OCR’s Anatomy: HIPAA Breaches, Investigations, and Enforcement

Clinton Mikel
The Health Law Partners, P.C.

Alessandra Swanson
U.S. Department of Health and Human Services - Office for Civil Rights
Disclosure

These materials should not be considered legal advice.

They are not intended to, nor do they, create an attorney-client relationship.

The materials are general and may not apply to certain individual legal or factual circumstances.

I have no relevant financial relationships or commercial interests to disclose.
1) HIPAA Breaches
   ➢ How HIPAA Breaches Arise
   ➢ How to Respond to HIPAA Breaches

2) OCR HIPAA Breach Investigations
   ➢ Types of OCR Investigations
   ➢ What to Expect During an OCR Investigation
   ➢ How to Respond to OCR Investigations
How to Respond to a Potential HIPAA Breach: Overview and Best Practices
• What is a reportable “Breach” under HIPAA?

  ➢ Acquisition, access, use, or disclosure of unsecured PHI not permitted by the Privacy Rule unless there is low probability the PHI has been compromised based on a risk assessment.

  ➢ Breach presumed unless demonstrated otherwise.

  ➢ March 1, 2016, reporting deadline for calendar year 2015 small breaches (where < 500 individuals impacted).

  ➢ State Law Considerations.
Breach Investigation Best Practices

- Prompt investigations of possible breaches is critical.
- Work with health care legal counsel and IT experts.
- Document everything
- Rapid Response and Notification
- **Two Tracks (critical)**
  - 1) Breach Response
  - 2) Prepare for the investigation/get your house in order!
If you suspect a breach of computerized data:

• Do not delete, move, or alter files on affected system.
• Do not contact the suspected perpetrator.
• Do not attempt to conduct a forensic analysis.
Breach Investigation Best Practices

Instead, if you suspect a breach:

1) Immediately **notify** health care legal counsel and IT experts to establish a **plan of action** for the investigation and analysis.

2) **Secure** the premises.

3) **Isolate affected system** to prevent further intrusion, data release, or damage. Take infected machines offline, but leave the power on.

4) Use **telephone** to communicate. Attackers may be capable of monitoring email traffic.

5) Activate all **auditing software**, if not already activated.

6) IT experts should preserve all pertinent system logs (firewall, router, intrusion detection system, etc.). Files on the affected systems should **never be deleted, moved, or altered** in any way.

7) If files are damaged or altered, IT experts should **create backup** copies and store them in a secure location.

8) Identify **systems that connect** to the affected system and where the affected system resides within the network topology.

*Continued...*
9) Identify the **programs and processes** that operate on the affected system(s), pre-identify the associated IP address, MAC address, Switch Port location, ports and services required, physical location of system(s), the OS, OS version, patch history, safe shut down process, and system administrator or backup.

10) Locate **backup** or “cousin” data, if any.

11) Take an **inventory** of missing items and their locations.

12) Review keycard and surveillance data for **unusual activity**.

13) Retain an **external forensic IT expert** to assist and to image the data.

14) Determine whether **breach notification** is required. (See next slide.)

15) If necessary, after consultation with health care legal counsel, notify **affected patients** and the appropriate **law enforcement agenc(ies)**.
   
   a) **Document** all conversations with law enforcement, if any, and the steps taken to restore the integrity of the system.
   
   b) In the event the affected system is collected as evidence, make arrangements to provide for the **continuity of services**, i.e., prepare redundant system and obtain data back-ups.

16) After the investigation and notification (if necessary) are completed, conduct a **post-investigation review** of the events and make necessary adjustments to the technology and/or response procedure to reflect the lessons learned.
How to Determine if breach notification is required under HIPAA:

1) Determine whether the use or disclosure violates the Privacy Rule. If no, then no breach notification required. If yes, then continue to Step 2.

2) Determine whether the PHI was unsecured. If secured pursuant to HHS guidance (e.g., encryption or destruction), then no breach notification required. If not, then continue to Step 3.

3) Determine whether a breach notification exception applies. The three exceptions include:
   a) Unintentional acquisition, access, or use of PHI by a workforce member or person acting under authority.
      ➢ Made in good faith and within the scope of authority and does not result in further use or disclosure which violates the Privacy Rule.
   b) Inadvertent disclosures by a person who is authorized to access PHI to another person authorized to access PHI at the same entity.
      ➢ PHI not further used or disclosed in a manner that violates Privacy Rule.
   c) Disclosure of PHI where there is a good-faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

4) Conduct and document an objective risk assessment to determine whether the violation compromised the PHI. (See next slide.)
HIPAA Risk Assessment:

Any acquisition, access, use or disclosure of PHI in a manner violative of the Privacy Rule is presumed to be a breach. If a Privacy Rule violation has occurred, determine if breach notification is not required based on a reasonable, good-faith risk assessment that there is a low probability that the PHI has been compromised. Four factors to consider are:

a) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

b) The unauthorized person who used the PHI or to whom the disclosure was made;

c) Whether the PHI was actually acquired or viewed; and

d) The extent to which the risk to the PHI has been mitigated.
Breach Investigation Best Practices

- Do or don’t do risk assessment?
  - Make sure it is **thorough**, with a **good-faith** application of the law and **reasonable** conclusions.

- Log the unauthorized use or disclosure in the patient’s disclosure tracking log

- Do a Security Incident Report
  - 164.308(a)(6)(ii)

- Remember the 2 Tracks!

- **Move to your gap analysis and IMPLEMENT**
  - Update Notice of Privacy Practices
    - First thing OCR auditors will do is go to the CE’s website to see if the NPP is posted.
    - OCR will look to see that the NPP is updated for the HIPAA Omnibus Rule.
  - Update breach notification policies and physical and technical safeguards. Make sure to **implement**.
  - Conduct and document employee training.
  - Conduct and document risk assessment.
  - Update BAAs and document satisfactory assurances from BAs.
    - *E.g.*, consultants, experts, shredding companies, document and cloud storage companies, etc.
OCR HIPAA Enforcement: Types of OCR Investigations and How to Respond
The Office for Civil Rights (OCR) is responsible for enforcing the HIPAA Privacy & Security Rules.

How does OCR enforce HIPAA?

1) Investigation of breaches and complaints filed with OCR.
2) HIPAA compliance reviews/audits.
3) Education and outreach to foster compliance.
OCR HIPAA Audits

- OCR completed the pilot audit program in 2012.
- The second round of OCR HIPAA audits were initially delayed last fall. Many expected the audits to occur this year, but there may be another delay.
- **What you need to know about OCR audits:**
  - All CEs and BAs are eligible to be audited.
  - Protocols not yet finalized for 2nd round (Omnibus Rule updates).
  - The objectives of the pilot program were to: (i) examine mechanisms for compliance; (ii) identify best practices; (iii) discover risks and vulnerabilities that may not have come to light through complaint investigations and compliance reviews; (iv) renew attention of CEs to health information privacy and security compliance activities.
  - During the pilot program, the OCR:
    1) Notified the CE in writing of the audit and asked for documentation of compliance efforts within 10 business days;
    2) Conducted a site visit (provided 30–90 days’ notice of site visit; site visits generally took 30-90 business days);
    3) Provided a “draft” final report to the CE, and the CE had 10 business days to review and provide written comments; and
    4) Completed final audit report 30 days after receiving CEs comments.
OCR HIPAA Investigations

HIPAA Privacy & Security Rule Complaint Process

Complaint

Intake & Review

Possible Criminal Violation

DOJ

Accepted by DOJ

Resolution

OCR finds no violation
OCR obtains voluntary compliance, corrective action, or other agreement
OCR issues formal finding of violation

Possible Privacy or Security Rule Violation

 Investigation

The violation did not occur after April 14, 2003
Entity is not covered by the Privacy Rule
Complaint was not filed within 180 days and an extension was not granted
The incident described in the complaint does not violate the Privacy Rule

OCR Investigations: Step-By-Step

1) OCR receives a complaint, breach notice, et cetera
   - *E.g.*, complaints filed by patients or employees.

2) OCR conducts intake & review to determine if a possible Privacy or Security Rule violation occurred.

3) At any time, the OCR may refer the complaint to the DOJ if a possible criminal violation occurred.

4) If no Privacy or Security Rule violation, case is closed.

5) If there is a possible violation, then OCR will notify the complainant and the CE. (See next slides.)
   - The CE will receive a letter from the OCR asking for specific information to be submitted for review.
   - In some cases, the letter will not have any requests, but will instead list corrective actions for the CE to take.

6) Respond to OCR’s information requests or compliance demands.
Dear Dr. [Redacted]:

The U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) received a complaint on [Redacted] alleging that Dr. [Redacted] (the covered entity) is not in compliance with certain aspects of the Federal Standards for Privacy of Individually Identifiable Health Information and/or the Security Standards for the Protection of Electronic Protected Health Information (45 C.F.R. Parts 160 and 164, Subparts A, C, and E, the Privacy and Security Rules) promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Specifically, [Redacted] (the complainant) alleges that on [Redacted], this allegation could reflect a violation of 45 C.F.R. 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(4)(i), 164.308(a)(5)(i), 164.308(a)(5)(ii)(B), 164.308(a)(6)(i), 164.308(a)(7)(ii)(A), 164.312(a)(1), 164.312(e)(1), 164.314(a), 164.404, 164.406, 164.408, 164.502(a), 164.502(e), 164.504(e), 164.530(c), and 164.530(f), respectively.

OCR enforces the Privacy and Security Rules, and also enforces Federal civil rights laws that prohibit discrimination in the delivery of health and human services because of race, color, national origin, disability, age, and, under certain circumstances, sex and religion.

OCR is responsible for enforcing the Privacy and Security Rules as they apply to covered entities. Covered entities include health care providers that transmit health information in electronic form in connection with a transaction for which HHS has adopted standards. See 45 C.F.R. Part 162. The covered entity is a covered entity pursuant to HIPAA.

OCR’s authority to collect information and ascertain a covered entity’s compliance is found at 45 C.F.R. §§ 160.300 – 160.316. As set forth in those provisions, to the extent practicable, OCR will seek the cooperation of covered entities in obtaining compliance with the applicable provisions of the Privacy and Security Rules. A covered entity is required to submit records...
and compliance reports as may be necessary for OCR to ascertain whether the covered entity has complied with the Privacy and Security Rules.

We respectfully request that the covered entity provide OCR the following:

1) Please submit a response to the allegations made in the complaint. Please describe the circumstances leading to the alleged incident to include the date of the incident and the date of discovery of the incident. Please list in detail the protected health information (PHI) that was made available to unauthorized individuals.

2) Copies of any notes, documents and reports relating to any internal investigation, including of any forensic analysis, conducted by the covered entity, or its designated contractor or agent, of this alleged incident. Please detail any corrective measures taken as a result of this alleged incident.

3) Please indicate whether you conducted a breach risk assessment for the alleged incident. If so, please provide a copy of the breach risk assessment.
   a. If you determined that a breach of patients’ PHI occurred as a result of this incident, please indicate, as applicable, whether you notified the affected individuals, the media, and the HHS Secretary.
   b. If you notified the affected individuals, the media, and the HHS Secretary, please provide OCR with documentation of said notifications.

4) A copy of the covered entity’s policies and procedures with respect to uses and disclosures of PHI and safeguarding PHI developed pursuant to HIPAA.

5) Please identify the vendor that maintained [REDACTED] on the covered entity’s website.
   a. Please provide a copy of the covered entity’s business associate agreement with the vendor that was in effect at the time of this incident.

6) A copy of any risk analysis performed pursuant to 45 C.F.R. § 164.308(a)(1)(ii) prior to [REDACTED] and any risk management plans developed as a result of the risk analysis.
   a. Any revisions or updates made to the risk analysis to include malware infection or hacking attacks as a risk item.
   b. Evidence of all implemented security measures to reduce the risk of malware infection or hacking (e.g. screenshots, configuration settings).

7) Evidence of information system activity reviews (e.g. user access, user activity, network security, etc.)
8) Evidence of any network scans or penetration tests performed before and/or after the incident.

9) A copy of the covered entity’s approved access management policy pursuant to 45 C.F.R. §164.308(a)(4).

10) A copy of the covered entity’s security awareness and training materials prior to the incident. Please include evidence of workforce attendance to the training.

11) Evidence of malicious software protection (antivirus system) installed at the time of the incident. Please also include evidence of patching on the affected systems.

12) A copy of the covered entity’s approved data backup procedures. Please include evidence of data backup mechanism/ process.

13) Evidence of technical access controls that the covered entity implemented. Please include a copy of the covered entity’s approved password management policy and procedure.

14) Evidence of implemented network security devices such as firewalls, intrusion detection systems, etc. Please include evidence of any network scans performed on the network/computer before and/or after the incident.

15) Details of network security monitoring to identify network related threats and vulnerabilities.

For each data request item listed above, specify the name and title of each individual who furnished information in response to the request.

We ask that the information requested above be provided within 20 days of the receipt of this letter. The information submitted in response to this request will be treated as confidential and will not be disclosed, except as necessary for ascertaining or enforcing compliance with the applicable administrative simplification provisions of HIPAA.

Under the Freedom of Information Act, we may be required to release this letter and other information about this case upon request by the public. In the event OCR receives such a request, we will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

Please be assured that OCR is committed to resolving this matter in an efficient and timely manner. If you have any questions, please do not hesitate to contact [Contact Information]. When contacting this office, please remember to include the reference number that we have given this file. That number is located in the upper left-hand corner of this letter.
Thank you for your cooperation in this matter.

Sincerely,

[Redacted]

Acting Regional Manager

Enclosure: Privacy and Security Rules Penalty Provisions Fact Sheet
OCR Investigations: Sample Letter #1

Highlights from sample letter #1:

• OCR transaction number.
• Short description of the breach allegations in the complaint & potential HIPAA violations
• List of OCR’s requests, including written responses and document requests (in this case, 15 separate requests), including:
  ➢ Response to allegations in complaint;
  ➢ Internal investigation documents;
  ➢ Breach risk assessment;
  ➢ Patient notification letter;
  ➢ CE’s HIPAA policies and any HIPAA training;
  ➢ Any HIPAA risk analysis performed;
  ➢ Evidence of technical safeguards, including network scans, malicious software protection, network security devices, and data backup.
• Deadline to respond set at 20 days after receipt of letter.
• Name of the investigator in charge.
DEPARTMENT OF HEALTH & HUMAN SERVICES

On [redacted], the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR), received a complaint alleging that [redacted], the covered entity, has violated the Federal Standards for Privacy of Individually Identifiable Health Information and/or the Security Standards for the Protection of Electronic Protected Health Information (45 C.F.R. Parts 160 and 164, Subparts A, C, and E, the Privacy and Security Rules). Specifically, the complaint alleges that on [redacted], the covered entity [redacted]

These allegations could reflect a violation of 45 C.F.R. §§ 164.502(a) and 164.530(c).

OCR enforces the Privacy, Security, and Breach Notification Rules, and also Federal civil rights laws which prohibit discrimination in the delivery of health and human services because of race, color, national origin, disability, age, and under certain circumstances, sex and religion.

A covered entity may not use or disclose an individual’s protected health information without an authorization, unless permitted or required by the Privacy Rule. In addition, a covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards (i) to prevent the intentional or unintentional use or disclosure of protected health information in violation of the Privacy Rule and (ii) to limit its incidental use and disclosure pursuant to an otherwise permitted or required use or disclosure.

OCR has determined that the following corrective actions are needed to bring [redacted] into compliance with the Privacy Rule:

1. Conduct an internal investigation regarding the allegations.

2. Based on the findings of the internal investigation take the following actions:
   a. To the extent that [redacted] is able to identify the workforce member(s) responsible for [redacted]
such that protected health information was

i. Retrain such workforce member(s) on obligations under the Privacy Rule;

ii. Determine whether sanctioning such workforce member(s) is appropriate, consistent with policies and procedures;

b. To the extent that is able to identify any of the individuals whose protected health information was

i. Determine appropriate actions to mitigate, to the extent practicable, any harmful effect that is known to of any impermissible use/disclosure of protected health information;

ii. For each impermissible use/disclosure identified, conduct a risk assessment to determine whether is required to provide notice of a breach of unsecured protected health information to the affected individual(s) and to HHS pursuant to 45 C.F.R. §§ 164.404-164.408. This risk assessment must consider: 1) the nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification; 2) the unauthorized person who used the protected health information or to whom the disclosure was made; 3) whether the protected health information was actually acquired or viewed; and 4) the extent to which the risk to the protected health information has been mitigated. In making this determination, please be advised that the impermissible use or disclosure of unsecured protected health information is presumed to be a reportable breach unless the covered entity or business associate demonstrates a low probability that the protected health information has been compromised or an exception applies. Breach notifications to HHS may be made using the online breach notification tool at

http://ocrnotifications.hhs.gov

3. Implement additional administrative, technical and/or physical safeguards to protect the privacy of protected health information, in particular, reasonable safeguards to protect against any intentional or unintentional use or disclosure, such as the disclosures at issue in this complaint;

Please note that, after a period of six months has passed, OCR may initiate and conduct a compliance review of related to your compliance with the Privacy Rule.

Based on the foregoing, OCR is closing this case without further action, effective the date of this letter. OCR’s determination as stated in this letter applies only to the allegations in this complaint that were reviewed by OCR.
Under the Freedom of Information Act, we may be required to release this letter and other information about this case upon request by the public. In the event OCR receives such a request, we will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

If you have any questions regarding this matter, please contact [redacted] Investigator, at [redacted].

Sincerely,
[redacted]

Regional Manager
Highlights from sample letter #2:

• Includes much of the same information as sample letter #1 (i.e., OCR transaction number, short description of the allegations in the complaint, name of investigator in charge, etc.).

• However, instead of requiring the CE to respond to document requests and written questions, sample letter #2 lists “corrective actions” the CE must take to comply with HIPAA, including:
  - Conduct an internal investigation of the allegations in complaint;
  - Re-train workforce members involved in incident on Privacy Rule;
  - Determine if sanctions against workforce members are appropriate;
  - Mitigate harm to patients affected;
  - Conduct HIPAA risk assessment; and
  - Implement administrative, physical, and technical safeguards to prevent similar incidents.

• Sample letter #2 states that the case is closed as of the date of the letter and notifies the CE that OCR may conduct a compliance review in six months. In contrast, sample letter #1 kept the investigation open pending the CE’s response (which essentially was a compliance review).
Best Practices for Response to OCR

• Get the *response deadline in writing*.  
  ➢ *E.g.*, notify the OCR investigator via email of the date the CE received the letter and confirm the response deadline calculated from the date of receipt.  
  ➢ Or, in the sample letter #2 scenario where no response is required, begin implementing the corrective actions immediately.

• **Gap Analysis and Fixing.**  
  • Forget the allegations, fix the ecosystem  
  • **Overreact.** Don’t underreact.  
    ➢ Show the OCR that the CE takes HIPAA compliance very seriously.

• Put your *best foot forward*.  
  ➢ Even if not specifically requested by the OCR, make sure to state the ways in which the CE is HIPAA compliant and the corrective actions the CE has taken to become/remain HIPAA compliant.  
  ➢ Focus on reputable compliance history and what CE has done correctly.  
  ➢ **LOTS OF DOCUMENTS**

• Don’t highlight, but *don’t hide from weaknesses*.  
  ➢ OCR wants to see that the CE is acting in good faith, learning, and taking corrective actions to ensure compliance. Highlight this when discussing your weaknesses.  
  ➢ Focus on how you can and will improve and your ongoing compliance efforts.  

• Highlight the CE’s *compliance barriers*, but don’t rely on this too heavily.  
  ➢ *E.g.*, small practice with few employees/resources doing the best it can.
Best Practices for Response to OCR

- Update Notice of Privacy Practices
  - First thing OCR auditors will do is to go to the CE’s website to see if the NPP is posted.
  - OCR will look to see that the NPP is updated for the HIPAA Omnibus Rule.
- Update breach notification policies and physical and technical safeguards. Make sure to implement.
- Conduct and document employee training.
- Conduct and document risk assessment.
  - Make sure it is thorough, with a good-faith application of the law and reasonable conclusions.
- Accounting of disclosures for purposes other than treatment, payment, and health care operations
- Update BAAs and document satisfactory assurances from BAs.
  - E.g., consultants, experts, shredding companies, document and cloud storage companies, etc.
7) After receiving CE’s response, OCR reviews evidence to determine if a violation occurred. If evidence indicates that CE was not in compliance, then OCR will attempt to resolve the case by obtaining:
   - Voluntary compliance;
   - Corrective action; and/or
   - Resolution agreement.

8) Sometimes OCR will request additional information/evidence (e.g., follow-up questions/requests about whether the CE actually took the corrective actions it said it would take in its response).

9) If CE does not take action to resolve the matter that is satisfactory to OCR, then OCR may impose CMPs and CE may request an evidentiary hearing.

10) If OCR is satisfied with the CE’s corrective actions, OCR will typically request a phone call to “offer HIPAA technical assistance” to the CE. This is usually an indication that OCR is closing the file.

11) Once investigation is closed, OCR will send a letter (see next slide).

12) CE should review its response to investigation and determine how it can improve for next time.
DEPARTMENT OF HEALTH & HUMAN SERVICES
Office of Civil Rights
Office for Civil Rights, Region
http://www.hhs.gov/ocr/

Mr. [redacted]

Dr. [redacted]

OCR Transaction Number: [redacted]

Dear [redacted],

On [redacted], the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) received a complaint alleging that [redacted] (the covered entity), is not in compliance with certain aspects of the Federal Standards for Privacy of Individually Identifiable Health Information and/or the Security Standards for the Protection of Electronic Protected Health Information (45 C.F.R. Parts 160 and 164, Subparts A, C, and E, the Privacy and Security Rules) promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Specifically, [redacted] (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the complainant) alleges that on [redacted], [redacted], (the com
Based on OCR’s investigation, the covered entity conducted an internal investigation of this matter. The covered entity advised OCR that it learned of this incident on [insert date].

The covered entity acknowledged the incident and attributed it to human error. [insert details of internal investigation]. The covered entity advised OCR that its internal investigation determined that the PHI as a result of this incident including, the individual’s name, date of birth, address, telephone number, medical and dental insurance information, social security number, and medical history.

In light of the foregoing, the covered entity took various corrective actions to prevent a recurrence of the breach. Specifically, the covered entity [insert details of corrective actions]. The covered entity also advised OCR that as a result of this incident, it terminated its relationship with its business associate. Also, as a result of this incident, the covered entity will no longer [insert details of new policies or changes].

In addition, the covered entity determined that the unauthorized access to its patients’ PHI constituted a breach and accordingly, on [insert date], it notified all affected individuals. The covered entity provided OCR with documentation showing that it offered each affected patient one year of free credit monitoring and identity theft insurance. On [insert date], during a telephone conversation with an OCR staff member, the complainant acknowledged receipt of the breach notification letter along with the offer for one year of free credit monitoring services. The complainant advised OCR that while he did not take advantage of the free credit monitoring services because he had already signed up for credit monitoring service, the entity offered to reimburse him for the cost of his credit monitoring service.

The covered entity provided OCR with written assurances that as required by the Breach Notification Rule, it will submit a breach report to HHS no later than sixty calendar days after the end of 20 [insert date]. The
covered entity also provided OCR with written assurances that, as required by the Privacy Rule, it documented the impermissible disclosure of the affected individuals' PHI for accounting of disclosure purposes.

Further, based on OCR’s investigation, the covered entity updated its internal policies and procedures with respect to the requirements of HIPAA’s Privacy and Security Rules and it trained its workforce members on them. Additionally, the covered entity executed business associate contracts with all of its business associates, placed a physical lock on its server, and performed a new assessment of the risks and vulnerabilities to its systems that contain electronic PHI. On [redacted], OCR provided the covered entity with extensive technical assistance regarding HIPAA’s Privacy, Security Rules, and Breach Notification Rules.

Based on the corrective action measures taken by the covered entity, OCR deems that all matters raised by this complaint at the time it was filed have now been resolved through the voluntary compliance actions of the covered entity. Therefore, OCR is closing this case.

OCR’s determination, as stated in this letter, applies only to the allegations in this complaint that were reviewed by OCR.

Under the Freedom of Information Act, we may be required to release this letter and other information about this case upon request by the public. In the event OCR receives such a request, we will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

Should you have any questions regarding this matter, please contact [redacted] Investigator by [redacted].

Thank you for bringing this matter to our attention.

Sincerely,

[redacted]

[redacted]

Regional Manager
Highlights from OCR closure letter:

- Letter addressed to the CE and the complainant.
- Outlines the evidence collected from CE and complainant.
- Focused on the mitigating and corrective actions taken by CE.
  - CE conducted an **internal investigation** and **quickly took steps to protect PHI** compromised and to **prevent similar incidents**.
  - CE terminated its relationship with BA involved in breach.
  - CE **updated its HIPAA policies**, conducted employee **training**, and increased **physical and technical safeguards**.
  - CE **notified** affected patients and offered one year of **credit monitoring**.
  - CE gave assurances it would **report breach to OCR** within 60 days after end of year and document breach for **accounting of disclosure** purposes.
- “Based on the **corrective action measures** taken by the covered entity, OCR deems that all matters raised by this complaint at the time it was filed have now been **resolved through the voluntary compliance actions** of the covered entity. Therefore, OCR is **closing this case**.”
- OCR’s determination only applies to issues raised in complaint.
Questions?

Clinton Mikel, Esq.
Partner
The Health Law Partners, P.C.
Southfield, Michigan
(248) 996-8510
cmikel@thehlp.com