7 Things all Law Firms (and their IT staff) need to know about HIPAA
Ian Campbell and Gavin W. Manes, Ph.D.

The information contained herein is for informational purposes only as a service to the public, and is not legal advice or a substitute for legal counsel.

HIPAA Regulations and What they Protect

Short for Health Insurance Portability and Accountability Act, HIPAA provides national standards to protect the privacy of personal health information. To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, included "Administrative Simplification" provisions that required HHS to adopt national standards for electronic health care transactions. Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information.

The new rules regarding HIPAA can now be interpreted to mandate that e-discovery vendors who handle Personal Health Information (PHI) and the tools they use to host and access PHI are required to comply with HIPAA rules under Business Associate Agreements (BAA). This is a shift from the previous situation where being under contract with an attorney or firm that had a BAA with their client afforded enough protection for any contractor and lawyers who handled PHI.

Documentation such as medical records, identifiable demographic and other information relating to the past, present, or future physical or mental health condition of an individual are all considered to be PHI, thus governed by HIPAA regulations. Law firms, hosting vendors and e-discovery software manufacturers who host or access such information need to understand and follow much stricter guidelines for data handling, access, written policies and procedures, audits recordkeeping, and more; the Final Rule officially went into effect on September 23rd, 2013.

Firms who handle PHI for their clients need to be aware of some potential pitfalls of non-compliance. It is more important now than ever to ask key questions of outside vendors about their policies, procedures and document review software platforms.

Who is Allowed Access to PHI Data and How?

Controlling access to PHI is a key component to fulfilling HIPAA regulations, so restricting and monitoring physical and remote access is necessary. Most BAAs only allow for the disclosure of PHI as necessary to perform services or for proper business management and administration. User authentication and authorization capabilities go beyond simply handing out user names and passwords. Software applications housing PHI must employ authentication mechanisms capable of validating user identity prior to the user accessing anything within the application. Further, applications must have various levels of user access controls so that user rights and privileges are aligned to sensitive functions (i.e., setting up or changing
user credentials. Applications must also be able to restrict the user's access to functionality within the program for printing, exporting and modifying the data.

Since the PHI is information that is owned by the individual, anyone in possession of PHI may receive a request from the individual for their own personal health information; at that point, any actions should follow the procedure outlined in their Business Associate Agreement. Many times, this may mean giving that person a copy of their own records. In such a scenario, there are extensive documentation requirements that can be audited by Business Associates (based on the terms of any BAA) and government entities. Use of any contractors or outsourced providers means additional layers of protection and monitoring may be necessary.

PHI data must be securely stored but also capable of being completely removed. This may require controlling or owning all parts of e-discovery processing and document review hosting and preventing 3rd party access (Non-BAA). These requirements may not allow the use of public cloud infrastructures or even colocation facilities. It may also be necessary to utilize multi-factor user authentication and secure connection pipelines to access the data. Although e-discovery service providers and firms (or their clients) must bear the onus of securing their review systems at this point, the increased requirements may lead to e-discovery processing and online review tools providing a "HIPAA-compliant” package in the future.

**Store Information in a Format That Can’t Be Read by the Naked Eye**

HIPAA regulations require that PHI be “rendered unusable, unreadable, or indecipherable by encryption using an algorithmic process to transform data into a form in which there is a low probability of assigning meaning with the use of a confidential process or key.” These encryption requirements are mandatory, whether the data is in transit or at rest (i.e., if it is sitting on a hard drive in a processing laboratory or being emailed or uploaded to an FTP site for production). HIPAA requires using a method of encryption that meets the current National Institute of Standards and Technology (NIST) standards.

Encryption introduces a substantial layer of security which must be in place at all times. As with any increase in security, there is a corresponding decrease in convenience. In any situation or case involving PHI, users should expect longer timeframes for upload and other data transmission events. There may even be heavy restrictions on email communications which would typically involve sending a link to a document held within the system to a 3rd party or using properly configured email encryption. Restrictions must be in place to ensure that any communication meets HIPAA regulations. Many of these changes will involve IT departments at law firms and vendors to help set up the appropriate keys and passwords to restrict access to PHI only to those that are aware of the rules and regulations around access.

Performing e-discovery and online review of data or documents containing PHI is also substantially affected by encryption and other security requirements. Very few current platforms offer the ability to layer encryption into the review process in such a way that fulfills the HIPAA requirements. Some document review platforms are unique in that their software has been written with HIPAA compliance in mind. Reviewers interacting with PHI must comply with rigorous individual login procedures as well as constant monitoring and controls surrounding a user’s access to the PHI information. Once a session is completed or becomes dormant, review platforms must log out automatically with no residual information being accessible.
HIPAA Policies and Procedures

E-discovery vendors handling PHI must have specific policies and procedures in place for HIPAA compliance. This means creating, implementing, and training appropriate employees on their responsibilities. It also means appointing a HIPAA Compliance Officer that serves as the point of contact and the oversight for all PHI-related matters at the company. This is no small duty as the Compliance Officer is considered responsible for any deviations from procedure and any violations of HIPAA.

Any procedures should include normal data handling as well as incident response in case of a data breach. Policies and procedures should specifically acknowledge and identify the ways that datasets including PHI should be treated differently than other documents and data as part of a company's standard operating procedure. This includes encryption requirements, monitoring, breach procedures, required documentation, and staffing.

Legacy IT Platforms and Operating Systems

The Microsoft Windows XP operating system is set to retire in April 2014; this means that Microsoft will no longer be supporting the system and creating security patches when needed. XP still maintains a global market share of approximately 40% so law firms are certainly not alone. The general rejection of Windows Vista and new hardware requirements of Windows 7 meant that many corporations and firms did not make a change. XP’s ability to run modern internet browsers (such as Chrome and Firefox) did not force the hand of business owners, causing a delay in the necessity for hardware upgrades. IT departments did not turn to alternative operating systems because of worries that internally developed applications would not work. However, security and compatibility concerns will soon require that most law firms and corporations make an operating system change.

There are several risks and issues with this retirement of XP beyond the change in user experience. External attacks will grow since Microsoft will stop providing patches to security loopholes. IT departments must spend or budget money for an upgrade as part of their 2014 plans. Legacy tools may not be compatible with a new or upgraded system; for example, many older desktop e-discovery tools do not perform well, or accurately, in modern operating systems or on modern data. Much like our consumer lives, some of these risks and issues can be mitigated by turning towards web-based platforms that can be accessed securely by browsers such as Chrome, Safari, Firefox and IE.

Logging and Monitoring Access

HIPAA’s “Information System Activity Review” implementation specification requires the implementation of procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. PHI applications must capture information system activity as well as be capable of reporting the activity for periodic review purposes. Event capturing systems must be in place to record all successful and failed access attempts to the application by user and program accounts. Review systems must monitor all access to any system utility that possesses the ability to modify sensitive data and provide reports of information system activity (e.g., failed login attempts, application alerts, etc.) sufficient to support regular review. Review platforms must provide reports (or logs) that allow...
monitoring user activity in the system, and to troubleshoot problems with specific tasks.

**Storage of PHI in Any Cloud**

Firms should be leery of storing PHI with a vendor who uses a public cloud to store PHI. Whether to use the cloud continues to be a question for many law firms and corporations. Current common uses of the cloud include file sharing (Dropbox, YouSendIt, Apple accounts), and webmail (such as Yahoo, gmail or Hotmail), all of which require only an Internet browser to interface.

Benefits of the cloud in general include massive processing power and eliminating the need for extensive IT department overhead. Drawbacks of clouds include privacy and security concerns, data disposal, and jurisdiction. Privacy and security are paramount for attorneys and most corporations, and it can be difficult to ensure that confidential information remains that way; the computers with that information are at an unknown location being administered by unknown personnel.

When it comes to HIPAA compliance, several questions come to light including the purging of data on deletion (it may be difficult to definitively state that specific information has been purged) and keeping tight control of the data at all times (may not meet an attorney’s professional obligation to do so). Jurisdiction can become a major issue since many cloud computing facilities may not be located geographically nearby the users of the data. In fact, computers with key data may be located outside the borders of the United States and are therefore not subject to the same privacy and privilege rules. Many questions need to be asked before PHI is handed over to a vendor for processing and/or hosting.

**E-Discovery Vendors Must Make Changes to Comply**

E-Discovery vendors and software developers who manage PHI in the legal and/or healthcare space are discovering that their current policies, procedures and hosting review software do not meet some of HIPAA’s requirements in their current format. Most will have to modify their business model to meet the required workflows and adopt processing and review platforms built to be able to maintain PHI security. By continuing to reinforce that the management of PHI data is “different” than the norm, law firms, corporations, and vendors can ensure that the integrity and security of an individual’s private information is held intact.

**Ian Campbell**  
**President and Co-Founder**  
**iCONECT Development, LLC**

Ian Campbell is President and Co-founder of iCONECT Development LLC, a world leader in litigation support and collaboration software. He is responsible for sales operations and business development, product lifecycle development, legal service provider (LSP) and partner relations. A key priority is cross-marketing the company’s products and services to the legal, medical, government, corporate, and insurance industries.

With more than 14 years of strategic product development in the litigation support field, Campbell has consulted on major international legal projects to help firms
achieve their long-range business goals. He is a frequent industry spokesperson, sharing his experiences and expert commentary with audiences for the American Bar Association, LegalTech, ILTA, AIIM, IQPC, Marcus-Evans, and other legal and management groups around the world.

Gavin W. Manes, Ph.D.
CEO
Avansic: E-Discovery and Digital Forensics

Dr. Gavin W. Manes is a nationally recognized expert in e-discovery and digital forensics. He is currently the CEO of Avansic, a firm that provides the legal, business, and government sectors with e-discovery, digital forensics, data preservation, and online review services. He founded Avansic in 2004 while serving as a Computer Science professor at the University of Tulsa. There he led the creation of nationally recognized research efforts in digital forensics and telecommunications security.

Dr. Manes has served as an expert witness for many legal proceedings through courtroom testimony, depositions and consulting with attorneys on data preservation issues. He has given hundreds of presentations to law firms, corporate officers, legal conferences and judges on the latest topics in e-discovery. Dr. Manes has briefed the White House, Department of the Interior, the National Security Council, and the Pentagon on computer security and forensics issues.