How the HIPAA HITECH Act Affects Your Business

Dear [Salutation],

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) is a relatively new law, and with it comes a brand new list of things you must keep in mind from an management standpoint. In this email series, we'll be helping you to gain a better understanding of how the HITECH Act affects your company and what preventive steps you can take to avoid losing thousands of dollars in fines as a result of noncompliance.

As you likely already know, all healthcare providers are subject to the Health Insurance Portability and Accountability Act (better known as HIPAA). This act focuses primarily on data privacy and security regulations. More specifically, it establishes rules and regulations about how healthcare providers must handle sensitive information of respective patients. In other words, it makes ensuring patient privacy and non-disclosure to third parties a legal responsibility to you, the healthcare provider.

The HITECH Act expands the reach of these obligations to also include "business associates" of healthcare providers. Factually, it means that law firms and accounting companies conducting business with a healthcare provider are now subject to HIPAA regulations. Thus, even ancillary business associates are now held accountable for the same data security compliance as healthcare providers themselves.

Another important facet of the HITECH Act changes how HIPAA is enforced. A number of recent cases have shown the new system to be more punitive - and a lot less forgiving. In fact, as of February 17, 2011, "willful neglect" is amongst the violations for which monetary penalties can be issued.

If your company somehow managed to get by without paying too much attention to HIPAA compliance in the past, today is the day you need to start reviewing your current processes, procedures and systems. Privacy and data security breaches are being taken a lot more seriously, and if you're not careful, your company might be next on the radar for hefty fines and penalties.

In the next installment, we'll provide you with a few examples of HIPAA violations, and what steps you can take to prevent them from happening to you.

[Closing info]

Violating HIPAA is Easier than You Probably Think

Dear [Salutation],

As previously explained, the goal of the new HIPPA HITECH Act is to improve data security and patient confidentiality. Unfortunately as a healthcare provider or business associate of a healthcare provider, the act makes compliance much more complicated. Complications are no defense against the law, however, so it's imperative for you to take all necessary precautions to keep your company off the list of HIPAA violators.

All data protected by HIPAA is referred to in a single term – Protected Health Information (PHI). PHI refers to any documents or data that includes information that can be traced to a specific individual. It includes, but is not limited to:

- Names, birth dates and images of the patient
- Social Security and medical record numbers, IP address numbers
- Phone or bank account numbers

All healthcare providers and their business associates must now follow specific guidelines as to how this information is properly stored and used, and under what circumstances it can be disclosed to third parties. Easier said than done, when violating the HIPAA by accident is so easy!

Let's take a look at a few examples of what can land you in hot water:

1. Disclosing PHI to law enforcement officials in a manner that does not conform to the Privacy Rule. In fact, providing a patient's health information to public safety institutions can only be done as a response to a formal, written request.
2. Providing a law firm or any other partner company with a patient's PHI if you haven't already entered a Business Associate Agreement. The agreement makes your business associates legally responsible for safeguarding the data.
3. Sending test results and other health-related information to the patient's employer or family without the patient's consent.

It is possible that unbeknownst to you, the employees of your company - or even automated processes - are currently violating HIPAA on a daily basis. If you don't evaluate your current data protection policies, you could receive an unpleasant letter from the Office of Civil Rights very soon. Pushing this off until tomorrow could prove to be costly.

In part 3 of this HIPPA HITECH series, we'll show you why it's a bad idea to ignore HIPAA and what damage can be caused simply by not being up to date with the respective laws. Stay tuned!

[Closing info]

HIPPA: Compliance and Damages from Ignoring It

Dear [Salutation],

Now that you know how changes in HIPPA compliance have been affected due to HITECH, it's important that you understand why reviewing and evaluating your policies and processes is a must.

The Office of Civil Rights (OCR) is responsible for enforcing all HIPAA Privacy and Security Rules. Keep in mind that while the job is massive, the agency has a number of tools at its disposal on any given day. Compliance violations are not taken lightly so knowing what to expect is the first step in protecting your company from fines and penalties.

Here's a quick summary of how compliance is enforced:

1. **Patient complaints are not just empty words.**
   Over the past few months, OCR has become more active than ever, investing massive amounts of time and resources into investigating complaints about healthcare providers. During these investigations, your data safety measures are closely inspected, revealing any non-compliance with HIPAA. This means that if a patient feels you've mishandled their personal information, you could be facing quite a hefty fine.

2. **An auditor could be knocking on your door at this very moment.**
   On November 8, 2011, U.S. Department of Health and Human Services (HHS) announced details on a new audit program to be performed on all HIPAA covered entities. In the release, they say that audits provide a chance to "examine mechanisms for compliance, identify best practices and discover risks and vulnerabilities that may not have come to light through OCR's established complaint investigations and compliance reviews."

   These audits will act as a thorough examination of the healthcare provider's or its business associate's compliance to HIPAA. In this sense, audits will go much deeper in investigating the safety measures and policies than the investigations performed by OCR.

One thing does remain the same in both cases – any non-compliances are sure to result in large monetary punishments.

If you think that you're exempt or that "it'll never happen to you," here's a grim example to illustrate why ignoring these inspections is a bad idea. Over a two-year period, OCR received a number of complaints about a specific treatment provider. Cignet Health Care, a health care issuer, ignored requests for access to the health records of 41 individuals. To make matters worse, Cignet failed to respond to OCR's investigation and for the most part just ignored it. The result? A $1.3 million penalty attributable to failure to provide access to the health records, as well as a $3 million fine for not cooperating with the investigators. Could your business afford to survive if assessed these types of fines?

The easiest way to prevent this from happening is to maintain compliance at all times and learn from other companies mistakes. In this case, precedent can be an absolute saving grace for your business.

In part 4 of our series, we'll be discussing the most common mistakes health care providers make, and how to avoid them. Check your inbox in a few days!

[Closing info]

Worst Mistakes Health Care Providers Make

Dear [Salutation],

Since you now understand the danger of not being up to date with HIPAA regulations and compliance, you're probably wondering where to start when it comes to reviewing your current safety policies. To make sure you don't overlook anything, we've put together a list of the most common mistakes, with the end goal of preventing frustrating legal issues and hefty fines being assessed in your immediate future.

Leaving It All to the Employees
To ensure your business complies with all the HIPAA guidelines, you must ensure you're competent in the subject. Too often, proper safety measures are not undertaken because the people supervising the work are simply not educated enough. To ensure the safety of your patients' data, you must have thorough knowledge of all the relevant laws and regulations. Once you do, only then can you start devising proper data safeguarding policies throughout your company.

Leaving Someone Out of the Puzzle
If you have employees handling sensitive data on a daily basis, you must make sure each knows what necessary precautions should be taken. No matter how large or small the scope of sensitive information accessible to a member of your staff may be, each employee must be trained about HIPAA guidelines – and more importantly, about HIPPA compliance. Keep in mind that many violations are a result of personnel inadvertently failing to work according within the guidelines.

Burying Your head in the Sand
When OCR comes knocking, the easiest and only way of properly dealing with the situation is by cooperating to the fullest. Trying to hide your mistakes or blatantly ignoring an investigation only causes more trouble, as illustrated by the large numbers of health care providers who have recently come to face hefty fines as a result of this lack of cooperation. Quite frankly, the best you can do in the case of an audit or a compliance investigation is to provide OCR with and any all data that is requested.

The most common mistake is going to one of the extremes – either only having management personnel keep track of compliance, or allowing employees to handle it solely on their own, with no oversight or interaction with management about it. Obviously, a balance between the two needs should be established for the best end results. Otherwise, an investigation by OCR runs the risk of damaging or completely shutting down your business.

Truth be told, once an investigation starts, there isn't much you can do. As such, the only way to keep your company safe is to ensure compliance in all areas. Stay tuned for the final installment in this series, where we'll be sharing tips on how to actually ensure your organization complies with HIPPA regulatations – and more importantly, stays there.

[Closing info]

Better Safe than Sorry!

By studying examples of HIPAA violations, it becomes clear that a large portion of them could have been easily avoided had the health care provider followed the rules and regulations specifically set out by HIPPA and HIPPA HITECH. To prevent your company from ending up in the same boat, here are a few general tips to ensure the safety of your patients' private information:

1. **Educate, Educate and Educate a Little More**

If your staff isn't aware of all the specifics of HIPPA, you're literally asking for trouble. Organize staff training and task all relevant personnel to take courses. Knowledge is power and the only way to prevent accidental violations is by ensuring that your employees are in-the-know.

2. **Make-Do with the Minimum**

Providing a patient's entire health history on every form and document is the data privacy equivalent of walking around with a grenade in your pocket. As a rule of thumb – never write birth dates, medical histories, phone numbers or any patient-specific information on documents that can land in the hands of anyone but the patient. This also means that you should refrain from using specific department names in publically accessible documents that could be traced to a specific patient.

3. **Measure Twice before Cutting Once**

If you're not sure whom you can disclose the PHI to, research it. A typical case of violating HIPAA occurs when a health care provider thought he (or she) could share the PHI – perhaps by sending health information to the patient's family or employer. Before disclosing any information about your patient, make sure it complies with the HIPAA. No exceptions.

4. **Provide a Copy of the *Notice of Privacy Practices* to ALL Your Patients**

This rule just can't be stressed enough. With this notice, you're letting each patient know what information you'll be gathering and how it will be used. It describes your privacy rights, and covers all cases when the PHI might be disclosed to third parties. This greatly reduces the number of disputes between patients and their health care providers, and ensures that both parties have a clear agreement about how sensitive information will be used.

Hopefully using these tips, your company will be one step closer to full compliance with HIPAA. It's a good idea to treat your patients' personal information as if it were your own, ensuring it doesn't get in the wrong hands. This common sense approach can prevent headaches and fines from being assessed in the future.

[Closing info]