CLIENT - ALERT

GILPIN | GIVHAN
A PROFESSIONAL CORPORATION

TO: Clients and Contacts

FROM: D. Brent Wills, Esq.

RE: ***HIPAA Update***

DATE: January 25, 2016

This Memorandum provides updates pertaining to the Health Insurance Portability and Accountability Act ("HIPAA") and its related privacy, security and breach notification regulations.

2015 enforcement highlights

The U.S. Department of Health and Human Services Office of Civil Rights ("OCR") entered into a number of additional settlements (called "resolution agreements") with HIPAA covered entities during 2015 relating to data breaches caused by the entities' various failures to comply with HIPAA requirements. These include, for example:

- Cancer Care Group, PC, a physician oncology practice in Indiana, paid $750,000 to OCR to resolve an investigation into a data breach that occurred when an unencrypted laptop and backup data were stolen from the vehicle of an employee of the practice. The laptop contained information pertaining to about 55,000 patients of the practice (i.e., "protected health information," or "PHI," in HIPAA terms). In its investigation, OCR noted numerous deficiencies in the practice's PHI safeguards: among other things, the practice failed to conduct a HIPAA-compliant security risk analysis and to implement appropriate safeguards to protect PHI accessed and stored using mobile electronic devices. The settlement is the largest to date entered into with a physician practice.

- University of Washington Medicine paid $850,000 to OCR to resolve an investigation into a data breach that occurred as the result of a phishing scam: an employee mistakenly downloaded malware unto UW's network, potentially compromising PHI pertaining to about 90,000 patients. In its investigation, OCR noted, among other deficiencies, that UW had failed to properly train its workforce in regard to phishing scams and similar cyber attacks and to perform an appropriate security risk analysis.

- St. Elizabeth's Medical Center, a community hospital in Massachusetts, paid $218,400 to resolve an OCR investigation into a data breach that occurred when members of the hospital's workforce used an unsecure network to share

patient PHI. OCR also determined that the hospital had failed to conduct an appropriate security risk analysis.

- Cornell Prescription Pharmacy, a single location pharmacy in Denver, Colorado, paid $125,000 to resolve an OCR investigation into a 2012 data breach that occurred when employees of the pharmacy placed PHI pertaining to about 1,600 pharmacy patients in an open dumpster. The information was in paper format and had not been shredded or de-identified. The breach became publicized when a local television news station reported on the incident. The resolution agreement followed prior $1 million-plus settlements between OCR and pharmacy giants CVS and Rite Aid for improperly disposing of PHI.

The settlements summarized above further evidence OCR's commitment to HIPAA enforcement and illustrate the potentially significant economic impact a data breach and resulting OCR investigation may have on a HIPAA covered entity (and, likewise, on HIPAA business associates, which are now also subject to OCR enforcement) that fails to put in place reasonable and appropriate safeguards for PHI, in accordance with the HIPAA regulations. Moreover, in order to reduce their risk of a data breach and any OCR entanglements, HIPAA covered entities and business associates should be sure to:

- Obtain and timely update a security risk analysis in accordance with the HIPAA security regulations.

- Encrypt electronic PHI (especially e-PHI stored on or transmitted using mobile electronic devices, such as laptop computers, smart phones and flash drives), or, in lieu of encryption, put in place reasonable and appropriate alternative technical safeguards.

- Properly document compliance with the HIPAA regulations, including implementing reasonable and appropriate policies and procedure, and timely and appropriately documenting compliance with such policies and procedures.

- Regularly train their workforces regarding their responsibilities under the HIPAA regulations, diligently monitor workforce compliance, and appropriately sanction workforce members who fail to meet their responsibilities.

- Enter into business associate agreements with their business associates (in general, any outside entity or individual not on the workforce who creates, maintains, transmits or receives PHI on behalf of the covered entity or business associate).

OCR notification deadline February 29, 2016

HIPAA breach notification regulations require that covered entities (and business associates, in some circumstances) notify OCR regarding any breaches of unsecured PHI. If the breach affects 500 or more individuals (i.e. a "major" breach), OCR must be notified contemporaneously with notice to the affected individuals – i.e., without unreasonably delay, but in no event later than the date 60 days after the date the breach is discovered. Breaches that affect fewer than 500 individuals (i.e., a "non-major" breach) must be reported not later than the end of February following the calendar year in which the breach occurs. In either case, the notification is provided using an online form on the OCR website.[1] Covered entities (and business associates, if applicable) who experienced one or more non-major breaches during 2015 should examine the OCR online notification form and compile the necessary information to report the breach to OCR not later than February 29, 2016. Importantly, notifying OCR regarding a data breach is tantamount to self-reporting a possible HIPAA violation, potentially subject to an OCR investigation or other enforcement. Consequently, reporting entities should strongly consider coordinating notification to OCR with appropriate legal counsel.

OCR publishes guidance pertaining to individual access to PHI

On January 7, 2016, OCR published guidance pertaining to individuals' rights under HIPAA to access their PHI under HIPAA. Although the guidance is targeted to individuals, it includes information that likely will be useful to HIPAA covered entities and business associates. The guidance provides additional explanations, including a number of "Questions and Answers About HIPAA's Access Right," to supplement the regulatory language and related guidance in the HIPAA privacy regulations (specifically, 45 CFR § 164.524), as recently modified by the Health Information Technology for Education and Clinical Health Act ("HITECH").

Among other things, the guidance reiterates and clarifies that:

- Other than in certain limited circumstances (for instance, in the case of psychotherapy notes), individuals are entitled to review or obtain a copy of their PHI on request. In general, a covered entity (or a business associate, in some circumstances) must respond to such a request within 30 days.

- If an individual requests that a covered entity (or a business associate, in some circumstances) provide the individual with a copy of his/her PHI in an electronic form that is readily producible, the covered entity (or business associate) must provide the PHI in the specified format.

- If an individual directs a covered entity (or business associate, in some circumstances) to deliver or transmit his/her PHI, in paper or electronic

[1] The online form may be accessed at https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true.

format, to a third-party recipient, and the individual clearly identifies the recipient, the covered entity must comply with the request.

- An individual must not be required to come to a covered entity's (or business associate's, if appropriate) premises or write a letter to obtain a copy of his/her PHI if the PHI is available in electronic format. The covered entity is entitled to take reasonable and appropriate steps to verify the identity of an individual requesting PHI; however, such steps should not unduly inhibit or delay access to the information.

- HIPAA allows a covered entity (or business associate, if appropriate) to charge a reasonable, cost-based fee for copying PHI requested by an individual, including labor and supply costs (including, for example, the cost of a CD or portable drive, if the individual requests electronic PHI using such devices); however, covered entities may not charge any fees for retrieving or handling the information or for processing the request.

If you are a HIPAA covered entity or business associate with questions or in need of guidance regarding HIPAA or any of the issues or matters discussed in this Memorandum, please feel free to contact me at (334) 409-2211.

This Client Alert is provided by Gilpin Givhan, PC for informational purposes only. It is not intended to constitute legal advice. For legal advice regarding particular matters, please contact Gilpin Givhan, PC or other appropriate legal counsel.