THINK SECURENET | SECURENETMD

THE 50-POINT **HEALTHCARE DATA BREACH** PREVENTION CHECKLIST

Have you done everything you could do to prevent a data breach

Information security is critical for every business, but especially for those in healthcare. Our self-evaluation can help identify areas of concern so you can make sure your patient's information is as safe and secure as possible.

- ☐ Information safety, security, and protection of protected health information (PHI) and individually identifiable health information are core values of our organization.
- ☐ We have an annual 3rd party independent HIPAA Security Risk Assessment.
- ☐ We annually conduct a HIPAA Privacy Assessment.
- ☐ We annually conduct a HIPAA HITECH Subtitle D Audit.
- ☐ We annually conduct a HIPAA Security Standards Audit.
- ☐ We annually conduct a HIPAA Asset and Device Audit.
- ☐ We annually conduct a HIPAA Physical Site Audit.
- ☐ We document gaps and deficiencies after each audit.
- ☐ We have remediation plans that address deficiencies in audits.
- ☐ We update and review remediation plans annually.
- ☐ We retain remediation plan documents in our records for six (6) years.
- ☐ We have Policies and Procedures relevant to the annual HIPAA Privacy, Security, and Breach Notification Rules.
- ☐ We have a staff member designated as the HIPAA Compliance, Privacy, and/or Security Officer.
- ☐ All our staff members have undergone HIPAA training, and we have documentation indicating that each staff member has completed HIPAA training.
- ☐ We have documented policies and procedures related to PHI and HIPAA compliance.
- ☐ All staff members have read and legally attested to these policies and procedures.

16557 Coastal Highway
Lewes, DE 19958

Local: (302)703-9717
Toll Free: (855)645-8647

- [ ] All our staff can recognize PHI and individually identifiable health information in any form or media, whether electronic, paper, or oral.
- [ ] All our staff are educated about how to communicate with clients securely. Staff also know what methods of communication should not be used.
- [ ] We regularly provide staff education and training on cybersecurity, including common techniques used to obtain access to computer systems by hackers, like phishing, cryptojacking, tabnabbing, and cybersquatting.
- [ ] All our staff know how to avoid malware and virus infections, recognize symptoms of viruses or malware, and know who to contact in our organization if hacking is discovered. We remove access to user accounts for former employees promptly.
- [ ] If an employee is involuntarily terminated, account access is removed prior to an employee's notice of termination.
- [ ] We have a defined process for incidents or breaches, including tracking and managing the investigations and providing the required reporting of minor or meaningful breaches or incidents.
- [ ] Our staff members have the ability to report an incident anonymously.
- [ ] We have offsite backups of all our information stored according to HIPAA regulatory requirements.
- [ ] We have a recovery plan that covers how to access and restore backed-up data that meets compliance regulations.
- [ ] We have identified all our vendors and business associates and performed due diligence to assess their HIPAA compliance.
- [ ] We have confidentiality agreements with non-business associate vendors.
- [ ] We have identified all our vendors and business associates and performed due diligence to assess their HIPAA compliance.
- [ ] We know if our electronic health records vendors maintain an open connection to the installed software and affirm that it is secure.
- [ ] Our facility's handheld, portable, and mobile devices are secure and are protected with strong authentication and access controls.
- [ ] Handheld or mobile devices that support antivirus software have it installed and operating.
- [ ] Our portable devices have data encryption capabilities, and steps are taken to prevent unauthorized viewing and theft of mobile devices.
- [ ] Unused data files are regularly archived or removed from the system (in accordance with data retention requirements.)
- [ ] Our computer systems have antivirus protection software that is regularly updated.
- [ ] We constantly monitor software for critical and urgent patches and updates that require immediate attention.

- [ ] We update software used in our practice to the most recent version using automated tools or on a regular schedule.
- [ ] We review installation defaults or “standard” configurations when installing software to ensure that access is appropriately limited.
- [ ] We uninstall software applications that are not essential to running the practice.
- [ ] Outdated software, unused or unnecessary programs, and trial software are completely uninstalled from computers and devices.
- [ ] We require multi-factor authentication to access sensitive information.
- [ ] We have a password policy that includes requiring strong passwords that are changed regularly.
- [ ] Optional password protection is enabled on all our devices or programs that offer it.
- [ ] Our network uses a hardware firewall configured, monitored, and maintained by a specialist in this subject.
- [ ] Our wireless network is encrypted and permits access only to devices identified as legitimate.
- [ ] Visitors cannot access our wireless network.
- [ ] Peer-to-peer applications (instant messaging, social media, etc.) are not installed on any device that holds PHI without ensuring PHI is protected and secure.
- [ ] We limit the places that we store data and control access to PHI with role-based access control.
- [ ] Users have access only to information which they need to know to perform their duties.
- [ ] We control and monitor physical access to devices containing PHI and policies in place to limit physical access to devices and locations where PHI is stored. (Securing machines in locked rooms, managing physical keys, and restricting the ability to remove devices from a secure area.).
- [ ] We have disabled remote file sharing and remote printing within our system to prevent the accidental sharing or printing of files to locations where unauthorized individuals could view them.
- [ ] We ensure hardware with memory (like printers, fax machines, and scanners) is wiped before removal from the practice.
- [ ] We use professional-grade hardware (routers, network cabling, etc.) that meets security best practices.
- [ ] Our network is properly segregated and uses a hardware firewall that is configured, monitored, and maintained by a specialist in this subject.

ThinkSecureNet provides strategic technology solutions built around your healthcare organization.

With a 98% client retention rate over 15 years, ThinkSecureNet's healthcare division is a trusted long-term partner to organizations across the healthcare industry. Find out how our award-winning, HIPAA-compliant managed solutions can help you achieve higher levels of operational efficiency, security, and HIPAA compliance at **ThinkSecureNet.com**.

16557 Coastal Highway
Lewes, DE 19958

Local: (302)703-9717
Toll Free: (855)645-8647