HHS Office for Civil Rights in Action

June 8, 2017

OCR Quick Response Cyber Attack Checklist and Graphic

The U.S. Department of Health & Human Services (HHS), Office for Civil Rights (OCR) has developed a checklist and a corresponding infographic that explains the steps for a HIPAA covered entity or its business associate (the entity) to take in response to a cyber-related security incident.

Materials:

- Cyber Security Checklist - PDF
- Cyber Security Infographic

A Quick-Response Checklist from the HHS, Office for Civil Rights (OCR)

In the event of a cyber-attack or similar emergency an entity:

- ☐ Must execute its response and mitigation procedures and contingency plans.[i] 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,[ii] 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,[iii] if it has access to protected health information for that purpose).

- ☐ 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.[iv] 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.[v]

- ☐ Should report all cyber threat indicators[vi] to the appropriate 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.[vii]

- Must report the breach[viii] 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.

OCR considers all mitigation efforts taken by the entity during in any particular breach investigation.[ix] Such efforts include voluntary sharing of non-protected breach-related information with law enforcement agencies and other federal and analysis organizations as described above.[x]

For more information regarding ransomware, visit https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

---

[i] The HIPAA Security Rule requires HIPAA covered entities and business associate to identify and respond to suspect or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. See 45 C.F.R. § 164.308(a)(6). The HIPAA Security Rule also requires HIPAA covered entities and business associates to establish and implement contingency plans, including data backup plans, disaster recovery plans, and emergency mode operation plans. See 45 C.F.R. § 164.308(a)(7). See also https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf?language=es.

[ii] Protected health information or PHI includes all individually-identifiable health information held by HIPAA covered entities and business associate, except for employment records, records covered by FERPA, or information about individuals deceased more than 50 years. PHI includes any health information that relates to the care or payment for care for an individual, and includes, for example, treatment information, billing information, insurance information, contact information, and social security numbers. See also https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

[iii] A business associate includes any vendor that creates, receives, maintains, or transmits protected health information (PHI) for or on behalf of a HIPAA covered entity. This includes vendors that have access to PHI to provide IT-related services to the covered entity. See 45 C.F.R. § 164.103, § 164.308, and § 164.502. See also https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html.

[iv] The HIPAA Privacy Rule permits the disclosure to law enforcement agencies under certain circumstances. See 45 C.F.R. § 164.512(f). See also https://www.hhs.gov/hipaa/for-professionals/faq/505/what-does-the-privacy-rule-allow-covered-entities-to-disclose-to-law-enforcement-officials/index.html.

[v] See the HIPAA Breach Notification Rule at 45 C.F.R. § 164.412.

[vi] The Cybersecurity Information Sharing Act of 2015 (CISA) describes cyber threat indicators as information that is necessary to describe or identify: malicious reconnaissance; methods of defeating a security control or exploitation of a security vulnerability; a security vulnerability; methods of causing a user with legitimate access to defeat of a security control or exploitation of a security vulnerability; malicious cyber command and control; a description of actual or potential harm caused by an incident; any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or any combination thereof. See also https://www.hhs.gov/hipaa/for-professionals/faq/2072/covered-entity-disclose-protected-health-information-purposes-cybersecurity-information-sharing/index.html.

[vii] The Cybersecurity Information Sharing Act of 2015 (CISA) in Sec. 106 provides that "Liability protections are provided to entities acting in accordance with this title that: (1) monitor information systems; or (2) share or receive indicators or defensive measures, provided that the manner in which an entity shares such indicators or measures with the federal government is consistent with specified procedures and exceptions set forth under the DHS sharing process."

[viii] Breaches affecting fewer than 500 individuals should be reported to affected individuals as soon as possible, but within no later than 60 days, and reported to OCR within 60 days of the end of the calendar year in which the breach was discovered. See the HIPAA Breach Notification Rule at 45 C.F.R. § 164.404 and 164.408. See the HIPAA Breach Notification Rule at 45 C.F.R. § 164.402-414.

[ix] The HIPAA Enforcement Rule includes provides that in determining the amount of any applicable civil money penalty, OCR may consider mitigating factors, including matters that justice may require. See 45 C.F.R. § 160.408(e). See also https://www.hhs.gov/hipaa/for-professionals/special-topics/enforcement-rule/index.html.

[x] The HIPAA Privacy Rule permits the disclosure to law enforcement agencies under certain circumstances. See 45 C.F.R. § 164.512(f). See also https://www.hhs.gov/hipaa/for-professionals/faq/505/what-does-the-privacy-rule-allow-covered-entities-to-disclose-to-law-enforcement-officials/index.html.