

HITECH Impact on Email and Web Outsourcing

The American Recovery and Reinvestment Act (ARRA, or The Obama Stimulus Bill), signed into law in February 2009, includes new, more comprehensive provisions for HIPAA. These provisions are in a section of the bill known as the Health Information Technology for Economic and Clinical Health Act (HITECH).

For organizations that are already required to abide by HIPAA (i.e. the “Covered Entities” of HIPAA), HITECH adds the following requirements:

- Mandatory yearly audits by Health and Human Services to make sure that you are meeting the HIPAA requirements
- Explicit fines of up to \$1.5 million dollars/year for disclosures of protected health information that violate the HIPAA Privacy Rules
- Business Associate Agreements with vendors and partners who have contact with your organization’s protected health information is now mandatory.
- New mandatory reporting requirements on unauthorized disclosures of protected health information — to those whose information was disclosed, to Health and Human Services, and for large enough disclosures, to the media.

For HIPAA Business Associates, HITECH imposes even more serious changes:

- Business Associates are now responsible for following all HIPAA Privacy and Security regulations with respect to all protected health information that they obtain or generate.
- Unauthorized use or disclosure by Business Associates of any protected health information leaves the Business Associate equally liable to damages and unfavorable publicity.

Organizations with Email and Web Services In House

For those with email and web services in house, you must be more vigilant now to ensure that you are abiding by all of the facets of the HIPAA Privacy and Security Rules.

What Makes a Web Site HIPAA-Secure?

What HIPAA Says about Email Security

Is a FAX document HIPAA-Secure?

You should expect to be audited. You should expect to pay heavy fines if there are any problems. Worse, if there are significant issues, you should anticipate negative publicity for your organization. Moving or keeping things in-house avoids having to place your trust in and rely upon third parties. However, opting not to outsource your email and web services, means that you have to trust that your infrastructure conforms to the new HIPAA legislation. Your staff must have the expertise, training and discipline to follow these new guidelines.

With HITECH, it makes more sense than ever to outsource:

You have less responsibility and overhead

Some of your liability shifts to your Business Associates

I.e. it generally costs you less, provides solutions that solidly meet HIPAA, and limits your HIPAA liability.

Outsourcing Email and Web Hosting Services

If you are outsourcing your email or web hosting services and there might be protected health information (PHI) passing through or stored on those servers, then you as a customer must ensure:

1. That you have a Business Associate Agreement (BAA) with your vendor.
2. Your vendor recognizes your account as containing PHI.
3. Your vendor is aware of the HITECH changes to HIPAA and this is reflected in its BAA.
4. Your vendor is actively safeguarding your PHI with all methods needed to follow the HIPAA Security and Privacy Rules.

Why is it prudent to take these steps?

- Many vendors do not know what are the changes to HIPAA imposed by HITECH. Really! We have spoken to many professionals who are surprised that HIPAA is changing and who are now scrambling to figure out “what to do”.
- The HITECH changes are very significant for Business Associates. In the old scheme, all burden and liability was on the customer (the Covered Entity) and most Business Associate agreements just said things like “be sure to use our services in a way that doesn’t violate HIPAA”. The Business Associate was under no obligation to follow HIPAA Security and Privacy rules themselves.
- The principal responsibility for safeguarding PHI still falls on you, the Covered Entity. If you do not bother to check and are using a vendor that is not updated for HITECH — it is your negligence and can result serious penalties if there is any kind of breach.

So, now is the time to review your PHI practices and policies. Check with your vendors and be sure that they are in step with the new legislation and that you have Business Associate Agreements that covers HITECH by February 17, 2010 deadline.

The Burden on the Business Associates

The HITECH changes described above place significant new burdens on Business Associates. They are now exposed to liability and monetary and publicity penalties in the event of a HIPAA privacy breach in their systems, so they must:

- Know what information in your account is PHI.
- Make sure that information is backed up, transmitted securely, and encrypted if needed.
- Implement access controls to track who could have accessed that information — both from the public interfaces and through their back end systems.
- Track uses and disclosures of that information.
- Ensure that all parts of their infrastructure that may be used to store or transmit PHI are covered by the Security and Privacy Rule Requirements.
- Ensure that all staff that may be accessing your PHI in any way are trained and authorized.
- Report unauthorized disclosures of PHI to Health and Human Services and possibly the media.

Here is a short overview of the vast checklist of action items that must be completed, policies that must be documented, training that must occur, etc.

It is important to note that Business Associates need to know what is PHI on their systems so that they can protect it. They must implement policies to ensure that this data is protected. If they leave these services “up to you” and you are doing things that are “not right with HIPAA”, then they have an explicit obligation to stop you or to terminate your account. If they “just let things slide” or “pay no attention”, then they themselves are being willfully negligent and can face some serious penalties if there is an issue. If you use a vendor that you know is lax, then you share that liability. And the burden of liability is very significant.

What about liability waivers? If the Business Associate has you sign a waiver where you agree to assume the liability of using their services inappropriately, that does not necessarily protect them from being sued by Health and Human Services or from bad press — it does allow them to counter-sue you, however. It certainly motivates you to make sure that you are following HIPAA.

What about vendor accounts with no Business Associate Agreement? Sure, it is up to the Covered Entity to make sure that they have a HIPAA Business Associate Agreement with the vendor, but what if they don't and are using the vendor's services for PHI anyway? If the vendor were to become aware of this, it would be incumbent upon the vendor to either establish a contract and start protecting the PHI, or to terminate the customer's services.

What does this all mean?

- Vendors will probably have to revise their privacy policies and Business Associate Agreements.
- Vendors may need to impose strict policies and usage restrictions on HIPAA customers so as to ensure that PHI is safeguarded to the maximum amount reasonably possible in their system.
- Vendor accounts used for HIPAA may be less flexible than previously in terms of how they can be used and configured.
- Expect to sign liability waivers for services where the Business Associate cannot be expected to monitor or control the flow of PHI. I.e. web site hosting where you are in control of your web site content, or email hosting if you resist encrypting all email messages.
- If you, as a HIPAA customer, need to do some things that are insecure (and do not involve PHI) and some things that are secure (do involve PHI), you should expect to setup separate accounts with separate levels of restriction. The better you compartmentalize PHI and regular data, the more reliably you and the Business Associate can safeguard that PHI.

Courtesy : <http://luxsci.com/blog>