particular attention to every question where your answer is No or Not Sure.

Practice: _____

Completed by: _____

1. Cybersecurity

Checklist question	YES	NO	NOT SURE
Do we use multi-factor authentication for email, remote access, and supported clinical systems?	☐	☐	☐
Are computers, servers, and clinical systems regularly updated in coordination with vendors?	☐	☐	☐
Are our systems actively monitored for potential security threats?	☐	☐	☐
Do staff receive ongoing training on phishing and protecting patient information?	☐	☐	☐
Do we have appropriate email security and spam/phishing protection?	☐	☐	☐
Are administrator privileges restricted and controlled?	☐	☐	☐
When staff or contractors leave, is their access promptly removed?	☐	☐	☐
Do staff know how to report a suspected incident and who will lead the response?	☐	☐	☐

2. Backup and Disaster Recovery

Checklist question	YES	NO	NOT SURE
Are critical practice systems and patient information backed up automatically?	☐	☐	☐
Are backups protected from threats that could affect our primary systems?	☐	☐	☐
Are backups regularly tested to confirm information can actually be restored?	☐	☐	☐
Do we know how long restoring critical systems would take?	☐	☐	☐
Have we prioritized the systems needed to resume patient care?	☐	☐	☐
Do we have a documented recovery plan with clear responsibilities?	☐	☐	☐

3. Critical Healthcare Applications

Consider your electronic health record (EHR), practice management, scheduling, billing, e-prescribing, patient portal, imaging, and lab systems—including services hosted by outside vendors.

Checklist question	YES	NO	NOT SURE
Have we identified the applications essential to patient care and daily operations?	☐	☐	☐
Do we know which networks, devices, and outside services these applications depend on?	☐	☐	☐
Are those underlying systems monitored and maintained?	☐	☐	☐
Do we have current support contacts for our EHR and other application vendors?	☐	☐	☐
Is responsibility clear when an issue involves both a software vendor and our IT provider?	☐	☐	☐
Do staff know how to continue care and reconcile records during and after an outage?	☐	☐	☐

4. Email and Patient Information Access

Checklist question	YES	NO	NOT SURE
Is multi-factor authentication enabled for email and other supported accounts?	☐	☐	☐
Are suspicious sign-ins and inappropriate access investigated?	☐	☐	☐
Does each staff member have an individual account with access suited to their role?	☐	☐	☐
Are permissions reviewed when roles change and access removed when staff leave?	☐	☐	☐
Do staff use approved methods to share patient information securely?	☐	☐	☐

5. Infrastructure and Reliability

Checklist question	YES	NO	NOT SURE
Do we maintain an inventory of computers, network equipment, and connected clinical devices?	☐	☐	☐
Do we know which systems are unsupported or approaching end-of-life?	☐	☐	☐
Are servers, networks, and connections between practice locations proactively monitored?	☐	☐	☐
Do we have a replacement plan and budget for aging technology?	☐	☐	☐
Do we have a plan for internet or power failures that could interrupt patient care?	☐	☐	☐
Are recurring IT problems addressed at their source rather than repeatedly patched?	☐	☐	☐

6. IT Support and Accountability

Checklist question	YES	NO	NOT SURE
Do staff know exactly who to contact when they need IT help?	☐	☐	☐
Are response expectations clear for urgent issues that interrupt patient care?	☐	☐	☐
Are important issues followed through until they are resolved?	☐	☐	☐
Does our provider explain problems and recommendations in plain English?	☐	☐	☐
Does our IT provider identify risks before they cause avoidable disruption?	☐	☐	☐
When multiple vendors are involved, does one person coordinate the resolution?	☐	☐	☐
Do we receive useful updates on the condition of our technology and open risks?	☐	☐	☐

7. IT Resources and Compliance Readiness

Checklist question	YES	NO	NOT SURE
Is there a clear owner for IT coordination and patient information security?	☐	☐	☐
Do we have reliable support coverage when our primary IT contact is unavailable?	☐	☐	☐
Are system details and vendor responsibilities documented and accessible?	☐	☐	☐
Have we reviewed risks to patient information and assigned follow-up actions?	☐	☐	☐
Are security policies, staff training, and relevant vendor agreements reviewed regularly?	☐	☐	☐

8. Technology Planning

Checklist question	YES	NO	NOT SURE
Do we have a documented technology plan for the next 12–36 months?	☐	☐	☐
Do leadership and IT agree on priorities for patient care and practice operations?	☐	☐	☐
Are security and compliance-readiness gaps prioritized with owners and target dates?	☐	☐	☐
Can leadership understand why major technology investments are recommended?	☐	☐	☐
Are budgets and technology plans aligned with staffing, new locations, and growth?	☐	☐	☐

How Did Your Practice Do

- **Mostly Yes:** You appear to have many important processes in place. Your next step is verifying that they are documented, tested, and consistently followed.
- **Several No Answers:** You have identified areas that deserve a closer look and should be prioritized with your IT team or provider.
- **Several Not Sure Answers:** You should be able to get clear answers about whether your practice is protected and prepared. Ask your IT team or provider to explain what is in place, who owns it, and how it is verified.

Three Questions for Leadership

1. If we experienced a serious cyberattack tomorrow, how confident are we that we could recover?
2. Which technology failure would most disrupt patient care, and what is our plan if it happens?
3. Who is ultimately accountable for making sure our technology risks are identified and addressed?

You Do Not Have to Become an IT Expert

Healthcare leaders should not have to carry technology and cybersecurity risks alone. At EK Computer, we understand the pressure to keep providers productive, support staff, and protect patient trust. We help practices reduce disruptions, strengthen security, and gain confidence through proactive management and clear recommendations in plain English.

1

Schedule a Discovery Call

2

Review risks and opportunities

3

Implement a proactive IT and security strategy

Know Where You Stand

Gain a clearer picture of the technology risks that could disrupt your practice or put patient trust at risk.

Schedule a Discovery Call with EK Computer to discuss your practice, current challenges, and goals. Together, we can identify next steps toward more reliable technology and stronger security.

SCHEDULE A DISCOVERY CALL • WWW.EKCOMP.COM

This checklist supports an initial discussion. It is not a security risk analysis, compliance assessment, or certification.