SmartPath Technologies, LLC HIPAA/HITECH OMNIBUS - EXPLAINED

As of September 23rd 2013, the federal government has published its long awaited final regulations implementing the HITECH Act and the HIPAA Omnibus regulation. This whitepaper will provide a very high level overview of these changes, how they will impact your facility, and what it means to you as healthcare providers. I must state as a forward to this notice that while SmartPath Technologies, LLC is one of the most well versed IT providers in the region in the intricacies of the HITECH and HIPAA Omnibus regulations, you should consult with your legal counsel on any potential HIPAA questions you may have and this document should only be construed as an overview guide. We will use the term "patient" in this document, keeping in mind they may be a "client", "consumer", or "someone provided service".

Since the original HIPAA regulations were initially put into force, the concept has been great but the reality has been that the regulations were rarely enforced. The new Omnibus regulations are, as described by the Office for Civil Rights (OCR) and the Department for Health and Human Services (HHS) as "the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented." The government has given the HHS the task of enforcing HIPAA and unlike times in the past, has also decided to allow the HHS to keep a portion of all fines levied. With the current economic state, this provides the HHS with a means to fund their department; therefore they have a vested interest in actively enforcing the regulations. Previously, the department didn't get to keep any fines levied; therefore, the regulations were not strictly enforced. It is safe to say that "we aren't in Kansas anymore" *and* "this is not your daddy's HIPAA."

The new regulations will likely require the following changes to your HIPAA policies and procedures:

- Breach notification requirements – The obligation to notify patients of a breach of their protected health information (PHI) is expanded and clarified. **All** breaches are now presumed reportable unless, after considering the following four factors, there is a "low probability of PHI compromise".
- Disclosures to health plans
- Marketing Communications
- Sale of PHI
- Childhood immunizations
- Decadents
- Copies of e-PHI
- E-Mailing PHI
- Charging for copies of e-PHI or PHI
- Research Authorizations
- Business Associate agreements
- Security of technology systems

We will explore each of these in this whitepaper in an easy to understand format.

1.) Patients are allowed to ask for and must be provided copies of their electronic medical record in electronic form capable of being read without special software and also in an HL7 or similar format that can be imported into different electronic medical record software. Providers now only have 30 days to respond to a patient's written request for records regardless of where or how records are kept. Hard copies are permitted ONLY when the individual rejects all readily reproducible e-formats.

2.) When patients pay out of pocket in full, they can instruct their provider to not share the information about their treatment with their health plan and should be offered that option. Previously, while providers could refuse to abide by any such request, the new rule *requires* physicians and other health care providers to abide by a patient's request not to disclose PHI to a health plan for those services for which the patient has paid out-of-pocket and requests the restriction. **Of all the changes made by the new rules, this change is likely to have the greatest impact on practice workflow both in terms of documentation and follow up to ensure the restriction is adhered to.** The only time this is not the case is in the rare event disclosure is required by law.

3.) If a Medicare beneficiary requests a restriction on the disclosure of PHI to Medicare for a covered service and pays out of pocket for the service, the provider cannot share the PHI with Medicare.

4.) You are not allowed to e-mail any PHI without using secure or encrypted e-mail. **If you e-mail PHI, please contact SmartPath.** We have an encrypted e-mail solution that will allow you to send PHI via e-mail. This rule includes sending PHI to people in the same organization or office as yourself. This includes X-Rays, MRIs, results, etc.

5.) You are not allowed to sell PHI or any medical records to another entity without the patient's permission. This means if you sell your practice, you cannot transfer medical records to the new ownership without each patient's approval.

6.) Previously, if you engaged a subcontractor, such as SmartPath Technologies, LLC, the subcontractor merely had to "ensure" that they would comply with your HIPAA policy. Now, those subcontractors are required to have written Business Associate agreements with your practice, and they bear the same responsibility for a PHI breach that you do. **While we have issued BA agreements to our clients, if your IT provider has not, you need to call us immediately.** A "business associate" is anyone subcontracted by you to perform services who may come in contact with PHI. This includes janitorial crews, business equipment service providers, data backup services, billing agencies, or anyone else who comes in contact with any PHI in any form. If you need a sample business associate agreement, please contact us. **This means we are be held to the same level of responsibility as you are in terms of all HIPAA requirements.** If you do not have BA agreements with these providers, you are out of compliance.

7.) All computer systems used to access PHI are required by HIPAA security rule section 164.308 to implement procedures for guarding against, detecting, and reporting malicious software. In addition, subsections A-D of this rule state

that computer systems must utilize a manufacturer supported operating system. <u>As of APRIL 14, 2014 Windows XP, Windows Server 2003, and Microsoft Office 2003 or prior versions will not be supported by their manufacturer. In addition, your firewall may not be compliant if it's older and no longer supported by it's manufacturer.</u> If you have any computers running Windows XP, you must upgrade them or replace them prior to April 14, 2014 to stay compliant. You need to schedule an appointment with us NOW to define a path forward to maintain HIPAA compliance after April 14, 2014. This also means you should have a strong perimeter firewall, antivirus software, and documented monitoring for threats. That is what we do. Call us today. Don't wait until next week. 1-270-205-4709.

8.) Your privacy notice needs to be revised to include a notice that an entity is required by law to notify affected individuals following a breach of unsecured PHI. The Notice must be revised to describe certain types of uses and disclosures that require an authorization, including disclosures of psychotherapy notes, marketing communications and the sale of PHI. The Notice must state that other uses and disclosures not described in the Notice will be made only with the individual's authorization. The Notice must make individuals aware that they can restrict certain disclosures to health plans (described above). The new rules do eliminate requirements to include information on appointment reminders, treatment alternatives, or health-related benefits or services, but do not require that information be removed if a provider chooses not to.

9.) The new rules modify the costs that may be charged to the individual for copies to include labor costs (potentially to include skilled technical labor costs for extracting electronic PHI and supply costs if the patient requests a paper copy, or if electronic, the cost of any portable media (such as a USB memory stick or a CD)), assuming state law does not set a lower reimbursement rate. The rules also clarify that physicians may impose a separate charge for creating an affidavit of completeness. All PHI supplied to a patient must include a provider signed affidavit of completeness of the records given.

10.) Under the new rules, physicians may disclose immunizations to schools required to obtain proof of immunization prior to admitting the student so long as the physicians have and document the patient or patient's legal representative's "informal agreement" to the disclosure.

11.) The new rules allow physicians to make relevant disclosures to the deceased's family and friends under essentially the same circumstances such disclosures were permitted when the patient was alive; that is, when these individuals were involved in providing care or payment for care and the physician is unaware of any expressed preference to the contrary. The new rule also eliminates any HIPAA protection for PHI 50 years after a patient's death.

12.) Providers must receive written authorization to provide marketing communication to patients. Generally speaking, the only time a provider may tell a patient about a third-party's product or

service without the patient's written authorization is when: 1) the physician receives no compensation for the communication; 2) the communication is face-to-face; 3) the communication involves a drug or biologic the patient is currently being prescribed and the payment is limited to reasonable reimbursement of the costs of the communication (no profit); 4) the communication involves general health promotion, rather than the promotion of a specific product or service; or 5) the communication involves government or government-sponsored programs. Physicians are also still permitted to give patients promotional gifts of nominal value (e.g., pamphlet).

Breach Notification Requirements

A breach is defined as the acquisition, access, use, or disclosure of PHI in a manner not permitted and that compromises the security and privacy of the protected health information.

(2)…an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the provider or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following four factors…

- HITECH Omnibus FR [78 FR 5566, January 25, 2013]

ALL breaches are now reportable unless, after completing a risk analysis applying the following four factors, it is determined there is a "very low probability of PHI compromise". The provider or business associate must consider the following four factors:

- the nature and extent of the PHI involved – issues to be considered include the sensitivity of the information from a financial or clinical perspective and the likelihood the information can be re-identified;
- the person who obtained the unauthorized access and whether that person has an independent obligation to protect the confidentiality of the information;
- whether the PHI was actually acquired or accessed, determined after conducting a forensic analysis; and
- the extent to which the risk has been mitigated, such as by obtaining a signed confidentiality agreement from the recipient.

Previously, the language regarding a breach was more subjective, stating "signifigant risk of financial, reputational, or other harm". The new rules further clarify that there is no need to have an independent entity conduct the risk assessment and indeed, no risk assessment need be conducted at all if the breach notification is made (although, providers will want to undertake an appropriate review and steps to mitigate the harm and reduce the likelihood of future breaches in any case). The new rules further confirm that the breach notification requirement may be delegated to a business associate, and providers are encouraged to coordinate with their business associates so that patients receive only one

notification of the breach. The new rules do not modify the actual reporting and timeframe requirements for Breach Notification; that is, covered entities must still adhere to requirements for individual notification, HHS notification, and where applicable media posting of the breach.

Under the new regulations, the fines **per PHI record** are regulated to be no lower than $1000.00 and no higher than $1,500,000.00. At the lowest fine level possible levied, 10 records of PHI that are wrongfully disclosed, lost, transmitted, or stored on non-supported computer systems would be $10,000.00.