

January 2013

HIPAA Business Associates (BAs)

The good news - Everyone who was a BA before the "Final" (aka Omnibus) Rule still is. The Rule contains a few additional illustrations / explanations which are summarized below:

- BAs include Health Information Organizations, E-Prescribing Gateways, and other data transmission services that "require access on a routine basis" to the PHI they transmit. What constitutes "access on a routine basis" is "fact specific."
- Personal Health Record vendors that offer their PHR on behalf of a covered entity are a BA as to those PHRs – even if they offer the same service directly to the public.
- Apparently in response to efforts of physical and electronic record storage vendors to fit in an earlier articulated "mere conduit" exception, the Office for Civil Rights (OCR) added "maintains" to the tasks a BA might perform with PHI on behalf of a Covered Entity (CE) and clarified that while "transient storage" of PHI did not create a BA relationship, less "transient" would. This makes the official definition of a BA a person (or company) who:

on behalf of such covered entity or of an organized health care arrangement ...,
but other than in the capacity of a member of the workforce of such covered entity or
arrangement, **creates, receives, maintains, or transmits protected health information...**

or who

provides, other than in the capacity of a member of the workforce of such covered entity,
legal, actuarial, accounting, consulting, data aggregation ..., management,
administrative, accreditation, or financial services... where the provision of the service
involves the disclosure of protected health information from such covered entity or
arrangement (§160.103)

- Internet Service Providers were given as a "transient storage" non-BA example.
- External researchers and Institutional Review Boards are not BAs unless they are doing something on behalf of a CE, such as de-identifying PHI or acting as a facility's Privacy Board.
- The mere purchase of malpractice insurance does not create a BA relationship, however, processing claims, conducting risk assessments and delivering related legal services may.
- Contractors that provide their services onsite at the CE's premises may be treated as "as either a member of the covered entity's workforce or a business associate."

The less good news - The prior limitation on Covered Entity civil monetary penalty liability for BA missteps has been eliminated and the combination of a "reasonable diligence" standard and the "federal common law of agency" take its place. Since the requirement of entering a written "business associate agreement" remains (and is now extended to BA subcontractors), expect great interest in revising these agreements.

BA Security Rule vs. Privacy Rule liability – The commentary to the Rule draws a distinction between direct BA liability to OCR for compliance with the Security Rule's provisions – when a BA has access to ePhi

CEs, BAs and other highlights from the HITECH (HIPAA) “Final” Rules

January 2013

– and more limited direct responsibilities under the Privacy Rule. The chart below summarizes this distinction and the available guidance thus far.

BAs (and their BAs) are directly liable for:	BAs are not responsible for:
Violations of the Security Rule if they have ePHI	Appointing a Privacy Official
Uses and disclosures of PHI in violation of the Privacy Rule and/or their BA agreement, e.g. using or accessing more than the minimum necessary information to accomplish their agreed to work	Creating a separate Notice of Privacy Practices
Keeping records and cooperating with OCR investigations and compliance reviews	Providing a copy of the PHI in their possession in response to a request by the patient (unless they agree to this in the BA Agreement)
Providing information in response to an individual’s request for a copy of his / her PHI (to the individual or the CE as specified in the BA Agreement)	
Failing to provide notice of breaches of unsecured PHI to the CE	
Failing to enter into BA agreements with subcontractors that meet these same requirements	

A notable omission – OCR did not finalize its proposed rule, pending since 2011, relating to the respective responsibilities of BAs and CEs in responding to patient requests for an accounting of disclosures. Most existing BA agreements probably have provisions relating to this responsibility.

Beyond BAs -- also of interest in the Rules:

Marketing Communications - CEs (and their BAs) may not communicate - without first obtaining a written HIPAA compliant authorization - with patients on behalf of third parties that provide the CE or BA with financial remuneration in exchange for the communication. The authorization must tell the patient about the remuneration and his/her right to revoke the authorization at any time. Being paid to take care of patients is not “financial remuneration”. CEs may still communicate – without authorization – about their own facilities and capabilities, even if those communications are financially supported by a third party. Existing exceptions for face-to-face communications and promotional gifts of a “nominal amount” – even when paid for by a third party - were continued. Refill reminders for drugs or biologics the patient is already on or generic equivalents are also exceptions from the prior authorization requirement as long as the remuneration is “reasonably related” to the costs of the communication.

“Sale of Protected Information” - Requires a prior written authorization by the patient. Pages and pages were devoted to defining what is not a “sale”. If someone offers something, whether cash or in kind, in exchange for PHI, just say “no” unless there is a prior patient authorization included in the transaction or the amount involved is so large that it justifies hiring an attorney to find an applicable “exception”.

PHI of Decedents - The protection of your PHI will now end 50 years after you die. CEs will also be permitted (but not required) to disclose your PHI to “family members and others who were involved in [your] care or payment for care ... prior to death” unless you express a preference otherwise before you die. [Before implementing any policy change, check applicable state laws which may be more stringent about release of information in these circumstances.]

Student Immunizations - Health Care providers will be able to disclose child immunization records to schools based on an oral agreement by the parent or an emancipated child – rather than the previously required written authorization. The parent’s “agreement” must be documented in the provider’s records,

January 2013

but the method of documentation is up to the provider. In states where such disclosures are required by law, no agreement is necessary.

Research Authorizations - Authorizations may now include provisions authorizing the use of the patient's data in related or future studies, so long as psychotherapy notes are not involved. (Psychotherapy notes still require a separate, stand-alone authorization.)

Fundraising - Providers may still use PHI to direct fundraising solicitations to patients so long as they include "clear and conspicuous opt out" options for further communications. Providers retain flexibility about the "opt out" methods they employ so long as the patient does not incur more than nominal expense or effort to exercise them. A somewhat heightened standard of care towards not sending further communications to those that have "opted out" was adopted. Importantly, the final rule allows for the first time the use of the patient's treating department, treating physician and outcome information for fundraising purposes. The CE's practice must match what's in its Notice of Privacy Practices.

Notice of Privacy Practices - Certain statements about psychotherapy notes (if the CE maintains such records), marketing, authorizations, restricting information to health plans when the patient pays in full, breach notifications and sales of PHI must be included in each provider's NPP. The requirements for posting and distributing the new NPP by provider CEs differ from distribution requirements for health plans.

Restricting Disclosures By Paying In Full - Patients have the right to restrict disclosures to their health plan(s) about receiving certain services so long as they pay the provider in full and request that the information be withheld. The multitudes of practical problems with responding to such requests are acknowledged in the commentary.

Copies of the EMR - Providers with EMRs must provide "machine readable copies" to patients of all electronic records in the form or format requested or agreed to by the patient. The actual costs of labor used in creating the copy(ies), postage /delivery and any associated media may be charged, but not a standard "retrieval" fee. (HIPAA preempts more limited rights of access and the fees found in some state laws, unless the fee calculated under the State provisions is less.) This includes requests for copies to be sent to third parties. Copies must be provided within 30 days (with one 30 days extension possible).

Breach Notification - Breaches are presumptively reportable to OCR, unless the CE does a risk assessment which is described somewhat differently than in the past. Instead of assessing the "risk of harm" to the individual(s) whose information is involved the focus has shifted to measuring the "probability" that the PHI has been "compromised". Four specific factors must be included in this probability assessment - (1) nature and extent of the information involved, (2) who received or used the PHI, (3) whether the information was actually used / acquired, and (4) the extent to which the risk to the PHI has been mitigated.

Genetic Information - The use of such information for underwriting is now prohibited by all "health plans" that are covered by HIPAA, except issuers of long term care policies.

Last of all - the final Rules contain several references to obligations under the Civil Rights laws regarding communication to those with disabilities and those with limited English proficiency. Providers should consider how the various HIPAA notices to patients (e.g. Notice of Privacy Practices, Authorizations, Notice of Breach) are included in their compliance efforts for those statutes as well.

When? Although the rule has an "Effective Date" of March 26, 2013, the "Compliance Date" is September 23, 2013. BA relationships that are (1) in existence on the publication date (January 25, 2013) and (2) are not renewed or modified between the "Effective" and the "Compliance" dates are grandfathered for up to one year (September 23, 2014). (§164.532(f)) "Evergreen" contracts are eligible for the extended "transition period". Oral agreements are not.