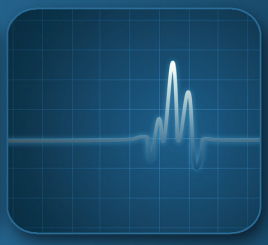
Polsinelli Shughart

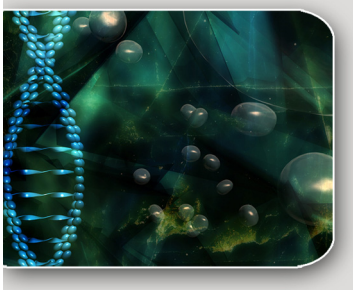




HEALTH CARE LAW | IN THE NEWS

February 2013

Changes Affecting Who is a Business Associate and New Business Associate Obligations

Breaking Down the HIPAA Changes: Part 2 of our 5-Part Series



Some of the most significant changes that were made by the final HIPAA omnibus rule, published on January 25, 2013, in the *Federal Register* (the Final Rule) relate to the expanded definition of HIPAA Business Associate (BA) and newly imposed legal obligations on BAs. The Final Rule also included an expansion of the elements that are required to be included in Business Associate Agreements (BAAs). The purpose of this e-alert is to provide a comprehensive look at: (i) the expansion of, clarifications to, and explicit inclusion of certain entities in the definition of a BA; (ii) the direct liability that the Final Rule imposes on BAs for noncompliance; and (iii) the elements that the Final Rule requires be included in BAAs and the compliance dates related thereto.

I. Expansion of, Clarifications to, and Explicit Inclusions in the Definition of BA

The Final Rule included several additions and clarifications to the HIPAA definition of BA. Identifying persons and entities which meet the definition of BA is important because

the Final Rule clarified that a person or entity becomes a BA by meeting the definition of a BA and by creating, receiving, maintaining, or transmitting protected health information on behalf of a Covered Entity, not by contracting with the Covered Entity and entering into a BAA. Moreover, the type of protected health information involved does not matter; if the information is tied to a Covered Entity, it is considered protected health information by definition (even if it is, for example, strictly limited to demographic information). Whether or not a person or entity is a BA is significant because as will be further discussed below, BAs have direct liability under the Final Rule for not complying with certain HIPAA requirements.

A. HIOs, e-Prescribing Gateways, PHRs, and Entities that Maintain Protected Health Information

Pursuant to the Final Rule, the following types of entities are now considered BAs: (i) health information organizations, e-prescribing gateways, or other persons or entities that provide data transmission services with respect to protected health information to a Covered Entity and that require routine access to such protected health information; (ii) a person or entity that offers a personal health record (PHR) to one or more individuals on behalf of a Covered Entity; and (iii) persons or entities that maintain protected health information, even if the person or entity does not actually view the protected health information.

The Final Rule explained that when interpreting the term "routine access," the often relied upon "conduit exception" will be construed very narrowly. Historically, entities that act as a temporary conduit for protected health information, such as the United States Postal Service, UPS, other courier services, and their electronic equivalents, such as internet service providers, have been excluded from the BA definition. While these entities will continue to be excluded from the definition of BA, those companies that *maintain* protected health information for a Covered Entity, but do not actually view the protected health information or only do so on a random or infrequent basis, such as a storage company or a cloud-computing company, will now meet the definition of a BA.

The Final Rule also clarified that all vendors of PHRs are not automatically considered BAs. Rather, the vendor of the PHR must offer the PHR on behalf of the Covered Entity health care provider or health plan. This means that some vendors of PHRs may wear two separate hats when it comes to complying with HIPAA – when the vendor provides the PHR on behalf of a Covered Entity, the vendor of PHR would be subject to the HIPAA requirements and the HIPAA Breach Notification Rule. However, when the vendor of PHR does not offer its services on behalf of a Covered Entity, the vendor of PHR is not subject to HIPAA; rather, it must comply with the breach notification requirements set forth by the Federal Trade Commission.

B. Subcontractors of BAs

The Final Rule expands the definition of BA to include subcontractors of a BA (i.e., those persons that perform functions for or provide services to a BA involving protected health information for purposes of the BA fulfilling its obligations to the Covered Entity with which it has contracted). As such, the definition creates a BA relationship chain which starts with the Covered Entity and a primary BA and flows down through subcontractor BAs, with each subcontractor BA having contractual obligations (in addition to the legal obligations of a BA)

to the party immediately preceding such party in the BA relationship chain. Legal and contractual obligations of a BA are discussed in more detail below. The Final Rule clarified that disclosures of protected health information that a BA makes to a subcontractor for purposes of the BA's own management and administration or to carry out the BA's legal responsibilities do not create a BA subcontractor relationship.

C. Other Modifications and Clarifications

i. Patient Safety Activities. The Final Rule adds patient safety activities to the list of functions and activities that a person or entity may undertake as a BA. Related to this change, the Final Rule also added "patient safety activities" to the HIPAA definition of "health care operations." This modification makes it clear that entities that perform patient safety activities on behalf of a Covered Entity, such as Patient Safety Organizations, must have a BAA in place with the Covered Entity. Further, when a committee is formed by a Covered Entity to perform patient safety activities and the committee includes persons who are not workforce members of the Covered Entity, the Covered Entity should have BAAs in place with the non-workforce members.

ii. Banking and Financial Institutions. The Final Rule explained that banking and financial institutions are not BAs with respect to payment process activities (as identified in § 1179 of HIPAA) (e.g., activities that constitute authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments for health care or health plan premiums). However, where a bank or financial institution provides activities which go beyond the exempted activities, such as performing accounts receivable functions on behalf of a health care provider, then the bank or financial institution will be considered a BA.

iii. Health Plan Products and Other Insurance. The Final Rule clarified that when a Covered Entity purchases a health plan product or other insurance (such as professional liability insurance) from an insurer, the insurer is not a BA of the Covered Entity merely for purposes of providing the insurance. However, if the insurer performs a function on behalf of the Covered Entity that involves protected health information (such as providing legal services for the Covered Entity), then the insurer becomes a BA of the Covered Entity.

iv. Hybrid Entities. Under the Final Rule, if an entity is a hybrid entity (i.e., it performs both HIPAA covered and non-covered functions) and the component of the hybrid entity providing non-covered functions provides BA functions for the division that provides covered functions, the component providing non-covered functions must be included as part of the covered division and thus subject to and directly liable for HIPAA compliance.

II. BAs' Direct Liability Under the Final Rule

Under the Final Rule, BAs are directly liable for:

- The impermissible use and disclosure of protected health information. A BA makes an impermissible use or disclosure of protected health information when the BA uses or discloses protected health information for any reason or purpose other than as is allowed by the BAA. Further, a BA is not making a

permitted use or disclosure if it does not apply the minimum necessary standards, where appropriate.

- A failure to provide notifications of a breach to the Covered Entity. The details of the BA's obligations to the Covered Entity related to breach notification are set forth in the BAA.

- A failure to provide access to a copy of electronic protected health information to either the Covered Entity, the individual, or the individual's designee, as specified in the BAA.

- A failure to disclose protected health information where required by the Secretary of the United States Department of Health and Human Services (HHS) to investigate or determine the BA's compliance with the HIPAA rules.

- A failure to provide an accounting of disclosures to the Covered Entity in order to allow the Covered Entity to comply with its accounting of disclosures obligations to an individual. The details of such obligations should be set forth in the BAA.

- A failure to comply with the requirements of the Security Rule. The Security Rule now applies to BAs. This means that BAs must have administrative, physical, and technical safeguards in place, in accordance with 45 C.F.R. §§ 164.306, 164.308, 164.310, 164.312, and 164.314), as well as the policies and procedures and documentation requirements found in 45 C.F.R. § 164.316. When fulfilling their obligation to comply with the Security Rule, BAs may use the same process as Covered Entities. For instance, in deciding which security measures to implement, a BA may take into consideration its size, capabilities, the costs of the specific security measures, and the operational impact. BAs should note that as part of their compliance with the administrative safeguards, BAs must perform their own risk analyses, establish a risk management program, and designate a security officer, as well as have in place written policies and procedures, conduct employee training, and document compliance with the requirements.

- Failure to enter into BAAs with subcontractors that create or receive protected health information on their behalf.

While the Final Rule imposes direct liability on BAs for the foregoing, it does not impose direct liability for BAs with respect to all requirements of the HIPAA Privacy Rule. Rather, BAs will remain contractually liable to Covered Entities for any other requirements appearing in the BAA which are not described above.

III. BAAs: Required Provisions Under the Final Rule and the Compliance Date

The Final Rule included an expansion of the elements which must be contained in the BAA. Under the Final Rule, all BAAs must include provisions which require the BA to:

- Comply with the Security Rule.

- Report breaches of Unsecured Protected Health Information to Covered Entities.

- Obtain satisfactory assurances (in the form of a written BAA) from any subcontractor that creates or receives protected health information on behalf of

the BA that the subcontractor agrees to the same restrictions and conditions that apply to the BA with respect to such information. From a practical perspective, this means that each BAA in the BA/subcontractor relationship chain must be as stringent or more stringent as the BAA above it with respect to the permissible uses and disclosures of protected health information.

- To the extent the BA is to carry out a Covered Entity's obligations under the Privacy Rule, the BA must comply with the requirements of the Privacy Rule that apply to the Covered Entity in the performance of such obligations.

It should be noted that the Final Rule removes the requirement that Covered Entities report to HHS when a Covered Entity is aware of noncompliance by a BA, the BA is unable to cure the breach, and termination of the BAA is not feasible. This is a provision that previously appeared in BAAs.

While compliance with most of the requirements of the Final Rule is required by September 23, 2013, the Final Rule contains a transition period for HIPAA-compliant BAAs that were already in effect prior to January 25, 2013. If any such BAA is not renewed or modified between March 26, 2013, and September 23, 2013, it will "grandfather" in and the Covered Entity and BA may operate under the existing BAA for up to one (1) year beyond the compliance date (i.e., September 23, 2014). The Final Rule also clarified that BAAs which contain evergreen clauses (i.e., they renew automatically and indefinitely) would be eligible for the transition period and would not terminate when the BAA automatically rolled over. New BA relationships and the resulting BAAs entered into after January 25, 2013 but prior to September 23, 2013, must comply with the Final Rule requirements prior to September 23, 2013, and are not subject to the transition period. As a starting point, HHS released a new, updated version of its sample BAA (click here to view). However, please note that HHS provides no guarantee that its sample BAA fully complies with the provisions of the Final Rule; thus, entities should evaluate and tailor BAAs to meet their specific needs.

In conclusion, because the Final Rule imposes direct liability on BAs, it is now more important than ever for a Covered Entity to identify persons and entities that meet the HIPAA definition of a BA and for any such persons and entities to confirm a compliant BAA is in place. Further, it is critical that BAs fully understand their duties and obligations under HIPAA.

Stayed tuned for the next e-alert in this five-part series, on the modifications to the Breach Notification Rule, which will be circulated on Friday, February 8, 2013.

For More Information

For any questions on the topics covered in this Alert, please contact:

- Tom O'Donnell at todonnell@polsinelli.com or (816) 360-4173
- Erin Dunlap at edunlap@polsinelli.com or (314) 622-6661
- Rebecca Frigy at rfrigy@polsinelli.com or (314) 889-7013
- Matt Murer at mmurer@polsinelli.com or (312) 873-3603

Matthew J. Murer
Practice Area Chair
Chicago
312.873.3603
mmurer@polsinelli.com

Colleen M. Faddick
Practice Area Vice-Chair
Denver
303.583.8201
cfaddick@polsinelli.com

Bruce A. Johnson
Practice Area Vice-Chair
Denver
303.583.8203
brucejohnson@polsinelli.com

Alan K. Parver
Practice Area Vice-Chair
Washington, D.C.
202.626.8306
aparver@polsinelli.com

Janice A. Anderson
Chicago
312.873.3623
janderson@polsinelli.com

Douglas K. Anning
Kansas City
816.360.4188
danning@polsinelli.com

Jane E. Arnold
St. Louis
314.622.6687
jarnold@polsinelli.com

Jack M. Beal
Kansas City
816.360.4216
jbeal@polsinelli.com

Cynthia E. Berry
Washington, D.C.
202.626.8333
ceberry@polsinelli.com

Mary Beth Blake
Kansas City
816.360.4284
mblake@polsinelli.com

Gerald W. Brenneman
Kansas City
816.360.4221
gbrenneman@polsinelli.com

Teresa A. Brooks
Washington, D.C.
202.626.8304
tbrooks@polsinelli.com

Jared O. Brooner
St. Joseph
816.364.2117
jbrooner@polsinelli.com

Anika D. Clifton
Denver
303.583.8275
aclifton@polsinelli.com

Anne M. Cooper
Chicago
312.873.3606
acooper@polsinelli.com

Lauren P. DeSantis-Then
Washington, D.C.
202.626.8323
ldesantis@polsinelli.com

S. Jay Dobbs
St. Louis
314.552.6847
jdobbs@polsinelli.com

Thomas M. Donohoe
Denver
303.583.8257
tdonohoe@polsinelli.com

Cavan K. Doyle
Chicago
312.873.3685
cdoyle@polsinelli.com

Meredith A. Duncan
Chicago
312.873.3602
mduncan@polsinelli.com

Erin Fleming Dunlap
St. Louis
314.622.6661
edunlap@polsinelli.com

Fredric J. Entin
Chicago
312.873.3601
fentin@polsinelli.com

Jennifer L. Evans
Denver
303.583.8211
jevans@polsinelli.com

T. Jeffrey Fitzgerald
Denver
303.583.8205
jfitzgerald@polsinelli.com

Michael T. Flood
Washington, D.C.
202.626.8633
mflood@polsinelli.com

Kara M. Friedman
Chicago
312.873.3639
kfriedman@polsinelli.com

Rebecca L. Frigy
St. Louis
314.889.7013
rfrigy@polsinelli.com

Asher D. Funk
Chicago
312.873.3635
afunk@polsinelli.com

Randy S. Gerber
St. Louis
314.889.7038
rgerber@polsinelli.com

Mark H. Goran
St. Louis
314.622.6686
mgroan@polsinelli.com

Linas J. Grikis
Chicago
312.873.2946
lgrikis@polsinelli.com

Lauren Z. Groebe
Kansas City
816.572.4588
lgroebe@polsinelli.com

Brett B. Heger
Dallas
314.622.6664
bheger@polsinelli.com

Jonathan K. Henderson
Dallas
214.397.0016
jhenderson@polsinelli.com

Margaret H. Hillman
St. Louis
314.622.6663
mhillman@polsinelli.com

Jay M. Howard
Kansas City
816.360.4202
jhoward@polsinelli.com

Cullin B. Hughes
Kansas City
816.360.4121
chughes@polsinelli.com

Sara V. Iams
Washington, D.C.
202.626.8361
siams@polsinelli.com

George Jackson, III
Chicago
312.873.3657
gjackson@polsinelli.com

Lindsay R. Kessler
Chicago
312.873.2984
lkessler@polsinelli.com

Joan B. Killgore
St. Louis
314.889.7008
jkillgore@polsinelli.com

Anne. L. Kleindienst
Phoenix
602.650.2392
akleindienst@polsinelli.com

Chad K. Knight
Dallas
214.397.0017
cknight@polsinelli.com

Sara R. Kocher
St. Louis
314.889.7081
skocher@polsinelli.com

Dana M. Lach
Chicago
312.873.2993
dlach@polsinelli.com

Jason T. Lundy
Chicago
312.873.3604
jlundy@polsinelli.com

Ryan M. McAteer
Los Angeles
310.203.5368
rmcateer@polsinelli.com

Jane K. McCahill
Chicago
312.873.3607
jmccahill@polsinelli.com

Ann C. McCullough
Denver
303.583.8202
amccullough@polsinelli.com

Ryan J. Mize
Kansas City
816.572.4441
rmize@polsinelli.com

Aileen T. Murphy
Denver
303.583.8210
amurphy@polsinelli.com

Hannah L. Neshek
Chicago
312.873.3671
hneshek@polsinelli.com

Gerald A. Niederman
Denver
303.583.8204
gniederman@polsinelli.com

Edward F. Novak
Phoenix
602.650.2020
enovak@polsinelli.com

Thomas P. O'Donnell
Kansas City
816.360.4173
todonnell@polsinelli.com

Aaron E. Perry
Chicago
312.873.3683
aperry@polsinelli.com

Mitchell D. Raup
Washington, D.C.
202.626.8352
mraup@polsinelli.com

Daniel S. Reinberg
Chicago
312.873.3636
dreinberg@polsinelli.com

Donna J. Ruzicka
St. Louis
314.622.6660
druzicka@polsinelli.com

Charles P. Sheets
Chicago
312.873.3605
csheets@polsinelli.com

Kathryn M. Stalmack
Chicago
312.873.3608
kstalmack@polsinelli.com

Leah Mendelsohn Stone
Washington, D.C.
202.626.8329
lstone@polsinelli.com

Chad C. Stout
Kansas City
816.572.4479
cstout@polsinelli.com

Steven K. Stranne
Washington, D.C.
202.626.8313
sstranne@polsinelli.com

William E. Swart
Dallas
214.397.0015
bswart@polsinelli.com

Tennille A. Syrstad
Denver
312.873.3661
etremmel@polsinelli.com

Emily C. Tremmel
Chicago
303.583.8263
tysrstad@polsinelli.com

Andrew B. Turk
Phoenix
602.650.2097
abturk@polsinelli.com

Joseph T. Van Leer
Chicago
312.873.3665
jvanleer@polsinelli.com

Andrew J. Voss
St. Louis
314.622.6673
avoss@polsinelli.com

Joshua M. Weaver
Dallas
214.661.5514
jweaver@polsinelli.com

Emily Wey
Denver
303.583.8255
ewey@polsinelli.com

Mark R. Woodbury
St. Joseph
816.364.2117
mwoodbury@polsinelli.com

Janet E. Zeigler
Chicago
312.873.3679
jzeigler@polsinelli.com

Additional Health Care Professionals

Julius W. Hobson, Jr.
Washington, D.C.
202.626.8354
jhobson@polsinelli.com

Harry Sporidis
Washington, D.C.
202.626.8349
hsporidis@polsinelli.com

About Polsinelli Shughart's Health Care Group

The Health Care group has vast national resources and strong Washington, D.C. connections. With highly trained, regulatory-experienced attorneys practicing health care law in offices across the country, we are familiar with the full range of hospital-physician lifecycle and business issues confronting hospitals today. A mix of talented, bright, young attorneys and seasoned attorneys, well known in the health care industry, make up our robust health care team.

Polsinelli Shughart is the 10th largest health care law firm in the nation, according to the 2010 rankings from Modern Healthcare magazine. The publication annually ranks law firms based on their total membership in the American Health Lawyers Association. With one of the fastest-growing health care practices in the nation, Polsinelli Shughart has the depth and experience to provide a broad spectrum of health care law services.

About Polsinelli Shughart

With more than 600 attorneys, Polsinelli Shughart is a national law firm and a recognized leader in the areas of health care, financial services, real estate, life sciences and technology, energy and business litigation. Serving corporate, institutional and individual clients, our attorneys build enduring relationships by providing practical, business-driven legal advice with a commitment to helping clients achieve their objectives. The firm has offices in Chicago; Dallas; Denver; Kansas City; Los Angeles; New York; Phoenix; St. Louis; Washington, D.C.; and Wilmington. In California, Polsinelli Shughart LLP.

The firm can be found online at www.polsinelli.com.

Polsinelli Shughart PC. In California, Polsinelli Shughart LLP.

About This Publication

If you know of anyone who you believe would like to receive our e-mail updates, or if you would like to be removed from our e-distribution list, please contact us via e-mail at Interaction@polsinelli.com.

Polsinelli Shughart provides this material for informational purposes only. The material provided herein is general and is not intended to be legal advice. Nothing herein should be relied upon or used without consulting a lawyer to consider your specific circumstances, possible changes to applicable laws, rules and regulations and other legal issues. Receipt of this material does not establish an attorney-client relationship.

Polsinelli Shughart is very proud of the results we obtain for our clients, but you should know that past results do not guarantee future results; that every case is different and must be judged on its own merits; and that the choice of a lawyer is an important decision and should not be based solely upon advertisements.

Polsinelli Shughart PC. In California, Polsinelli Shughart LLP.

Polsinelli Shughart® is a registered trademark of Polsinelli Shughart PC.