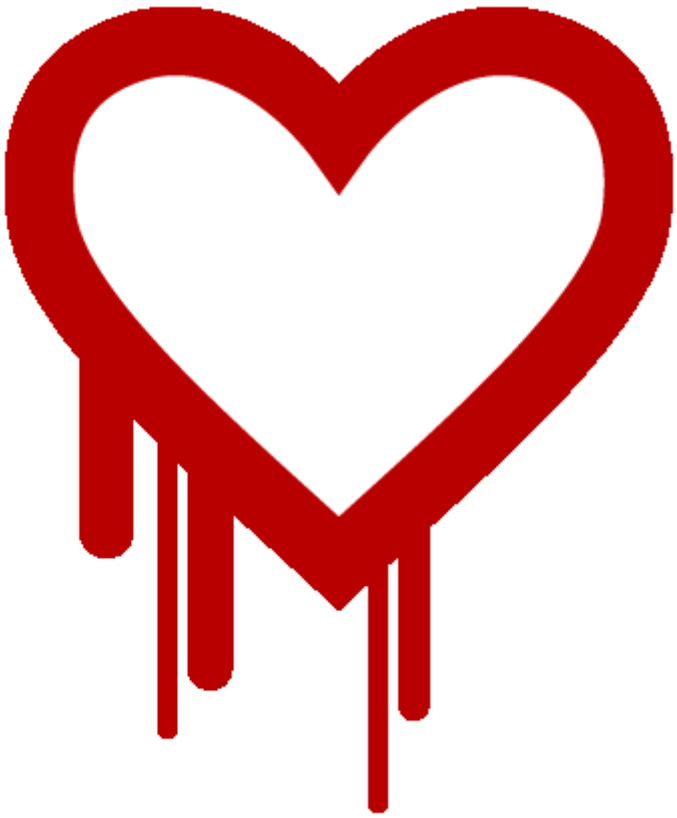
HIPAA, HITECH and Heartbleed:



Did Your Medical Practice Complete These 7 Easy Steps?

Qinaya
IT Architects
Design • Develop • Deploy

Did Your Medical Practice Complete These 7 Easy Steps?

It has been a month now since the discovery of the Heartbleed bug. In that time, many companies have undertaken audits and completed corrective actions, when needed, to ensure their data is protected moving forward. Computer Scientists at the University of Michigan reported at least 41 separate groups had probed data intentionally placed on the internet as a test and as of just a few weeks ago estimated over 1 million web servers were still vulnerable.[i]

What is Heartbleed?

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).[ii]

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate

services and users.[iii]

HIPAA and HITECH

Why is this important to my practice? The simple answer: HIPAA and HITECH.
Under the Health Insurance Portability and Accountability Act of 1996[iv], as amended ("HIPAA") and the Health Information Technology for Economic and Clinical Health (HITECH) Act[v], covered entities have specific responsibilities and duties to safeguard Protected Healthcare Information (PHI). With the widespread adoption of EHR's/EMR's and Practice Management Systems, combined with new patient access models, the PHI your practice stores may be at risk.

One very important part of the HITECH Act amended section 1176(b) of the Social Security Act and very clearly states:

Striking the previous bar on the imposition of penalties if the covered entity did not know and with the exercise of reasonable diligence would not have known of the violation (such violations are now punishable under the lowest tier of penalties); and

Providing a prohibition on the imposition of penalties for any violation that is corrected within a 30-day time period, as long as the violation was not due to willful neglect.

We read this to mean that a medical practice can avoid any penalties under HIPAA or the HITECH Act so long as the violation is corrected within 30 days from the knowledge of the vulnerability – or basically 30 days from when the Heartbleed bug became widely known.[vi]

Having said that, let's look at the areas a prudent practice would have examined. And as always, the best prevention is

documentation.

Your office/facility systems

With the widespread use of computers and computerized systems, it is entirely possible that a software program running in your practice, or that you or your staff access via the internet, is vulnerable to the Heartbleed bug.

To the right is a list of some of the most common systems that medical practices utilize on a regular basis. Have you, your office manager or your IT staff checked with each vendor and examined each software and hardware system to determine vulnerability?

If you have, congratulations! We recommend keeping a copy of the source documentation (e.g. an email from the vendor) in a file for future reference. But looking through this list, if something has slipped your mind, take this opportunity to obtain the necessary documentation or ensure the appropriate upgrades have been performed.

1. ***EHR/EMR***
2. ***Patient Scheduling/Front Office***
3. ***Bookkeeping/Back Office/Banking***
4. ***Mobile Devices***
5. ***Servers***
6. ***Modems and in-office hardware***
7. ***What about the Hospital/ASC/Clinic?***

Your vendors' systems

You've signed Business Associate Agreements with your vendors, and they know about their requirements under HIPAA and HITECH. Even so, the prudent practitioner should ask each vendor to supply documentation of their systems examination and that Heartbleed had either not been an issue, or that corrective action has been completed.

Here are some common vendors for medical practices. Do you have documentation from each?

1. ***EHR/EMR connections to other providers***
2. ***Billing System interfaces***
3. ***Eligibility Verification***
4. ***Medical Supply Orders***
5. ***Laboratory/Pathology Provider systems***
6. ***Pharmaceuticals orders***
7. ***Pharmacy***

What about my patients?

That's right! What about your patients? It is their PHI you are charged with protecting, and we know patients today have access to wide ranging information and have been bombarded with Heartbleed data from their own banks, insurance companies and other services providers.

This is an opportunity for you to show your patients how much you truly care for them and how well you and your team protect their PHI.

Additionally, many practices now allow online bill payments, online appointment setting, online consultations and online records reviews. If this is the case with your practice, we recommend that you ask patients to update passwords for access to your systems.

1. The most important step to take with your patients – ***let them know what you've done.***
2. The second most important step to take with your patients – if they have passwords, ask them to change them.

HIPAA, HITECH and Heartbleed

7 easy steps

1. Check your software and your hardware
2. Contact each vendor and have them provide certification of checking their software
3. Contact your contracted healthcare provider relations representatives; have them provide certification of checking their software
4. Change your passwords (you and everyone in your staff) in every system AFTER the three steps above
5. If you use patient access software, ask patients to change passwords
6. Document, document, document – keep a file (digital is ok) of your documentation
7. *Let your patients know!* They'll appreciate it: post a sign in your waiting rooms reassuring your patients that their PHI is safe with you!

About the Authors:

Fernando Goicochea is a Founder and Chief IT Architect of Qinaya, LLC. Qinaya is an IT Architectural Firm based in Miami, Florida with additional offices in Pune, India. Qinaya designs, develops and deploys customized software solutions and integrations. Qinaya clients include healthcare, finance and government organizations.

Robert Cardwell is President of The Cardwell Group, Inc. The Cardwell Group provides Healthcare Management and Healthcare Information Systems Technology Senior Executive Advisory Services. Past and current clients include companies in the medical treatment, medical diagnostics and medical information technology spaces.

---

[i] N Perlroth: Heartbleed Internet Security Flaw Used in Attack, New York Times, 18 April, 2014

[ii] Heartbleed.com website

[iii] ibid

[iv] Health Insurance Portability And Accountability Act OF 1996 (Public Law 104-191)

[v] The Health Information Technology for Economic and Clinical Health Act, abbreviated HITECH Act, was enacted under Title XIII of the American Recovery and Reinvestment Act of 2009 (Public Law 111–5)

[vi] We are not Healthcare Attorneys and this should not be construed as Legal Advice. Consult your practice's Healthcare Attorney for further information.

Qinaya WP-1405

www.qinaya.net

Qinaya
IT Architects
Design • Develop • Deploy