VGM Insurance Services

The van Halem Group
A Division of VGM Group, Inc.

1111 W. San Marnan Drive
P.O. BOX 1328
WATERLOO, IA 50704
PHONE: 800-362-3363 FAX: 319-235-6656
EMAIL: info@vgminsurance.com

MANAGING HIPAA COMPLIANCE AND RISK

Brought to you by VGM Insurance Services in conjunction with The van Halem Group, an affiliate company of VGM Insurance Services.

Throughout 2017, the Office of Civil Rights (OCR) issued more than $19 million in fines related to HIPAA violations.

Insurance SERVICES

The van Halem Group
A Division of VGM Group, Inc.

1111 W. San Marnan Drive
P.O. BOX 1328
WATERLOO, IA 50704
PHONE: 800-362-3363 FAX: 319-235-6656
EMAIL: info@vgminsurance.com

There are a number of good reasons to get and keep your business on track toward HIPAA compliance. For one, throughout 2017, the Office of Civil Rights (OCR) issued more than $19 million in fines related to HIPAA violations. Compare that to fines in 2015 totaling approximately $6 million, and it becomes clear that businesses responsible for handling patient health information (PHI) need to be more diligent than ever.

COMMON HIPAA VIOLATIONS

Do a quick search of recent HIPAA violations, and you'll find headlines proclaiming multi-million dollar settlements for breaches resulting in the loss of hundreds, thousands, or even millions of patient records.

Yes, it's true that the health care industry is the number one target for cyberattacks, and you should use the technology and resources available to you in order to secure your patients' data. However, there are four other common violations that fail to make the headlines but are potentially as devastating as experiencing a cyberattack.

1) Mishandled Medical Records

With all the talk of cyberattacks, one might think that keeping all patient records as hard copy could limit exposure. It's important to remember how easy it is to misplace a document and how difficult it can be to pin down who has accessed it. Don't leave medical records out in the open. Ensure that they are filed and locked away to prevent records from falling into the wrong hands.

At some point, you will have a need to dispose of some records, either because they are outdated or you're transitioning to digital storage. Proper steps should be taken to ensure PHI is disposed of properly. Consider working with a secure document shredding company. To learn about proper disposal methods, you can visit the U.S. Department of Health and Human Services website at **www.hhs.gov.**

2) Social Media

Social media is thoroughly ingrained in everyday life. Many of us take pictures and post regularly as part of our default setting, not considering the content making its way onto the internet. But, when it comes to HIPAA, there are some precautions that must be taken. Never post a photo of a patient without written consent. Without proper documented consent, you're compromising that patient's protection. One of the best and simplest ways to prevent this is to ensure all employees are aware of the HIPAA policies in place to prevent the sharing of PHI.

3) Employees Disclosing Information

Violations aren't limited to what gets posted on the internet, however. Employees should be mindful of where they're discussing topics about patients and who they're discussing it with, even around the watercooler at work. Keep these conversations with friends and family to a minimum as well to avoid sharing PHI.

This can be easier said than done in close-knit communities, but asking a medical professional about a friend can lead to a breach as well. If you find yourself in this situation, be sure to have a canned response ready that explains you cannot disclose any information about a patient.

4) Accessing Patient Information on Home Computers

Information security officers dislike this as well, referring to "Bring Your Own Device," or BYOD. However, sometimes you have to take your work home with you. Your computer should never be left alone or without password protection when it handles PHI. Exposing it to family members or having it shared to the wrong online channels can lead to significant fines.

STEPS YOU CAN TAKE

It's never a bad time to plan and re-assess your compliance and risk. Below are five steps you can take to help get you started.

1) Select or Hire a Compliance and Security Officer

Having someone on staff dedicated to ensuring compliance along with training and updating other employees can help mitigate any non-compliance risks. If the budget allows, start looking to hire or educate a compliance officer. Remember, if you don't have someone designated to be leading compliance efforts, you're not in compliance.

1111 W. San Marnan Drive
P.O. BOX 1328
WATERLOO, IA 50704
PHONE: 800-362-3363 FAX: 319-235-6656
EMAIL: info@vgminsurance.com

2) Develop a Risk Assessment

This is a way of identifying potential risks, vulnerabilities, availability, and integrity of PHI. This includes the information your organization creates, maintains, receives, and transmits, and having a risk assessment in place is critical to being compliant. Because entities can now be fined for not identifying potential risks, this should be the next step after identifying your compliance officer.

3) Create HIPAA Privacy and Security Policies

These lay the groundwork when developing the rest of your compliance strategy. The goal in this step is to develop a plan on how your organization will protect PHI. The work doesn't stop with the creation of these policies, though. Review them with staff on a regular basis and update, at minimum, on an annual basis.

4) Educate your Employees

This step may come last in this section, but it certainly is not least. When it comes to breaches, whether by a cyberattack or the common violations discussed earlier, employee education is one of the most important ways to minimize the risk to patient records. Employees should receive annual education on all the policies and procedures in place, and accurate documentation of that education should be kept in case of an audit.

5) Purchase Cyber Liability Insurance

Finally, providers should consider purchasing a Cyber Liability insurance policy as an additional layer of protection for their business. Cyber policies can cover a business's financial liability for a data breach.

STAY THE COURSE

It may seem like a tall order, but don't lose sight of your HIPAA compliance goals. When it comes to protecting your patients' data, the stakes are simply too high.

If you do need a little help working through these steps, though, The van Halem Group's **HIPAAwise complete compliance program** provides a simple and affordable solution to avoiding HIPAA fines and penalties. Check out **www.hipaawise.com** to learn more about this powerful HIPAA compliance software. Also, be sure to visit The van Halem Group online at **www.vanhalemgroup.com** to learn more about what they can do to help you with audits, appeals, compliance, enrollment, education, and other complex issues.

The van Halem Group
A Division of VGM Group, Inc.