Questions? Contact the AAHA Business Insurance Program at 866-380-2242 to learn more about data breach coverage.

Small Commercial

AAHA RECOMMENDED The Standard of Veterinary Excellence

THE HARTFORD

8 TIPS TO HELP REDUCE YOUR RISK OF A DATA BREACH

START WITH THE BASICS

1. Lock and Secure Sensitive Information Stored in Paper Files and on Removable Storage Devices

Theft or loss, and the subsequent unauthorized release, of sensitive data, or Personally Identifiable Information (PII) (eg: social security number, credit/debit card information, medical records/charts), stored in paper files and/or a removable storage device (eg: computer disk, thumb drive) may constitute a data breach. Never leave sensitive information unattended. Store it in a locked drawer, cabinet, safe or other secure container when not in use. Also consider installing an alarm system that alerts law enforcement if you have a break-in on your premises.

2. Restrict Access to Data

Restrict access to sensitive data, whether physical or electronic, to those who have a "need to know." Most employees do not need unrestricted access to your company's entire network. Remember to limit network access on computer stations located in public spaces, such as the reception area.

3. Properly Dispose of Sensitive Data When No Longer Needed or Required

Shred documents containing sensitive data prior to recycling. Remove all data from computers and electronic storage devices – including those on copy machines – prior to disposing of them.

4. Record and Regularly Review Data Practices

Distribute and explain data protection practices to all employees. Review and revise these practices on a regular basis – at least annually. Make sure to re-train staff as changes to your data practices are made.

STRENGTHEN YOUR TECHNOLOGY PRACTICES

5. Password Protect Systems

Password protection helps to prevent unauthorized access to sensitive information, protect security of personal information and prevent unauthorized access to user and email accounts. All users should be assigned unique user names and strong passwords for access to systems – changed at least quarterly. Conduct a password audit on a regular basis.

6. Encrypt Data

Encryption helps protect the security and privacy of files as they are transmitted or while on your computer. Install encryption onto all laptops, mobile devices, flash drives and back-up tapes, and encrypt emails that contain sensitive information.

7. Ensure That Remote Access to Your Network is Secure

Remote access to your network should be made through appropriately enabled Virtual Private Network (VPN) connections and multi-factor authentication (e.g. soft tokens or fingerprints in addition to passwords). Passwords should be changed on a regular schedule and meet minimum complexity and length requirements.

8. Keep Software and Operating Systems Current

Keeping your software and operating systems current by installing software and security updates is your first line of defense against hackers, who often take advantage of unprotected systems to gain access to sensitive data stored on a computer.

You should also have a firewall and up-to-date anti-virus programs. A firewall helps to prevent your system from being attacked, while anti-virus software inspects the files and programs on your system to ensure they are not infected. Both are critical in helping to protect sensitive information stored electronically.

To maintain the most up-to-date protection, download recently issued system and security updates and antivirus and anti-malware updates to help protect you against the newest forms of viruses, Trojan horses and other malicious software.

NOTE: If your network security functions are outsourced to a 3rd Party, obtain documentation to understand how your company's data is protected, and, when appropriate, perform on-site due diligence. It's also important to have contract language that specifies privacy and data security expectations and grants you the right to audit the 3rd Party.

While these data protection policies, procedures and training can help reduce the likelihood of a data breach, no company can be completely certain that its customer, patient or employee data could never be at risk. For this reason, it is important for companies to also have appropriate data breach insurance coverage in place. To learn more, visit **www.hartforddatabreach.com**