WRIGHTBRAINED
SECURITY

FREE CHECKLIST · HEALTHCARE

10 Questions to Ask About Ransomware

For owners, CEOs and boards of any organization that handles patient data: hospitals, clinics, therapy practices, billing companies and health tech. What to ask, and what a good answer sounds like.

Why these questions

Ransomware crews don't pick targets by industry. They pick whoever left the door open, and organizations that handle patient data pay more and pay faster. You don't need to be technical to ask these. You need to listen for a specific answer.

> Ask your IT lead, your managed IT provider, or both. "It's handled" is not an answer. A number, a name, a date or a report is.

01 If our systems were locked tomorrow, how long until we could see patients and bill again?

A good answer: A number in hours or days, based on a restore someone actually tested.

A worrying answer: "We have backups." Backups aren't a plan until someone has restored from them.

02 Could a stolen staff password delete or encrypt our backups?

A good answer: No. At least one backup copy is kept offline or locked, with separate logins.

A worrying answer: Backups live on the same network, with the same admin passwords.

03 Does everyone need a second step, like a phone prompt, to get into email and remote access?

A good answer: Yes, for everyone, with no exceptions for executives or vendors.

A worrying answer: "Most people." Attackers only need the one account that was skipped.

04 Who is watching for an attack at 2 a.m. on a Saturday?

A good answer: A named team or service (a SOC or managed security provider) that can act, not just send an email.

A worrying answer: Alerts go to an inbox someone checks on Monday.

05 Which vendors can reach our systems or hold our patient data, and how do we know they are protected?

A good answer: A current list, with the critical ones asked about MFA, monitoring and backups.

A worrying answer: "Our IT company handles that." No one has the list.

06 How quickly do critical security updates get installed?

A good answer: A target, like two weeks, and a monthly report that shows it being met.

A worrying answer: "When we get to it," or no one knows.

07 Do everyday staff have administrator rights on their computers?

A good answer: No. Admin rights are limited to a few IT accounts that are not used for email or browsing.

A worrying answer: Most people are admins "because it was easier."

08 If we were hit, who do we call first, and is that written down somewhere we can reach without our network?

A good answer: A one-page playbook, printed and saved offline, with IT, the insurance carrier, legal counsel and a forensics firm.

A worrying answer: The plan is in a shared drive that would be encrypted too.

09 When did we last do a security risk assessment, and what did we fix because of it?

A good answer: Within the last year, with a short action list that has owners and dates. (HIPAA requires one.)

A worrying answer: It was done years ago, or it is sitting on a shelf.

10 What does our cyber insurance actually require of us, and are we meeting it?

A good answer: Someone has read the application answers and can show the controls are really in place.

A worrying answer: The application was filled out optimistically. Claims can be denied over that.

What to do with the answers

MOSTLY GOOD
Ask for the evidence behind two or three answers. Then schedule a restore test and a tabletop exercise this year.

SOME WORRYING
Turn each worrying answer into a task with an owner and a date. Start with backups, MFA and after-hours monitoring.

LOTS OF "I DON'T KNOW"
That's the most common result, and the easiest to fix. An independent security assessment will get you real answers fast.

Try the free 5-minute ransomware readiness check at wrightbrainedsecurity.com/tools/ransomware-check