

***Policy Analysis –***

Last week, [we looked at](https://nhisac.org/august-15-2017-federal-government-incident-response/) how the federal government organizes itself to support critical infrastructure in responding to significant cyber incidents that threaten national security. Today we will focus on the regulatory expectations for health care organizations responding to a cyber breach.

The primary federal regulator in this space is HHS’s Office of Civil Rights (OCR), which has responsibility for administering the Health Insurance Portability and Accountability Act (HIPAA). To implement its authorities under HIPAA, OCR published the [HIPAA Security Rule](https://www.hhs.gov/hipaa/for-professionals/security/index.html) (first proposed in 1998, finalized in 2003). The Security Rule “establishes national standards to protect individuals’ electronic personal health information that is created, received, used, or maintained by a covered entity.” This includes considerations for not only how to protect information, but also how to respond and recover from incidents that may compromise protected health information.

When an incident occurs, OCR is unequivocal in saying that a covered entity “must execute its response and mitigation procedures and contingency plans.” The clear message is that a health care organization should first worry about defending its own systems and mitigating the threat. Only after an incident is under control, should it begin considering regulatory reporting requirements. After all, HIPAA gives an entity up to 60 days after discovery to report a breach. If a health care organization has considered HIPAA expectations in advance, incident response should occur in a way that is easy to document and present to regulators if PHI is compromised and an investigation is conducted later.

As part of its incident response procedures, health care entities should also have a mechanism for reporting the incident to law enforcement agencies. Notifying law enforcement of an incident will enable a criminal investigation that can lead to the arrest and prosecution of those responsible, but it can also get your incident into the process set forth in PPD-41 and described last week. Law enforcement may also provide helpful network defense information if the incident is part of a larger campaign that they are already investigating.

Sharing information through NH-ISAC should also be part of your response plans. Actively sharing information informs your network defense, as well as enabling others in the sector to defend against similar threats. And sharing with NH-ISAC enables the sector to coordinate its response to campaigns or widespread attacks, freeing you to focus on your own enterprise. It is important to note that NH-ISAC does not share any cyber-threat indicators or incident information with OCR or other federal regulators.

OCR provides many helpful documents on the HIPAA [Security Rule](https://www.hhs.gov/hipaa/for-professionals/security/index.html) and [Privacy Rule](https://www.hhs.gov/hipaa/for-professionals/privacy/index.html). These include an [incident response checklist](https://www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf), and [quick response graphic](https://www.hhs.gov/sites/default/files/cyber-attack-quick-response-infographic.gif), in addition to the previously referenced resources. I recommend engaging your [local OCR Regional Office](https://www.hhs.gov/ocr/about-us/contact-us/index.html) with any questions on how to consider your responsibilities under the law.

***Hot Links* –**

[NIST proposes update to its cybersecurity controls](https://www.nist.gov/news-events/news/2017/08/nist-crafts-next-generation-safeguards-information-systems-and-internet) – Last week, NIST released a proposed update to its [special publication 800-53](http://csrc.nist.gov/publications/drafts/800-53/sp800-53r5-draft.pdf), which informs how federal agencies secure their digital infrastructure. SP 800-53 is also highly referenced by the private sector, including in the HIPAA Security Rule and the NIST Framework. The proposed revision integrates privacy considerations throughout its set of controls, and adds new controls related specifically to privacy, such as how sensors capture and store data in a way that protects individual privacy. This is, of course, relevant to the healthcare sector and worth your attention. Comments are due by September 12.

--[NIST Releases update of 800-53](http://www.nextgov.com/cybersecurity/2017/08/nist-releases-updated-cyber-and-privacy-guidance-draft/140265/?oref=ng-relatedstories) (NextGov)

--[Draft for public comment](http://csrc.nist.gov/publications/drafts/800-53/sp800-53r5-draft.pdf) (NIST)

--[New NIST draft embeds privacy into US govt security for the first time](https://www.theregister.co.uk/2017/08/18/new_nist_draft_embeds_privacy_into_security_for_the_first_time/) (the Register)

--The President’s National Infrastructure Advisory Council [released a report](https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17-508.pdf) on securing cyber assets within U.S. critical infrastructure. This report calls for actions to prevent or mitigate catastrophic impacts that may result from a cyber-attack against U.S. critical infrastructure. Many of the recommendations echo those within the Healthcare Task Force report earlier this year, although on a broader scale that reflects the multi-sector remit of the council. The council asks for a response from the Administration within six months.

--HHS Assistant Secretary starts work -- Robert P. Kadlec was [recently confirmed](https://www.senate.gov/legislative/nom_confc.htm) as Assistant Secretary for Preparedness and Response, in which capacity he will serve as the official responsible for working with the healthcare sector on protecting itself from cyber-attacks.

--[Trump order elevates cyber command](http://www.nextgov.com/cybersecurity/2017/08/trump-order-elevates-cyber-command/140344/) (NextGov); [Memorandum to the Secretary of Defense](https://www.whitehouse.gov/the-press-office/2017/08/18/presidential-memorandum-secretary-defense) (WH); [Statement by President Donald J. Trump on the Elevation of Cyber Command](https://www.whitehouse.gov/the-press-office/2017/08/18/statement-donald-j-trump-elevation-cyber-command) (WH)

--[VA sued over Cerner contract](http://www.healthcareitnews.com/news/ehr-vendor-clinicomp-sues-government-over-no-bid-va-contract-cerner) (Healthcare IT News)

**--**[The FBI is briefing US companies against using Kaspersky products, claims report](https://www.grahamcluley.com/fbi-briefing-us-companies-using-kaspersky-products-claims-report/) (Cluley)

--[Microsoft wins major court victory against DNC hackers](http://thehill.com/policy/cybersecurity/347627-microsoft-wins-major-court-victory-against-dnc-hackers) (The Hill)

--[More North Korea Sanctions](http://www.politico.com/story/2017/08/22/sanctions-china-russia-north-korea-241900) (Politico)

***The Week Ahead* –**

*Administration activity –* There are rumors that the Administration is getting ready to release a cyber deterrence strategy, but nothing has been made public as of now. Watch this space.

--[FDA Reauthorization signed into law](https://www.congress.gov/bill/115th-congress/house-bill/2430/text) – no mention of cybersecurity in the updated legal text

*Congressional Activity –* The House and Senate are both in recess, though the Senate continues *pro forma* sessions, which means that recess appointments are unlikely. Both chambers are likely to return to business after Labor Day on September 5.

*Conferences and Webinars –*

--[Basic Best Practices in Cybersecurity – Texas](https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-texas/) (NH-ISAC) (8/23)

--[HIPAA Training for the Business Associate](http://www.mentorhealth.com/control/w_product/~product_id%3D801043LIVE?infosec-conferences.com_Aug_2017_SEO) (webinar) (8/23)

--[HIPAA and Personal Devices](http://www.mentorhealth.com/control/w_product/~product_id%3D801044LIVE?infosec-conferences.com_Sep_2017_SEO) (webinar) (9/5)

--[Basic Best Practices in Cybersecurity – Minnesota](https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-minnesota/) (NH-ISAC) (9/6)

--[Medical Device Workshop at Medtronic – Mounds View, MN](https://nhisac.org/events/nhisac-events/nh-isac-mdiss-medical-device-cyber-security-workshop-sept-7/) (NH-ISAC) (9/7)

--[HIMSS Healthcare Security Forum](http://www.healthcaresecurityforum.com/boston/2017?utm_source=hitn&utm_medium=news&utm_term=ridge&utm_content=ridge&utm_campaign=register-now) (9/11-13)

--[Billington CyberSecurity Summit](https://www.billingtoncybersecurity.com/8th-annual-billington-cybersecurity-summit/) (9/13)

--[Basic Best Practices in Cybersecurity - Alabama](https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-alabama/) (NH-ISAC) (9/15)

--[NH-ISAC Fall Summit – Cyber Rodeo](https://nhisac.org/events/cyber-rodeo/) (11/28-30)

***Reports –***

--[Protenus: Hacking Incidents Outweigh Insider Breaches in July](https://www.healthcare-informatics.com/news-item/cybersecurity/protenus-hacking-incidents-outweigh-insider-breaches-july)

***Sundries –***

*August Vacation reading:*

--[Mobile device security for the road warrior](http://www.csoonline.com/article/3216468/mobile/mobile-device-security-for-the-road-warrior.html) (CSO)

*Policy:*

--[ONC, AHRQ would see budgets slashed under proposed House spending bill](http://www.healthcareitnews.com/news/onc-ahrq-would-see-budgets-slashed-under-proposed-house-spending-bill) (Healthcare IT News)

--[Uber Agrees to 20 Years of Privacy Audits by the FTC](https://www.infosecurity-magazine.com/news/uber-agrees-to-20-years-of-privacy/) (info security)

--[China opens its first ‘cyber court’](http://www.securityweek.com/china-opens-its-first-cyber-court) (Security Week)

*Government Cybersecurity:*

--[VA-DoD: Winning the Battle for Interoperability](https://www.healthcare-informatics.com/blogs/david-levin/interoperability/va-dod-winning-battle-interoperability) (Healthcare Informatics)

--[Officials: State Dept suffers worldwide email outage](https://federalnewsradio.com/cybersecurity/2017/08/officials-state-dept-suffers-worldwide-email-outage/) (Federal News)

--[Russian-Speaking APT Engaged in G20 Themed Attack](https://www.darkreading.com/attacks-breaches/russian-speaking-apt-engaged-in-g20-themed-attack/d/d-id/1329673) (Dark Reading)

--[U.S. Army to Protect Warfighters With Continuous Biometric Authentication](http://www.securityweek.com/us-army-protect-warfighters-continuous-biometric-authentication) (Security Week)

--[USS John S McCain incident, some experts speculate it was a cyber attack](http://securityaffairs.co/wordpress/62270/cyber-warfare-2/uss-john-s-mccain-incident.html) (Security Affairs)

*Op-eds:*

--[What New Research Says about Which Federal Financial Incentives Produce Health System Change](https://www.healthcare-informatics.com/blogs/mark-hagland/payment/what-new-research-says-about-which-federal-financial-incentives-produce) (Healthcare Informatics)

--[Invisible Hands and Iron Fists: Challenges in Regulating the Innovation Economy](https://www.lawfareblog.com/invisible-hands-and-iron-fists-challenges-regulating-innovation-economy) (Law Fare)

--“[Regulators in Cyberia](https://regproject.org/wp-content/uploads/RTP-Cyber-Privacy-Working-Group-Paper.pdf)” (Regulatory Transparency Project)

--['Every country should have a cyber war’: what Estonia learned from Russian hacking](http://www.nextgov.com/cybersecurity/2017/08/every-country-should-have-cyber-war-what-estonia-learned-russian-hacking/140221/) (NextGov)

--[Critical Infrastructure, Cybersecurity & the 'Devil’s Rope'](https://www.darkreading.com/vulnerabilities---threats/critical-infrastructure-cybersecurity-and-the-devils-rope/a/d-id/1329639) (Dark Reading)

--[How likely is a ‘digital Pearl Harbor’ attack on critical infrastructure?](https://nakedsecurity.sophos.com/2017/08/18/how-likely-is-a-digital-pearl-harbor-attack-on-critical-infrastructure/) (Naked Security)

--[Curbing the Cybersecurity Workforce Shortage with AI](https://www.darkreading.com/threat-intelligence/curbing-the-cybersecurity-workforce-shortage-with-ai/a/d-id/1329617) (Dark Reading)

*Tech:*

--[Tech Leaders Warn Against "Pandora's Box" of Robotic Weapons](http://www.securityweek.com/tech-leaders-warn-against-pandoras-box-robotic-weapons) (security week)

--[Blockchain Standards being influenced by FSB?](https://www.lawfareblog.com/blockchain-standards) (LawFare)

*Threats:*

--[Attackers turn to auto-updating links instead of macros to deliver malware](https://www.helpnetsecurity.com/2017/08/18/auto-updating-links-malware/) (HelpNetSecurity)

--[‘Pulse wave’ DDoS – another way of blasting sites offline](https://nakedsecurity.sophos.com/2017/08/18/pulse-wave-ddos-another-way-of-blasting-sites-offline/) (Naked Security)

-- [It’s baaaack: Locky ransomware is on the rise again](https://nakedsecurity.sophos.com/2017/08/17/its-baaaack-locky-ransomware-is-on-the-rise-again/) (Naked Security)

--[Cyber Criminals Hijack Chrome Extensions and put 4.7 Million Users at Risk](http://securityaffairs.co/wordpress/62090/hacking/chrome-extensions-risks.html) (Security Affairs)

*Network defense and vulnerabilities:*

--[Texas Healthcare Privacy, Security Focus in Recent Partnership](https://healthitsecurity.com/news/texas-healthcare-privacy-security-focus-in-recent-partnership) (Health IT Security)

--[Improve Healthcare Authentication with New NIST Guide](https://healthitsecurity.com/news/improve-healthcare-authentication-with-new-nist-guide) (Health IT Security)

--[Carbon Emissions: Oversharing Bug Puts Security Vendor Back in Spotlight](https://krebsonsecurity.com/2017/08/carbon-emissions-oversharing-bug-puts-security-vendor-back-in-spotlight/) (Krebs)

--[Decryption Key for Apple's SEP Firmware Posted Online](http://www.securityweek.com/decryption-key-apples-sep-firmware-posted-online) (Security Week)

--[It’s not exactly open season on the IOS Secure Enclave](https://threatpost.com/its-not-exactly-open-season-on-the-ios-secure-enclave/127533/) (Threat Post)

--[Patching Against the Next WannaCry Vulnerability (CVE-2017-8620)](http://www.securityweek.com/patching-against-next-wannacry-vulnerability-cve-2017-8620) (Security Week)

--[Facebook Doles Out $100K for Internet Defense Prize](https://www.darkreading.com/endpoint/facebook-doles-out-%24100k-for-internet-defense-prize/d/d-id/1329667) (Dark Reading)

--[Web Application Attacks Much More Common Than Ransomware](https://www.infosecurity-magazine.com/news/web-application-attacks-ansomware/) (info security)

--[Cybersecurity Pros Aren't Getting the Training They Need, Including in DevOps](https://www.infosecurity-magazine.com/news/cybersecurity-pros-training-devops/) (info security)

--[Three barriers to digital IDs on the blockchain](https://www.helpnetsecurity.com/2017/08/18/digital-ids-blockchain/) (HelpNetSecurity)

--[Unfixable Automobile Computer Security Vulnerability](https://www.schneier.com/blog/archives/2017/08/unfixable_autom.html) (Schneier)

--[Xerox CISO: How business should prepare for the future security threat landscape](http://www.csoonline.com/article/3217305/security/xerox-ciso-how-business-should-prepare-for-the-future-security-threat-landscape.html) (CSO)

--[So long and thanks for all the phish: Red teams need to be smarter now](https://www.theregister.co.uk/2017/08/18/red_team_tactics/) (the Register)

--[8 top cyber-attack maps and how to use them](http://www.csoonline.com/article/3217944/security/8-top-cyber-attack-maps-and-how-to-use-them.html) (CSO)

***(In)Secure Takes* –** Twitter’s best from the week



Contact us: follow @NHISAC and email at bflatgard@nhisac.org