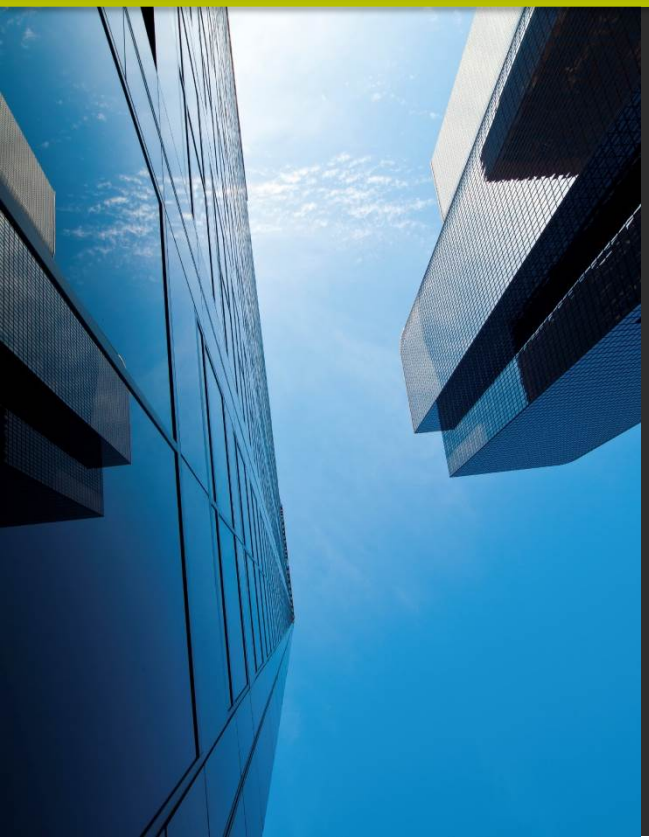
FOLEY HOAG LLP

Privacy and Security: To HIPAA and Beyond



MaHIMA Winter Meeting
January 22, 2016

Colin J. Zick, Esq.
Foley Hoag LLP
(617) 832-1275
czick@foleyhoag.com

2015 In Review

Breaches and attacks continued to occur at a high frequency and involving large numbers of individuals:

- Excellus BlueCross BlueShield: The Excellus BlueCross BlueShield breach exposed personal data from more than 10 million members after the company's IT systems were breached, beginning as far back as December 2013.
- Premera Blue Cross: Premera announced its breach, affecting the data of more than 11 million members, just one month after the Anthem Blue Cross breach. The company discovered the cyberattack in January, but the initial breach occurred in May 2014. Employees of Microsoft, Starbucks and Amazon were some of the customers affected.
- Anthem: Approximately 78.8 million patient records were breached, and an additional 8.8 to 18.8 million non-patient records.

HHS OCR Guidance: Individuals' Access to Health Information

- Earlier this month, HHS OCR issued guidance on "Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524."
  - Unreasonable Measures
  - Providing Access
  - Timeliness in Providing Access
  - Fees for Access
  - Denial of Access

HHS OCR: Unreasonable Measures

- While the Privacy Rule allows covered entities to require that individuals request access in writing and requires verification of the identity of the person requesting access, a covered entity may not impose unreasonable measures on an individual requesting access that serve as barriers to or unreasonably delay the individual from obtaining access. For example, a doctor may not require an individual:
  - Who wants a copy of her medical record mailed to her home address to physically come to the doctor's office to request access and provide proof of identity in person.
  - To use a web portal for requesting access, as not all individuals will have ready access to the portal.
  - To mail an access request, as this would unreasonably delay the covered entity's receipt of the request and thus, the individual's access.
- While a covered entity may not require individuals to request access in these manners, a covered entity may permit an individual to do so, and covered entities are encouraged to offer individuals multiple options for requesting access.

HHS OCR: Form and Format and Manner of Access

- A covered entity also must provide access in the manner requested by the individual, which includes arranging with the individual for a convenient time and place to pick up a copy of the PHI or to inspect the PHI (if that is the manner of access requested by the individual), or to have a copy of the PHI mailed or e-mailed, or otherwise transferred or transmitted to the individual to the extent the copy would be readily producible in such a manner.
- A covered entity is not expected to tolerate unacceptable levels of risk to the security of the PHI on its systems in responding to requests for access; whether the individual's requested mode of transfer or transmission presents such an unacceptable level of risk will depend on the covered entity's Security Rule risk analysis.
- However, mail and e-mail are generally considered readily producible by all covered entities. A covered entity may not require that an individual travel to the covered entity's physical location to pick up a copy of her PHI if the individual requests that the copy be mailed or e-mailed.

HHS OCR: Timeliness in Providing Access

- In providing access to the individual, a covered entity must provide access to the PHI requested, in whole, or in part (if certain access may be denied as explained below), no later than 30 calendar days from receiving the individual's request.
- The 30 calendar days is an outer limit and covered entities are encouraged to respond as soon as possible. Indeed, a covered entity may have the capacity to provide individuals with almost instantaneous or very prompt electronic access to the PHI requested through personal health records, web portals, or similar electronic means.
- If a covered entity is unable to provide access within 30 calendar days -- for example, where the information is archived offsite and not readily accessible -- the covered entity may extend the time by no more than an additional 30 days.
- To extend the time, the covered entity must, within the initial 30 days, inform the individual in writing of the reasons for the delay and the date by which the covered entity will provide access. Only one extension is permitted per access request.

HHS OCR: Fees for Access

- The fee may not include costs associated with verification; documentation; searching for and retrieving the PHI; maintaining systems; recouping capital for data access, storage, or infrastructure; or other costs not listed above even if such costs are authorized by State law.

HHS OCR: Denial of Access

- A covered entity may not require an individual to provide a reason for requesting access, and the individual's rationale for requesting access, if voluntarily offered or known by the covered entity or business associate, is not a permitted reason to deny access.
- In addition, a covered entity may not deny access because a business associate of the covered entity, rather than the covered entity itself, maintains the PHI requested by the individual (e.g., the PHI is maintained by the covered entity's electronic health record vendor or is maintained by a records storage company offsite).

FAQ re: EHR Incentives

Under the EHR Incentive Program, participating providers are required to provide individuals with access to certain information on much faster timeframes (e.g., a discharge summary within 36 hours of discharge, a lab result within 4 business days after the provider has received the results) than under HIPAA. How do these requirements operate together?

- Health care providers participating in the EHR Incentive Program may use the patient engagement tools of their Certified EHR Technology to make certain information available to patients quickly and satisfy their EHR Incentive Program objectives. While the Privacy Rule permits a covered entity to take up to 30 calendar days from receipt of a request to provide access (with one extension for up to an additional 30 calendar days when necessary), covered entities are strongly encouraged to provide individuals with access to their health information much sooner, and to take advantage of technologies that enable individuals to have faster or even immediate access to the information.

Mental Health Information for Firearm Background Checks

- On January 4, 2016, the HIPAA Privacy Rule was modified to expressly permit certain covered entities to disclose to the National Instant Criminal Background Check System (NICS) the identities of those individuals who, for mental health reasons, already are prohibited by Federal law from having a firearm.
- The information that can be disclosed is the limited identifying information about individuals who have been involuntarily committed to a mental institution or otherwise have been determined by a lawful authority to be a danger to themselves or others or to lack the mental capacity to manage their own affairs – that is, only about those who are covered under the pre-existing mental health prohibitor."
- This rule applies to the subset of HIPAA covered entities that either make the mental health determinations that disqualify individuals from having a firearm or are designated by their States to report this information to NICS.

Mental Health Information for Firearm Background Checks (cont.)

The new HIPAA regulatory language, published in the January 6, 2016 Federal Register, is as follows:

164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.

(k)(7) National Instant Criminal Background Check System. A covered entity may use or disclose protected health information for purposes of reporting to the National Instant Criminal Background Check System the identity of an individual who is prohibited from possessing a firearm under 18 U.S.C. 922(g)(4), provided the covered entity:

(i) Is a State agency or other entity that is, or contains an entity that is:

(A) An entity designated by the State to report, or which collects information for purposes of reporting, on behalf of the State, to the National Instant Criminal Background Check System; or

(B) A court, board, commission, or other lawful authority that makes the commitment or adjudication that causes an individual to become subject to 18 U.S.C. 922(g)(4); and

(ii) Discloses the information only to:

(A) The National Instant Criminal Background Check System; or

(B) An entity designated by the State to report, or which collects information for purposes of reporting, on behalf of the State, to the National Instant Criminal Background Check System; and

(iii)(A) Discloses only the limited demographic and certain other information needed for purposes of reporting to the National Instant Criminal Background Check System; and

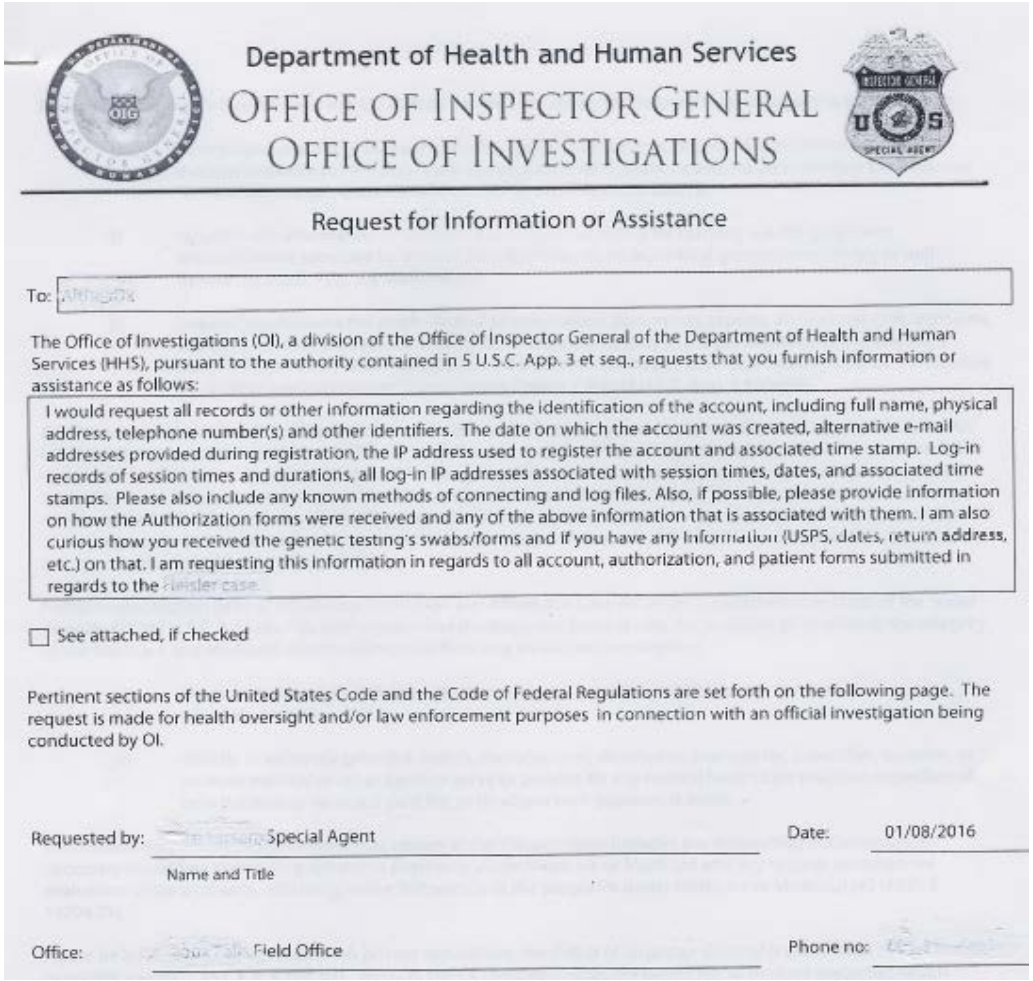
(B) Does not disclose diagnostic or clinical information for such purposes.

Are Attorneys Entitled to the "HIPAA Rate"?

- 45 CFR § 164.524 Access of individuals to protected health information is limited to requests from the individual whose records are at issue ("an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set") but not a third party (like a lawyer).
- In the December 2000 regulatory comments to HIPAA, it talks about who is the "individual":
  - Individual
    - We proposed to define "individual" to mean the person who is the subject of the protected health information. We proposed that the term include, with respect to the signing of authorizations and other rights (such as access, copying, and correction), the following types of legal representatives:
      - (1) With respect to adults and emancipated minors, legal representatives (such as court-appointed guardians or persons with a power of attorney), to the extent to which applicable law permits such legal representatives to exercise the person's rights in such contexts.
      - (2) With respect to unemancipated minors, a parent, guardian, or person acting in loco parentis, provided that when a minor lawfully obtains a health care service without the consent of or notification to a parent, guardian, or other person acting in loco parentis, the minor shall have the exclusive right to exercise the rights of an individual with respect to the protected health information relating to such care.
      - (3) With respect to deceased persons, an executor, administrator, or other person authorized under applicable law to act on behalf of the decedent's estate

HHS OIG "Request for Information or Assistance"

- A new form of HHS OIG request, less formal than the HIPAA subpoena.



Department of Health and Human Services
OFFICE OF INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS

Request for Information or Assistance

To: [redacted]

The Office of Investigations (OI), a division of the Office of Inspector General of the Department of Health and Human Services (HHS), pursuant to the authority contained in 5 U.S.C. App. 3 et seq., requests that you furnish information or assistance as follows:

I would request all records or other information regarding the identification of the account, including full name, physical address, telephone number(s) and other identifiers. The date on which the account was created, alternative e-mail addresses provided during registration, the IP address used to register the account and associated time stamp. Log-in records of session times and durations, all log-in IP addresses associated with session times, dates, and associated time stamps. Please also include any known methods of connecting and log files. Also, if possible, please provide information on how the Authorization forms were received and any of the above information that is associated with them. I am also curious how you received the genetic testing's swabs/forms and if you have any information (USPS, dates, return address, etc.) on that. I am requesting this information in regards to all account, authorization, and patient forms submitted in regards to the [redacted] case.

☐ See attached, if checked

Pertinent sections of the United States Code and the Code of Federal Regulations are set forth on the following page. The request is made for health oversight and/or law enforcement purposes in connection with an official investigation being conducted by OI.

Requested by: [redacted] Special Agent — Date: 01/08/2016

Name and Title

Office: [redacted] Field Office — Phone no: [redacted]

Breach Class Actions: "What's the Harm?"

Walker v. Boston Medical Center, MDF Transcription LLC and Richard J. Fagan, Suffolk County (Mass.) Superior Court, November 19, 2015

- Breach notice sent because patient records from physician office visits "were inadvertently made accessible to the public through an independent medical record transcription service's online site."
- Records "could potentially be accessed by non-authorized individuals"
- BMC had "no reason to believe that this led to the misuse of patient information" but could not say "how long the information was publicly accessible through the site."
- Patients sued.
- BMC moved to dismiss because there was no showing of harm.
- The court declined to dismiss, allowing discovery to proceed.

The Emerging Lessons of Walker v. BMC

- The law may be changing in this area.
- Breach response matters:
  - Finding breaches quickly matters, so that potential harm can be mitigated and there is a stronger argument against class actions.
  - Whether to give notice is now an even bigger decision.
  - If you decide to give notice, what you say in the breach notification matters.
- Who you choose as your vendors matters, especially if there is a breach:
  - Will the vendor cause a breach?
  - Will the vendor be around if there is a breach?

Colin Zick

Partner, *Co-Chair, Health Care Practice and Privacy & Data Security Practice*
Foley Hoag LLP

czick@foleyhoag.com | 617.832.1275