SQUIRE PATTON BOGGS

HHS Issues Cybersecurity Guidance

The Department of Health and Human Services (HHS) recently issued a report highlighting the largest threats facing the healthcare industry and 10 risk-prioritized recommended cybersecurity best practices to combat those threats. Although nonbinding, this guidance provides insight into HHS' expectations for organizations of all types and sizes and may indicate enforcement priorities as well.

The main report, titled "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients" (the "Report"), is coupled with two technical volumes for IT professionals and a companion guide containing additional resources and templates (collectively, the "HHS Guidance"). Advanced copies of HHS' upcoming "Cybersecurity Practices Assessments Toolkit," which HHS says will help organizations prioritize their cyber threats and develop their own action plans, are also available upon request.

What Prompted HHS to Issue This Guidance Now?

The Cybersecurity Act of 2015 (the "Cyber Act") required HHS to develop a "common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes" aimed at cost-effectively strengthening cybersecurity in the healthcare industry. Congress called on HHS to collaborate with the Department of Homeland Security (DHS), the Director of the National Institute of Standards and Technology (NIST), and other healthcare industry stakeholders to meet this goal. Acting on Congress' mandate, HHS assembled a task force consisting of more than 150 public and private sector healthcare and cybersecurity experts that worked on the HHS Guidance over the past 20 months.

As HHS emphasizes in its Report, the HHS Guidance is also timely given the heightened risks to healthcare organizations from hackers seeking the vast amounts of sensitive personal, financial, and health information that healthcare professionals collect daily. These attacks, as HHS reports, are having devastating and far-reaching effects on the industry.

Cybersecurity Threats Facing the Healthcare Industry and HHS-recommended Mitigation Practices

The HHS Guidance focuses on technical and nontechnical recommendations to address five cybersecurity threats that the task group determined to be the "most current and common" in the healthcare industry today. These include:

- Email phishing attacks
- Ransomware attacks
- Loss or theft of equipment or data
- Insider, accidental or intentional data loss
- Attacks against connected medical devices that may affect patient safety

These threats are coupled with short descriptions, mock real-world scenarios of how they might arise, explanations of potential impact, a series of recommended procedure-strengthening "Threat Quick Tips," and corresponding references to the companion technical volumes. The technical volumes themselves address 10 HHS-recommended "Cybersecurity Practices," aligned with 88 related "sub-practices" that are cross-referenced to NIST's Cybersecurity Framework. The top-level Cybersecurity Practices include:

- Email protection systems
- Endpoint protection systems
- Access management
- Data protection and loss prevention
- Asset management
- Network management
- Vulnerability management
- Incident response
- Medical device security
- Cybersecurity policies

The companion technical volumes contain specific recommendations for small (Volume 1) and medium-to-large (Volume 2) healthcare organizations. Reflecting the Health Insurance Portability and Accountability Act's (HIPAA's) approach to risk-based and resource-based security practices, the recommendations scale from 19 sub-practices for small organizations, to 37 sub-practices for medium organizations, and finally to all 88 sub-practices for large organizations.

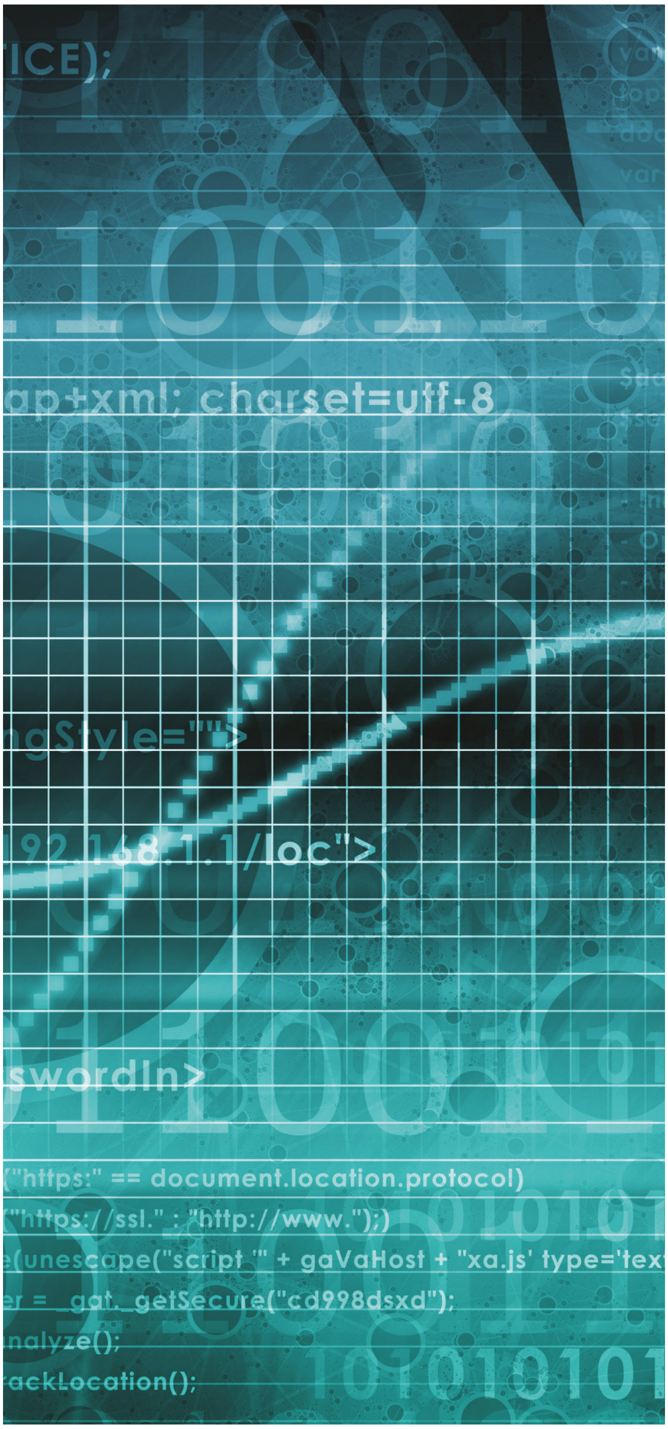
Did Congress Unintentionally Disrupt the Healthcare Industry?

Congress and the task group emphasize that the HHS Guidance does not create a new "mandatory" cybersecurity framework. However, the guidance is still likely to be relevant when regulators and courts are tasked with interpreting the "reasonableness" of security safeguards. For example, HHS may look to the guidance during audits and investigations to assess how companies implement the somewhat flexible HIPAA security requirements. Courts may similarly rely on the HHS Guidance in post-breach litigation, where plaintiffs frequently seek to establish "negligence" claims by reference to industry benchmarks and other guidance.

Does This New Cybersecurity Guidance Require Action Now?

A good defense is the best offense. The guidance itself says it is not prescriptive, but savvy healthcare companies should at least "kick the tires" to evaluate any gaps against the HHS Guidance. It also may help organizations to better understand how to prioritize and actually implement HIPAA security requirements. Finally, HHS may look favorably upon a company that has at least attempted to incorporate these recommendations into its cybersecurity program in the event of a breach or other OCR investigation.

For more information or assistance with the HHS Guidance, please contact the authors of this article, or your normal firm contact, and we will be happy to help.



ICE);
ap+xml; charset=utf-8
ngStyle="">
192.168.1.1/loc">
swordIn>
("https:" == document.location.protocol)
("https://ssl." : "http://www.");)
e(unescape("script '" + gaVaHost + "xa.js' type='tex
er = _gat._getSecure("cd998dsxd");
nalyze();
ackLocation();

Contacts

Elliot R. Golding
Partner, Washington DC
T +1 202 457 6407
E elliot.golding@squirepb.com

Daniel E. Vinish
Of Counsel, New York
T +1 212 872 9814
E daniel.vinish@squirepb.com

The contents of this update are not intended to serve as legal advice related to individual situations or as legal opinions concerning such situations, nor should they be considered a substitute for taking legal advice.