Your Money Or Your PHI: HHS Provides Guidance on Ransomware

Lucie F. Huger, Esq./ Kevin F. Hormuth, Esq.
Greensfelder, Hemker & Gale, P.C.
March 2, 2018

Jocelyn Samuels, Former Director of OCR

"We continue to see a lack of comprehensive and enterprise-wide risk analysis and risk management that leads to major breaches and other compliance problems. **That is why enforcement is a critical part of our arsenal of tools to ensure compliance**...These enforcements send out an important message about compliance issues and the need for covered entities and business associates to take their obligations seriously."

Roger Severino, Director of OCR

"I'd like to find the big, juicy, egregious case. That's what I am looking for. I haven't zoomed in on a particular area, whether it's going to be cybersecurity/ransomware/physical security, etc….it probably wouldn't be the best law enforcement tactic to announce 'Hey, this is the type of thing we're looking for'."

September 5, 2017 comments during the "Safeguarding Health Information: Building Assurance through HIPAA Security-2017" conference.

True or False?

The penalties for OCR enforcement actions have increased since 2014.

Resolution Agreements, 2014

- In **2014**, there were **6** reported resolution agreements with the OCR.
- The average fine issued is valued at **$1,323,370**.

Resolution Agreements, 2014

1. HIPAA Settlement Underscores the Vulnerability of Unpatched and Unsupported Software - December 2, 2014
2. $800,000 HIPAA Settlement in Medical Records Dumping Case - June 23, 2014
3. Data Breach Results in $4.8 Million HIPAA Settlements - May 7, 2014
4. Concentra Settles HIPAA Case for $1,725,220 - April 22, 2014
5. QCA Settles HIPAA Case for $250,000 – April 22, 2014
6. County Government Settles Potential HIPAA Violations - March 7, 2014

Source: OCR website http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html

Resolution Agreements, 2015

- In **2015**, there were **6** reported resolution agreements with the OCR.
- The average fine issued is valued at **$1,032,233**.

Resolution Agreements, 2015

1. $750,000 HIPAA Settlement Underscores the Need for Organization Wide Risk Analysis - December 14, 2015
2. Triple-S Management Corporation Settles HHS Charges by Agreeing to $3.5 Million HIPAA Settlement - November 30, 2015
3. HIPAA Settlement Reinforces Lessons for Users of Medical Devices - November 24, 2015
4. 750,000 HIPAA Settlement Emphasizes the Importance of Risk Analysis and Device and Media Control Policies - August 31, 2015
5. HIPAA Settlement Highlights Importance of Safeguards When Using Internet Applications - June 10, 2015
6. HIPAA Settlement Highlights the Continuing Importance of Secure Disposal of Paper Medical Records - April 22, 2015

Resolution Agreements, 2016

- In **2016**, there were **13** reported resolution agreements with the OCR.
- The average fine issued is valued at **$1,808,100**.

Resolution Agreements, 2016

1. UMass settles potential HIPAA violations following malware infection – November 22, 2016
2. $2.14 million HIPAA settlement underscores importance of managing security risk – October 17, 2016
3. HIPAA settlement illustrates the importance of reviewing and updating, as necessary, business associate agreements – September 23, 2016
4. Advocate Health Care Settles Potential HIPAA Penalties for $5.55 Million - August 4, 2016
5. Multiple alleged HIPAA violations result in $2.75 million settlement with the University of Mississippi Medical Center (UMMC) - July 21, 2016
6. Widespread HIPAA vulnerabilities result in $2.7 million settlement with Oregon Health & Science University - July 18, 2016
7. Business Associate's Failure to Safeguard Nursing Home Residents' PHI Leads to $650,000 HIPAA Settlement – June 29, 2016
8. Unauthorized Filming for "NY Med" Results in $2.2 Million Settlement with New York Presbyterian Hospital - April 21, 2016
9. $750,000 settlement highlights the need for HIPAA business associate agreements
10. Improper disclosure of research participants' protected health information results in $3.9 million HIPAA settlement - March 17, 2016
11. $1.55 million settlement underscores the importance of executing HIPAA business associate agreements - March 16, 2016
12. Physical therapy provider settles violations that it impermissibly disclosed patient information- February 16, 2016
13. Administrative Law Judge rules in favor of OCR enforcement, requiring Lincare, Inc. to pay $239,800 - February 3, 2016

Resolution Agreements, 2017

- In **2017**, there were **10** reported resolution agreements with the OCR.
- The average fine issued is valued at **$1,939,320**.

Resolution Agreements, 2017

1. Failure to protect the health records of millions of people costs entity millions of dollars - December 28, 2017
2. Careless handling of HIV information jeopardizes patient's privacy, costs entity $387k - May 23, 2017
3. Texas health system settles potential HIPAA violations for disclosing patient information - May 10, 2017
4. $2.5 million settlement shows that not understanding HIPAA requirements creates risk – April 24, 2017
5. No Business Associate Agreement? $31K Mistake - April 20, 2017
6. Overlooking risks leads to breach, $400,000 settlement - April 12, 2017
7. $5.5 million HIPAA settlement shines light on the importance of audit controls - February 16, 2017
8. Lack of timely action risks security and costs money - February 1, 2017
9. HIPAA settlement demonstrates importance of implementing safeguards for ePHI - January 18, 2017
10. First HIPAA enforcement action for lack of timely breach notification settles for $475,000 - January 9, 2017

Resolution Agreements, 2018

- So far this year, the OCR has issued **$3,600,000** in fines.

You Name It!

Can you name one of the most common causes of breaches resulting in resolution agreements? Hint: OCR has identified 5.

Common Causes of Breaches Resulting in Resolution Agreements

- Impermissible uses and disclosures of protected health information;
- Lack of safeguards of protected health information;
- Lack of patient access to their protected health information;
- Use or disclosure of more than the minimum necessary protected health information; and
- **Lack of administrative safeguards of electronic protected health information.**

True or False?

The number of incidents of ransomware attacks is declining.

Ransomware On the Rise

A 2016 federal interagency report on the topic called ransomware the “fastest growing malware threat,” with an average of more than 4,000 attacks each day in 2016, a 300% increase from the year before.

True or False?

The OCR believes that cyberattacks are really not that big of a deal.

Former Director Samuels on Ransomware

"**One of the biggest current threats to health information privacy is the serious compromise of the integrity and availability of data caused by malicious cyberattacks on electronic health information systems, such as through ransomware.**" July 11, 2016 blog post.

Name that Outcome!

Can you name 3 negative outcomes arising out of a ransomware attack?

Impacts of Ransomware

- May compromise patient care.
- May leave patients vulnerable.
- May leave employees vulnerable.
- May impact operations.

True or False?

HHS believes that it is not possible to prevent a ransomware attack.

"Dear Colleague" Letter from HHS

"***Ransomware attacks can be prevented***. Appropriate cybersecurity prevention measures, team member education, proper cyber hygiene, comprehensive backup and recovery procedures, and continuity planning are the best tools to combat ransomware. Just like health care professionals wash their hands before procedures, we need to develop the habit of keeping our systems and data healthy, secure and recoverable."

True or False?

Recently issued Guidance from HHS makes it clear that if your organization is a victim of ransomware, then the organization is the victim and there is no need to report to OCR because as a victim, the organization is not subject to the breach reporting provision if it reports the attack to law enforcement.

Former Director Samuels on Guidance

"The guidance makes **clear** that a ransomware attack usually results in a 'breach' of health care information under the HIPAA Breach Notification Rule. Under the rule, and as noted in the guidance, entities experiencing a breach of unsecure PHI must notify individuals whose information is involved in the breach."

Guidance Fact Sheet

In the Fact Sheet, HHS states that when ePHI "is encrypted as a result of a ransomware attack, **a breach has occurred** because the ePHI encrypted by the ransomware was acquired" by an unauthorized person, and, therefore, the ePHI was "disclosed" in violation of the Privacy Rule.

While HHS uses the phrase "**a breach has occurred**" in the Fact Sheet, it also acknowledges that while an impermissible disclosure is presumed to constitute a reportable breach under the Breach Notification Rule, that presumption can be overcome by demonstrating that there is a low probability that PHI has been compromised based on a risk assessment.

Can You Name It?

What are 3 pieces of guidance from HHS to help prevent ransomware attacks?

Guidance

- Conduct a risk analysis to identify threats and vulnerabilities to electronic protected health information (ePHI) and establish a plan to mitigate or remediate those identified risks;
- Implement procedures to safeguard against malicious software;
- Train authorized users on detecting malicious software and report such detections;
- Limit access to ePHI to only those persons or software programs requiring access; and
- Maintain an overall contingency plan that includes disaster recovery, emergency operations, frequent data backups, and test restorations.

True or False?

The OCR believes that ransomware is like any other security issue and your policies/risk analyses do not need to specifically take into account ransomware.

Beware of Ransomware

"Organizations need to take steps to safeguard their data from ransomware attacks."

Jocelyn Samuels, Former Director of OCR.

True or False?

If you are the victim of ransomware, it is an automatic breach.

Consider the 4 Factors

In the breach assessment, the following need to be considered:

1. the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. the unauthorized person who used the PHI or to whom the disclosure was made;
3. whether the PHI was actually acquired or viewed; and
4. the extent to which the risk to the PHI has been mitigated.

Creative Thinking Challenge

How can you prove Lo-Pro-Co in a ransomware analysis?

How Does This Translate?

1. Can you confirm the malware impacted your operations?
2. Was the data already encrypted?
3. The type of ransomware employed
   a. Can you trace the commands
      i. Did it exfiltrate?
      ii. Did it propagate?
      iii. Did it delete the data?
4. Can you restore the PHI through backups?

Trends in Data Breach Litigation

- One of the fastest growing areas in civil litigation.
- Relatively new area of the law.
- Not static as the result of changes in technology and societal attitudes toward privacy.
- Some trends, however, have developed in the areas of standing, theories of liability, damages, and class certification.

Standing

- Has the plaintiff suffered an injury in fact sufficient to support standing to sue?
- Most cases of theft, loss, or compromise do not lead to immediate fraud or misuse.
- Issue: Is the possibility of future injury sufficient to support standing to sue?

Evolution of Data Breach Standing

- Early data breach cases were often dismissed for lack of standing.
- Cases in the Seventh and Ninth Circuit started reversing that trend.
- Clapper v. Amnesty International, 133 S. Ct. 1138 (2013)
  - Holding: Threatened injury must be "certainly impending."

Evolution of Data Breach Standing (Continued)

- In re Adobe Systems, Inc., 66 F. Supp. 3d 1197 (N.D. Cal 2014)
  - Certainly impending standard satisfied.
  - Proof that information had been stolen and surfaced on the internet.

Evolution of Data Breach Standing (Continued)

- Remijas v. Nieman Marcus Group, LLC, 794 F.3d 688 (7th Cir. (Ill.) 2015)
  - Certainly impending standard satisfied.
  - Cited Adobe.
  - Nieman Marcus offered credit monitoring and theft protection to improve public relations, and the court used that against Nieman Marcus in deciding whether injury was "certainly impending."

Theories of Liability

- Tort Theories
  - Negligence
    - Breach of duty nearly assumed by reason of hacking event
    - Economic loss doctrine
  - Negligence per se
    - HIPAA
  - Invasion of Privacy
    - Requires publication of the stolen information

Theories of Liability (Continued)

- Breach of Contract
  - Privacy policy
  - Terms of service
- Bailment
- Consumer Protection Statutes
- Data breach notification laws

Theories of Liability (Continued)

- Federal Statutes
  - Fair Credit Reporting Act
  - Stored Communications Act
- Some state specific laws
  - California: Confidentiality of Medical Information Act

Theories of Damages

- Future losses
- Mitigation expenses
- Actual out-of-pocket
- Time/inconvenience
- "Benefit of the bargain"
- Non-economic damages
- Statutory damages

Class Certification

- In re Hannaford Co. Customer Data Breach Litigation, 293 F.R.D. 21 (D. Me. 2013)
  - Class not certified: Questions of law or fact did not predominate.
- In re Target Corp. Customer Data Security Breach Litigation, 309 F.R.D. 482 (D. Minn. 2015)
  - Class certified, but not a consumer class action.

OCR RANSOMWARE CHECKLIST

1. Must execute its response and mitigation procedures and contingency plans. For example, the entity should immediately fix any technical or other problems to stop the incident. The entity should also take steps to mitigate any impermissible disclosure of protected health information, which may be done by the entity's own information technology staff, or by an outside entity brought in to help (which would be a business associate, if it has access to protected health information for that purpose).

   (Footnotes omitted)

OCR RANSOMWARE CHECKLIST
(continued)

2. Should report the crime to other law enforcement agencies, which may include state or local law enforcement, the Federal Bureau of Investigation (FBI), and/or the Secret Service. Any such reports should not include protected health information, unless otherwise permitted by the HIPAA Privacy Rule. If a law enforcement official tells the entity that any potential breach report would impede a criminal investigation or harm national security, the entity must delay reporting a breach (see below) for the time the law enforcement official requests in writing, or for 30 days, if the request is made orally.

OCR RANSOMWARE CHECKLIST
(continued)

3. Should report all cyber threat indicators to federal and information-sharing and analysis organizations (ISAOs), including the Department of Homeland Security, the HHS Assistant Secretary for Preparedness and Response, and private-sector cyber-threat ISAOs. Any such reports should not include protected health information. OCR does not receive such reports from its federal or HHS partners.

OCR RANSOMWARE CHECKLIST
(continued)

4. Must report the breach to OCR as soon as possible, but no later than 60 days after the discovery of a breach affecting 500 or more individuals, and notify affected individuals and the media unless a law enforcement official has requested a delay in the reporting. OCR presumes all cyber-related security incidents where protected health information was accessed, acquired, used, or disclosed are reportable breaches unless the information was encrypted by the entity at the time of the incident or the entity determines, through a written risk assessment, that there was a low probability that the information was compromised during the breach. An entity that discovers a breach affecting fewer than 500 individuals has an obligation to notify: individuals without unreasonable delay, but no later than 60 days after discovery; and OCR within 60 days after the end of the calendar year in which the breach was discovered.

Questions?

- Lucie F. Huger
  314/345-4725
  E-mail: lfh@greensfelder.com

- Kevin F. Hormuth
  314/516-2665
  E-mail: kfh@greensfelder.com