MURTHA MEANS MORE information

February 1, 2013 **Health Care Update**

THE HITECH ACT GETS FINAL REGULATIONS

The HITECH Act of 2008 made significant changes to the HIPAA Privacy and Security rules, extending most of the obligations of covered entities to their business associates and subcontractors. The rulemaking process has gone through several stages since then, so the final regulations may not come as a major surprise. However, you will have to make some changes. The regulations become effective March 26, 2013 but entities have until September 22, 2013 to comply. You don't need to revise existing business associate agreements until September 22, 2014, but you probably need to add some by September 2013. The definition of "business associate" will now include a health information organization, an e-prescribing gateway, a data transmission or personal health record provider. If you haven't made any revisions to your BAAs since HITECH, now would be an ideal time to have them reflect the burdens placed on business associates and their subcontractors.

Let's start with what we consider to be the biggest change, one that will influence whether a covered entity decides to notify affected individuals that there has been a breach of their PHI. In earlier drafts of the rules the standard was whether there was "the acquisition, access, use, or disclosure of protected health information in a manner not permitted [by the Privacy Rule] which compromises the security or privacy of the protected health information." The covered entity was to determine whether the event compromised the security or privacy of the PHI by conducting a risk analysis that includes the question: "Did the breach pose a significant risk of financial, reputational, or other harm to the individual?"

Fearing that this left too much wiggle-room for covered entities to decide *not* to notify, the final rule directs covered entities to *presume* such harm has resulted or will result from the unauthorized access, use or disclosure. The entity has the burden of demonstrating that there is a "low probability" of this occurring -- and its risk assessment should be retained to back up its decision not to notify. The final rules identify four factors to consider in determining the probability:

- the content and extent of the PHI and the likelihood that it can be re-identified;
- the unauthorized person who obtained or used the PHI;
- whether it was actually viewed or used; and
- to what extent the risk has been mitigated.

Shifting the burden of proof on "risk of harm" will certainly push covered entities to disclose.

Although covered entities continue to have sixty days to notify affected individuals of a breach, the commentary indicates that waiting that long may not be appropriate

MURTHA CULLINA

If you have any questions about the issues addressed here, or any other matters involving Health Care law issues, please feel free to contact:

Heather O. Berchem
203.772.7728
hberchem@murthalaw.com

Marcel J. Bernier
860.240.6087
mbernier@murthalaw.com

Melissa A. Federico
860.240.6042
mfederico@murthalaw.com

Robert V. Giunta, Jr.
860.240.6033
rgiunta@murthalaw.com

H. Kennedy Hudner
860.240.6029
khudner@murthalaw.com

Paul E. Knag
203.653.5407
pknag@murthalaw.com

Mark F. Korber
860.240.6030
mkorber@murthalaw.com

Kenneth L. Levine
860.240.6121
klevine@murthalaw.com

Michael E. McDonough
860.240.6056
mmcdonough@murthalaw.com

Elizabeth Neuwirth
203.772.7742
eneuwirth@murthalaw.com

Alfred E. Smith, Jr.
203.772.7722
asmith@murthalaw.com

Louis B. Todisco
203.772.7718
ltodisco@murthalaw.com

to allow mitigation of possible harm, and timeliness is a factor in OCR's response to how the breach was handled.

You will have to modify your Notice of Privacy Practices ("Notice") by September 2013 to include a statement that most uses and disclosures of psychotherapy notes (if you maintain these), use of PHI for marketing, and the sale of PHI require an authorization. The Notice must advise patients that while PHI may be used to direct fundraising communications to them, they will be able to opt-out of receiving further fundraising communications. The Notice must also state that you will notify the patient after a breach and that you will honor a patient request not to disclose PHI to a health plan if the patient has paid fully for care out of pocket.

The definition of "marketing" is changed to require authorization for all treatment and health care operations communications where the covered entity receives financial support for making them. As a result, any subsidized communication (even if it promotes diagnosis and treatment) that markets a health related product or service will require an authorization. There is some good news on marketing and fundraising. Refill reminders, case management, and contacting people about treatment alternatives are excluded from the definition of marketing. Fundraisers can use the following PHI elements without obtaining authorization: name, address, contact information, DOB, treatment dates, treating physician, outcome information, and health insurance status. However, as noted above, with each fundraising communication, patients must be given the chance to opt-out of fundraising contacts.

More good news: the cap on HIPAA civil monetary penalties remains at $1.5 million and the penalty "tiers" remain unchanged. This is surprising considering that OCR has been handing out fines of ever increasing magnitude for privacy and security violations.

If you have questions about the issues addressed here, or any other matters involving Health Care Law, please contact your usual Murtha Cullina attorney, or Elizabeth Neuwirth at 203.772.7742 / eneuwirth@murthalaw.com.

Maria Pepe VanDerLaan
860.240.6128
mvanderlaan@murthalaw.com

Follow us on

This alert is one of a series of publications by Murtha Cullina LLP and should not be construed as legal advice or legal opinion on any specific facts or circumstances. The contents are intended for general information purposes only, and you are urged to consult your own lawyer concerning your own situation and any specific legal questions you may have.