juno EHR

Cyber Health **Checkup**

Everything you need to establish a baseline for security and compliance in your network

junoehr.com

Table of Contents

Introduction

PHI. It's the most vital information you can collect about your patients. And it turns out that cybercriminals think it's pretty valuable, too. On the dark web, a patient's Social Security number can sell for up to $1,000 – by comparison, a credit card or social security number might go for $5 or $1, respectively.

This security threat spawned the creation of HIPAA and all its related compliancy laws — because a data breach isn't just potentially dangerous for your patient, it might also be incredibly costly for your organization.

According to an IBM Security report, the average cost of a healthcare data breach has reached a staggering $9.3 million in 2021.

That total includes many things from lost business to the cost of the breached record and any costs incurred from fees, fines, penalties or lawsuits.

Maintaining an effective compliance strategy is one of the best lines of prevention a healthcare organization can institute. This eBook is a collection of informative content to keep you and your organization safe from would-be cybercriminals. Inside you'll find:

- A quick refresher on HIPAA and how to successfully stay compliant
- A thorough checklist to gauge your cyber readiness, both for general users and your IT team
- A special case study exploring how global tensions can affect US data security
- An important message from the FBI
- And more

HIPAA Refresher

As a healthcare provider, you're required to keep your patients' PHI protected. To be successful in this endeavor, we recommend this two-part approach:

Stay Current on HIPAA Rules

HIPAA rules aren't evergreen. Occasionally, important changes to state laws and other privacy and security requirements are enacted that you need to keep aware of. Post changes in staff gathering areas or disseminate through email so your whole team can stay current.

Create a Culture of Confidentiality

To ensure confidentiality, build privacy and security into the company culture. Communicate your expectations clearly and consistently, guide your staff's compliance efforts and remind them why securing patient information is important not only to the patient but to the practice.

$180

the average cost of each compromised record

44%

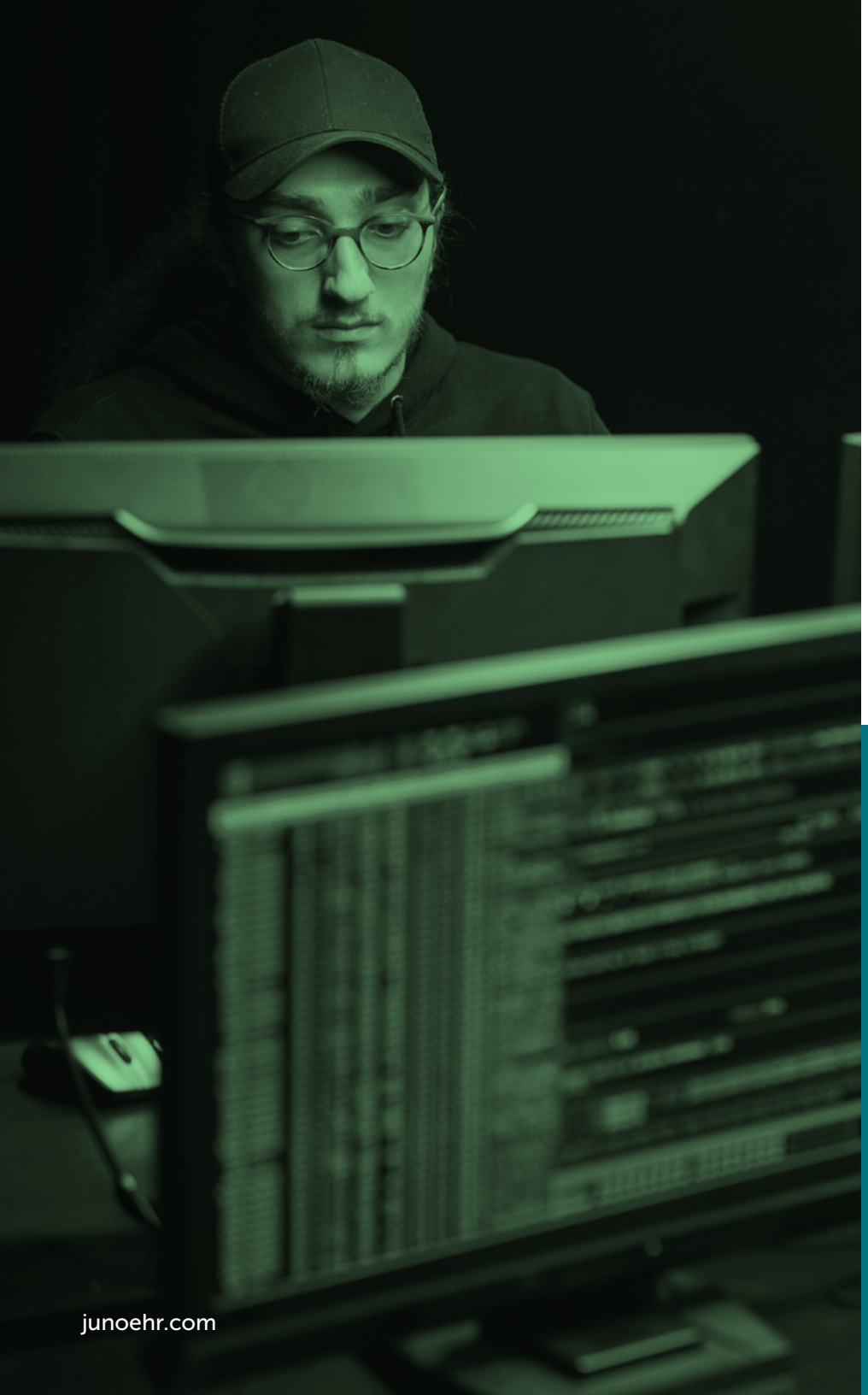
percentage of breaches in which PHI was targeted

20%

the amount of time a compromised credential was the cause of a breach

212

the average number of days to identify a data breach



FBI Ransomware Warning

The FBI urges local government agencies to take the following steps to protect sensitive data:

1. Do not pay ransoms
2. Keep all operating systems and software up to date
3. Implement a user training program with phishing exercises
4. Require strong, unique passwords
5. Encrypt all backup data
6. Keep all copies offline and investigate all abnormal activity

5 Warning Signs of a Cyber Attack*

1. Programs fail to load or quit unexpectedly
2. Files have been deleted or changed without your knowledge
3. A password has been changed suddenly
4. New programs or files appear on the system
5. Frequent pop-ups when accessing the internet

* Red Flags of a Potential Cyber Attack

Security Checklist

HIPAA compliance, cyber security and disaster management are all integral to protecting PHI. Use this guide as an organizational checkup to help with your organization's compliance, security and disaster management planning.

Below are the general tasks that should be reviewed regularly by your IT and leadership teams to maintain security, compliance and business continuity in the case of a disaster or other event.

- [ ] Develop policies and procedures regarding data privacy, PHI security and disaster management
- [ ] Review Policies and Procedures on an annual basis (at a minimum); note date of review or update
- [ ] Designate responsibilities for each leadership member in case of a disaster
- [ ] Train staff annually on HIPAA Breach Notification, Privacy and Security rules; document training; emergency management plan
- [ ] Create a business/associate tracking tool along with a list of URLs and contact information for any mission critical IT systems
- [ ] Review HIPAA requirements within disaster events, cyber security events, breaches or violations of HIPAA rules
- [ ] Ensure each member of leadership has access to at least two forms of the disaster management plans (hard copy and digital copy)
- [ ] Consider a third-party location to store a digital, encrypted copy of disaster management plans
- [ ] Perform PHI audits both within office workstations and on shared drives quarterly (at a minimum)
- [ ] Create a safety culture within workspaces by limiting guests in areas with PHI, monitoring passwords and other vital information left unsecured, and preventing other ways for PHI to be accidentally disclosed
- [ ] Dispense regular educational content to all staff regarding ways to reduce exposure to phishing, ransomware and malware

IT Specific Tasks:

These are tasks specific to your IT team for both prevention of and recovery from security incidents.

- [ ] Provide two-factor authentication for all employees who access PHI on laptops, mobile devices or personal devices
- [ ] Determine location and type of hosting for your EHR and other ways of accessing PHI
- [ ] If locally hosted, consider an alternate method of hosting that can be accessed in emergencies
- [ ] Verify your PHI backup cadence and ensure that backups are being completed regularly
- [ ] Make sure all WiFi networks are secured and passwords are changed regularly
- [ ] Ensure all virus, malware and ransomware software is regularly updated and working on all devices
- [ ] Audit for non-active users regularly and have policies in place for deactivation of accounts upon termination
- [ ] Review EHR mobile access protocols and provide proper training and planning utilization in the case of an emergency

Case Study

Global Tensions and The Effect on US Cyber Security

From espionage and misinformation to exploitation and ransomware, there's no shortage of ways valuable private information – like ePHI – can be compromised. And history shows us that in times of global tension, the desire to carry out cyber attacks grows exponentially, often spilling over into US networks.

Since the early days of the internet, cyber attacks have been carried out by bad actors in North Korea, Iran and China. But statistically speaking hacks by Russian cybercriminals have been more elaborate, more dangerous and often more costly.

Currently, Russia is at war with Ukraine, but that battle began long before 2022, deep in the terabytes of data that house the country's vital information. The ongoing conflict has seen Ukraine become a testing ground for Russian cyberwar tactics.

Many of these attacks branch out from Eastern borders and into US databases:

1. The infamous WannaCry ransomware;
2. Petya, the precursor to NotPetya;
3. NotPetya, which was widely viewed as a state-sponsored Russian cyberattack and led to data breaches from Pennsylvania to Tasmania, costing more than $10B in damages.

As the conflict continues, there is an expectation that attacks on cyber terrains will match those on physical terrains and CISA is keeping a close eye on potential threats. Experts agree that malware and ransomware are here to stay. Prevention is key. Organizations can bolster their cyber security measures with just these three simple steps: use strong and unique passwords, be wary of emails with unknown attachments and always keep an offline backup.

Compliance and cyber security are every bit as important to patient care as medical care and prescriptions, and healthcare organizations need to take steps to keep PHI and other confidential data secure. This eBook is a comprehensive collection of advice, educational and FUD content aimed at getting organizations to think critically about their cyber security and compliance measures.

Backed by more than 30 years of proven success in health information software development and systems integration, Juno Health is transforming digital healthcare. We think like healthcare providers because we listen to them first. Our team of experienced physicians, pharmacists, nurses and healthcare leaders drive our decisions and our process.

Providing seamless access to patient data is our lifeblood. From implementation through successful day-to-day use, our solutions are powered by our people, and our people empower you. We take a more human approach to create more user-friendly healthcare technology solutions.

Juno Health is the commercial division of DSS, Inc.

dsshealthit
juno-health-dss
561-284-7000
junoehr.com

juno EHR

Find more insights at junoehr.com