HITECH
Ignore at Your Own Peril

by: Darryl A. Ross, Esq.

There has been much discussion lately about data security and the new obligations imposed by the adoption of the final rules related to the **Health Information Technology for Economic and Clinical Health Act (HITECH)** and the **September 23, 2013** implementation date. For those who are already working to shore up any weak spots, good job! For those who are just starting, or worse yet, have never heard of HITECH, there is still time. First, you may want to review Wroten & Associates Spring newsletter (www.wrotenlaw.com/pdf/newsletters/2013/Spring-2013-Newsletter.pdf). Second, get moving!

WHAT IS HITECH?

HITECH was passed in 2009. It is intended to revise security and privacy requirements placed on healthcare providers and *extend those requirements* to their "business associates." As discussed in our last newsletter, a business associate includes a person or entity providing legal services involving the disclosure of Protected Health Information (PHI).

WHAT IS MATERIALLY DIFFERENT?

No matter what your knowledge base is, or your state of preparation for September's enactment date, you must be aware that under HITECH, healthcare providers may now be sanctioned for the failures of their vendors. Additionally, vendors must now become acquainted with HITECH's mandates as they are *directly subject to regulations* as a covered entity. (See 45 CFR §154.502(a).)

WHICH VENDORS MUST NOW HAVE BUSINESS ASSOCIATE AGREEMENTS?

- Data transmission service providers who may have "routine access" to the PHI.
- Data storage or document storage vendors – whether or not they view the PHI they maintain.
- Operators of portals or other interfaces created on behalf of covered entities that allow patients to share their data with the covered entity.
- Outside Counsel.

SO WHAT?

Some readers may question whether they are impacted by this. Some may say…"we have known about the need to protect PHI for years!", others may appreciate the need but think "I have more important things to think about!", some may not know about the requirements at all. HITECH is not simply about "privacy" or PHI. It's also about security, data integrity, restrictions on who may access, protocol to handle breach scenarios, and audits to make sure systems are in place. In

short, if you get nothing else from this piece, you must understand that "Privacy" and "Security" are separate and distinct concepts, and related.

SECURITY

Security refers to the systems that are used to protect PHI that is transmitted or maintained in electronic media. Every security plan should balance the following concepts:

- Confidentiality (*disclosure*): Ensuring that data is not disclosed to or made available to unauthorized persons.
- Integrity (alteration/ destruction): Data is not to be altered or destroyed without authority
- Availability (access): Data is accessible by authorized individuals and entities when needed.

IMPORTANT DEFINITIONS

Breach

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

There are three exceptions to the definition of "breach". The first exception applies to the unintentional acquisition, access or use of protected health information by a workforce member acting under the authority of a covered entity or business associate. The second exception applies to the inadvertent disclosure of protected health information from a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule. The final exception to breach applies if the covered entity or business associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information. (www.hhs.gove/ocr/privacy/hipaa).

Electronic Health Record (EHR)

A real-time patient health record with access to evidence-based decision support tools that can be used to aid clinicians in decision making. The EHR can automate and streamline a clinician's workflow, ensuring that all clinical information is communicated. It can also prevent delays in response that result in gaps in care. The EHR can also support in the collection of data for uses other than clinical care, such as billing, quality management, outcome reporting, and public health disease surveillance and reporting.

Health Information Technology (HIT)

The application of information processing involving both computer hardware and software that deals with the storage, retrieval, sharing, and use of health care information, data and knowledge for communication and decision making. Visit: www.healthit.gov/policy-researchers-implementers/glossary for more terms.

KEYS TO SUCCESSFUL IMPLEMENTATION

- Secure Network Infrastructure including sufficient firewall.
- Encryption policies including remote kill features for laptop computers, phones and tablets.
- Password reset policies.
- Automatic Logoff of computer terminals.

IMPORTANT DEADLINES

- *September 23, 2013* - Covered entities must comply with most of the new Rules' provisions.
- *April 8, 2014* – Microsoft will cease providing security updates for Windows XP3 and Office 2003. The continued use of these products will result in a compliance red-flag for any auditor.
- *September 22, 2014* – Covered entities must amend or modify to make compliant any business associate agreement in place before January 25, 2013. All business associate agreements entered into on or after January 25, 2013 must be compliant by the September 23, 2013 deadline.

About the Author:
Darryl Ross is a Shareholder with the firm of Wroten & Associates and maintains a diverse litigation practice with experience handling all aspects of civil litigation including arbitrations, complex settlements, trials (jury and court), and appeals. Mr. Ross' practice focuses on the defense of nursing homes and residential care facilities. He has successfully handled a wide variety of health care matters for public and private entities including insurance coverage issues, product liability claims, interpretation, advice and enforcement of medical staff bylaws, as well as class action litigation.

Mr. Ross is a frequent speaker at industry conferences and forums and has given numerous Webinars for clients on a variety of issues impacting their operations. Recent presentations include How to Deal with a Challenging Resident?, What Rights Do Facilities Have When They Discovery A Sex Offender is Living in the Building?, and How to Protect the QA Process.

Mr. Ross is a member of the California Association of Healthcare Facilities Legal Committee, as well as a member of the American Youth Soccer Organization's (AYSO) National Legal Commission. Mr. Ross is also a Planning Commissioner for the City of Aliso Viejo California, as well as Regional Commissioner of AYSO Region 889 located in Aliso Viejo, California.

For more information about Wroten & Associates, Inc. please visit www.wrotenlaw.com. To contact Darryl A. Ross directly please email DRoss@wrotenlaw.com.