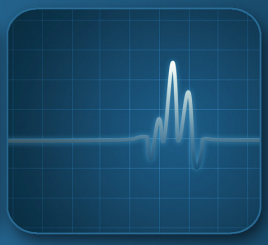
Polsinelli Shughart

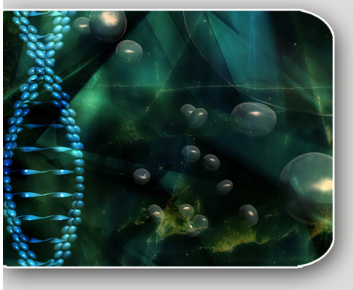




HEALTH CARE LAW IN THE NEWS

February 2013

Modifications to the Breach Notification Rule

Breaking Down the HIPAA Changes: Part 3 of our 5-Part Series



The final HIPAA omnibus rule published in the *Federal Register* on January 25, 2013 (the Final Rule) made a few changes to the Breach Notification Rule, which was implemented by an interim final rule shortly after the passage of the Health Information Technology for Economic and Clinical Health Act (HITECH Act) and became effective September 23, 2009 (the Interim Final Rule). Most significantly, the Final Rule altered the definition of "breach" – which will reshape how Covered Entities and Business Associates determine their breach notification obligations in the future.

The purpose of this e-alert is to (i) discuss the Final Rule's modifications to the Breach Notification Rule; and (ii) suggest some action items to comply with the Breach Notification Rule (as modified by the Final Rule) by September 23, 2013 -- the required compliance date.

I. Modifications to the Breach Notification Rule

A. Definition of "Breach"

One of the most notable changes made by the Final Rule to the Breach Notification Rule (as implemented by the Interim Final Rule), is a change to the definition of "breach." Under the Final Rule, there is now a presumption that an impermissible use or

disclosure of protected health information (PHI) constitutes a breach, and the "risk of harm standard" previously implemented in the Interim Final Rule is replaced with a more objective test of whether PHI has been "compromised."

Under the Final Rule, the term "breach" is defined as the acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule which compromises the security or privacy of such information. There are three exceptions to this definition (all of which remain unchanged by the Final Rule):

i. *Any unintentional acquisition, access or use of PHI by a workforce member or individual acting under the authority of a Covered Entity or a Business Associate if such access or use was made in good faith and within the scope of authority and does not result in a further unauthorized use or disclosure;*

ii. *Any inadvertent disclosure by a person who is authorized to access PHI at a Covered Entity or Business Associate to another person authorized to access PHI at the same Covered Entity or Business Associate, and the information is not further used or disclosed in an impermissible manner; and*

iii. *A disclosure of PHI where a Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.*

Whereas, under the Interim Final Rule, the phrase "compromises the security or privacy of [PHI]" means "poses a significant risk of financial, reputational, or other harm to the individual" (e.g., the risk of harm standard) and Covered Entities and Business Associates are required to perform a risk assessment to determine if there is such a risk of harm to the individual, under the Final Rule, the United States Department of Health and Human Services (HHS) removed the risk of harm standard and added language to the definition of "breach" to clarify that an unauthorized use or disclosure of PHI that does not meet one of the three exceptions is "presumed to be a breach," unless the Covered Entity or Business Associate, as applicable, can demonstrate that there is a "low probability that the PHI has been compromised." The reason for this change stems from HHS' concerns that the risk of harm standard was too subjective, leading to inconsistent interpretations and "setting a much higher threshold for breach notification" than it intended to set.

In order to ensure a more uniform interpretation and application of the regulations, in the Final Rule, HHS also (i) modified the risk assessment process to focus more objectively on the risk that the PHI has been compromised (as opposed to the risk of harm to the individual); and (ii) identified four factors that a Covered Entity or Business Associate must consider when performing a risk assessment to determine if the PHI has been "compromised":

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification. For example, could the information be used by an unauthorized recipient in a manner adverse to the individual or otherwise used to further the unauthorized recipient's own interests?

2. The unauthorized person who used the PHI or to whom the disclosure was made. For example, was the PHI impermissibly disclosed to another entity obligated to abide by HIPAA? If so, there may be a lower probability that the PHI has been compromised because the recipient of the PHI is obligated to protect the privacy and security of the PHI in a similar manner as the disclosing entity.

3. Whether the PHI was actually acquired or viewed. For example, if a laptop computer was stolen and later recovered and a forensic analysis shows that the PHI on the computer was never accessed or otherwise compromised, the entity could determine that the information was not actually acquired by the unauthorized individual even though the opportunity existed.

4. The extent to which the risk to the PHI has been mitigated. For example, did the disclosing entity obtain the recipient's satisfactory assurances that the information will not be further used or disclosed [through a confidentiality agreement or similar means] or will be returned or destroyed?

HHS emphasizes that a Covered Entity or Business Associate must evaluate all of these factors before making a determination about the probability of the risk that the PHI has been compromised, and clarified that other factors may also be considered in the risk assessment when necessary. HHS expects the risk assessment to be documented, thorough and completed in good faith, and the conclusions reached must be reasonable.

It is worth noting, however, that a Covered Entity or Business Associate, as applicable, has the discretion to provide the required notifications following an impermissible use or disclosure of PHI without performing a risk assessment. Because the Final Rule creates the presumption that a breach has occurred following every impermissible use or disclosure of PHI, entities may decide to make required breach notifications without evaluating the probability that the PHI has been compromised.

Ultimately, Covered Entities and Business Associates have the burden to prove that all notifications were provided or that an impermissible use or disclosure did not constitute a breach (by demonstrating through a risk assessment that there was a "low probability that the PHI had been compromised"). Covered Entities and Business Associates must maintain documentation sufficient to meet that burden of proof.

In the Final Rule, HHS also removed the exception for limited data sets that do not contain any dates of birth and zip codes from the definition of "breach." This exception was abandoned in favor of the more comprehensive risk assessment described above. According to HHS, the factors set forth above (particularly the type of PHI involved and the identity of the recipient of the PHI) are "suited to address the probability that a data set without direct identifiers has been compromised following an impermissible use or disclosure." Although HHS anticipates that entities may reasonably determine that there is a low probability of risk that a limited data set that does not contain any dates of birth and zip codes has been compromised, it is still a fact-specific determination to be made based on the circumstances of the impermissible use or disclosure.

B. Definition of "Unsecured Protected Health Information"

The Final Rule only made a few technical changes to the definition of "unsecured protected health

information" (e.g., replacing the term "unauthorized individuals" with "unauthorized persons"). However, in the preamble to the Final Rule, HHS pointed to its *Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable or Indecipherable to Unauthorized Individuals* (HHS Guidance) and emphasized that encryption and destruction are the only two methods for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals – or "secured" – and thus, exempt from the breach notification requirements. HHS strongly encourages Covered Entities and Business Associates to take advantage of this safe harbor provision of the Breach Notification Rule by encrypting PHI pursuant to the HHS Guidance.

C. Notice Requirements

The Final Rule made very few substantive changes to the notice requirements (*i.e.*, timing, content and method). One such change was the clarification that a Covered Entity is required to notify HHS of all breaches of unsecured PHI affecting fewer than 500 individuals not later than 60 days after the end of the calendar year in which the breaches were "discovered" – not in which the breaches "occurred." HHS recognized that there may be situations where, despite having reasonable and appropriate breach detection systems in place, a breach may go undetected for some time.

In the preamble, HHS also made a few noteworthy comments on the notice requirements in connection with Business Associates, including:

Covered Entities ultimately maintain the obligation to notify affected individuals of a breach, although a Covered Entity is free to delegate the responsibility to a Business Associate responsible for the breach or to another of its Business Associates. If there is such a delegation, the Business Associate Agreement should bind the Business Associate to the same breach notification obligations that the Covered Entity has under the Breach Notification Rule.

Covered Entities and Business Associates should consider which entity is in the best position to provide notice to the individual, which may depend on various circumstances such as the functions the Business Associate performs on behalf of the Covered Entity and which entity has the relationship with the individual.

Covered Entities are encouraged to discuss and define in their Business Associate Agreements the requirements regarding how and when a Business Associate should notify the Covered Entity (and who specifically should be notified) of a potential breach.

II. Action Items to Comply with the Breach Notification Rule

In the 180 day period between the effective date of the Final Rule (March 23, 2103) and the compliance date of the Final Rule (September 23, 2013), Covered Entities and Business Associates should comply with the breach notification requirements under the Interim Final Rule. Compliance with the Breach Notification Rule, as modified by the Final Rule, is required by September 23, 2013. The following is a list of suggested action items for Covered Entities and Business Associates to take to ensure compliance with the Final Rule beginning on September 23, 2013:

⇒ Evaluate whether or not encryption is feasible for all PHI possessed by the entity – including PHI at

rest and in transit. Again, if all PHI is encrypted, then there are no breach notification requirements following an impermissible use or disclosure.

⇒ Review and, if necessary, revise Business Associate Agreements to reflect the requirements of the Breach Notification Rule, as modified by the Final Rule, and to specify (among other items) which entity is responsible for notifying affected individuals and how and when the Business Associate should notify the Covered Entity (and who specifically should be notified) of a potential breach.

⇒ Implement or revise policies and procedures to reflect the requirements of the Breach Notification Rule, as modified by the Final Rule. Covered Entities and Business Associates must ensure that when they are evaluating the risk of an impermissible use or disclosure, they consider all of the factors set forth above and other factors if necessary. However, Covered Entities and Business Associates should continue to have a process in place to mitigate the harmful effects of potential breaches despite the elimination of the "risk of harm standard."

⇒ Train and educate workforce members and other agents on the Breach Notification Rule, as modified by the Final Rule, particularly on the importance of prompt reporting of potential impermissible uses or disclosures of PHI. Note: HHS declined to adopt the notion that Covered Entities are deemed to have "discovered" a breach only when management is notified of the breach, so it is important that workforce members at all levels understand the breach notification requirements and their related obligations.

There are real consequences if a Covered Entity or Business Associate does not comply with the Breach Notification Rule. Failure to comply with the Breach Notification Rule is in and of itself a HIPAA violation which is subject to HHS enforcement actions and civil money penalties. For this reason, it is crucial that Covered Entities and Business Associate clearly understand their obligations under the Breach Notification Rule and have appropriate polices and procedures in place to promote their compliance with the Breach Notification Rule.

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

Serving corporations, institutions, entrepreneurs, and individuals, our attorneys build enduring relationships by providing legal counsel informed by business insight to help clients achieve their objectives. This commitment to our clients' businesses has helped us become the fastest-growing, full-service law firm in America*. With more than 600 attorneys in 16 cities, our national law firm is a recognized leader in the industries driving our growth, including health care, financial services, real estate, life sciences and technology, energy and business litigation. The firm can be found online at www.polsinelli.com. Polsinelli Shughart PC. In California, Polsinelli Shughart LLP.

* *Inc.* Magazine, September 2012

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.