The Cyber Playbook for HealthTech Companies

Top 10 Red Flags in a HealthTech Company's Security Posture

Healthtech companies face unique risks — **995 healthcare records are breached daily by cyberattackers, resulting in a loss of over $19M* to healthtech and healthcare providers.** 58% of the ~ 77.3 million individuals affected by healthcare data breaches were breached due to attacks on healthcare's third-party providers. Additionally, **by law, all breached healthtech companies must notify the U.S. Department of Health and be featured on the public healthcare cybersecurity fails list**.

This playbook highlights the most common healthtech security red flags, the risks behind them, why they matter to patient data and compliance, and the kinds of questions executives should ask their teams.

#	Red Flag	Risk	Why It Matters	Insurance Impact	Exec Questions for Tech Teams
1	Unencrypted or Misconfigured Cloud Storage	Exposed PHI via S3 buckets, Blob storage, etc.	Data exposure violates HIPAA, can trigger fines and reputational harm.	High severity claims, regulatory fines, possible denial if encryption not enforced.	Do we encrypt all patient data at rest and in transit? Do we routinely scan for misconfigured buckets or public endpoints?

2	Weak Identity & Access Controls	Excessive permissions, shared accounts, or no MFA make it easy for attackers or insiders.	Leads directly to breaches of PHI.	Coverage may be denied if MFA not in place; major driver of breach claims.	Is MFA enforced everywhere, including admin and vendor access? How often do we audit access to patient data systems?
3	Unpatched / Legacy Systems	Outdated EMR/EHR software, medical devices, or third-party components exploited.	Patient safety and PHI integrity can be impacted. HIPAA requires addressing known vulnerabilities.	Insurers expect patch SLAs; claims increase if legacy systems exploited.	What’s our patching SLA for critical vulnerabilities? How do we monitor devices and apps for end-of-life status?
4	Unsecured APIs and Mobile Apps	Poorly secured FHIR/HL7 APIs, missing authentication, or vulnerable mobile apps.	API breaches expose entire patient records, impacting HIPAA and potentially FDA-regulated apps.	Claims from mass PHI exposure; insurers ask about API security testing.	Do we penetration-test APIs and mobile apps? Are all API calls authenticated, authorized, and logged?

5	Shadow IT & Unapproved SaaS	Teams storing PHI in unvetted apps (Dropbox, Google Sheets, Slack).	Bypasses HIPAA-compliant controls; regulators see it as negligence.	Likely coverage disputes; insurers may increase premiums for lack of SaaS governance.	How do we track and control unauthorized tools handling PHI? Do we have a process to quickly onboard and approve SaaS securely?
6	Inadequate Incident Response Planning	Breaches discovered too late, poor containment, delayed regulator notifications.	HIPAA requires 60-day notification; delays multiply fines and damage trust.	Insurers scrutinize IR planning; delays inflate claim amounts.	When was our last incident response drill? Do we have pre-drafted patient/regulator communications ready?
7	Insider Threats & Lack of Monitoring	Employees snooping on records or ex-staff accounts left active.	Some of the largest HIPAA settlements come from insider abuse.	High incident costs; insurers ask about logging and monitoring of PHI.	Do we log and monitor all access to PHI? How fast can we deprovision accounts when staff leave?

8	Weak Vendor & Partner Security	Business associates mishandling PHI.	HIPAA holds you liable for vendor breaches if BAAs and oversight are weak.	Third-party breaches often excluded; insurers require vendor diligence evidence.	Do we assess vendors' security before signing? Are Business Associate Agreements (BAAs) current and enforced?
9	Insecure Data Sharing & Integrations	PHI shared via spreadsheets, email, or poorly secured HL7/FHIR integrations.	Direct violation of HIPAA transmission security rules.	Frequent claims from insecure transmissions; insurers ask about encryption in motion.	Do we allow PHI to be sent via email or messaging? Are integrations tested for security, not just interoperability?
10	Lack of Ongoing Security Training & Culture	Phishing, credential reuse, and human error remain leading causes of breaches.	HIPAA explicitly requires workforce security training.	Claims tied to phishing/social engineering often excluded if no training program.	How often do we run phishing simulations and training refreshers? Do staff know how to report a suspected breach immediately?