

November 7, 2017



Life's inevitabilities: bills, taxes, ransom – this week's *Hacking Healthcare*:  
TLP White

### **Hot Links –**

1. **Ransomware in 2018** – The Emergency Care Research Institute this week [ranked](#) ransomware as their top health technology [hazard for 2018](#). This is probably unsurprising to most in the NH-ISAC community who have been dealing with the plague of ransomware for much of the last two years. The important acknowledgment is in the risk to patient safety that new ransomware attacks might pose. As we've seen, operational technology and medical devices are susceptible to ransomware and are being deliberately targeted. That's *my* top threat for 2018 – [IoT](#) attacks that hold physical activity ransom.
2. **HHS Cyber Bill** – A bipartisan [bill](#) was introduced in the House last week that would give the HHS Secretary the authority to re-organize cybersecurity personnel. The bill would also require HHS to develop a plan that lays out its approach to coordinating within the department to address cybersecurity challenges. This would include regulatory (e.g., ONC, FDA, OCR) offices, as well as those offices charged with maintaining the resiliency of the sector against all hazards (i.e., ASPR). HHS would also have to report on how it secures its own systems. This bill is a step in the right direction – and consistent with HHS cyber [task force](#) recommendations – but needs funding attached to have more than marginal impact.
3. **To Protect [the Healthcare Sector] Cut Taxes** – [This piece](#), which focuses on creating positive security incentives within the Energy sector, resonates in terms of how we might create better cybersecurity outcomes in the healthcare sector. The new meaningful use requirements ([Stage 3](#) and the enhanced oversight and accountability [rule](#)) are placing higher value on security within the HIT marketplace. But there is also a large base of unsecured legacy devices and administrative systems within the healthcare environments. Should we be looking at tax credits or grants for the purchase of secure systems? As foreign adversaries target the health sector with debilitating attacks, cyber-

November 7, 2017

resiliency needs to be prioritized. The HHS cyber [task force](#) also identified some recommendations in this space.

### ***Congress –***

Tuesday, November 7:

--Hearings to examine advancing the Internet of Things in rural America. ([Senate Commerce](#))

Wednesday, November 8:

--Confirmation Hearing for Kirstjen Nielsen, nominee to be Department of Homeland Security ([Senate Homeland](#))

--Hearing to examine protecting consumers in the era of major data breaches. ([Senate Commerce](#))

--Hearing: "Cybersecurity of Voting Machines" ([House Oversight](#))

### ***Conferences and Webinars –***

--[Business E-mail Compromise \(BEC\) Workshop](#) – Kansas City, MO (NH-ISAC) (11/7)

--[Biotech/Pharma Security Workshop at MSD, Prague](#) (NH-ISAC) (11/7)

--[Business E-mail Compromise \(BEC\) Workshop](#) – Los Angeles, CA (NH-ISAC) (11/8)

--[Health IT Summit](#) – Los Angeles, CA (NH-ISAC) (11/9)

--[Cyber Outbreak TTX](#) (NH-ISAC) (11/27)

--[NH-ISAC Fall Summit – Cyber Rodeo](#) (11/28-30)

--[Regional Healthcare Cybersecurity Summit](#) – Hebron, KY (NH-ISAC) (12/7)

--[Health IT Summit – Dallas](#) (NH-ISAC) (12/14)

### ***Sundries –***

--Trump signs cybercrime bill ([the Hill](#))

--'Hack back' bill picks up new cosponsors (the Hill)

--Kaspersky acknowledges taking inactive files in pursuit of hackers ([Reuters](#))

-- Watchdog: DHS prioritizing speed over context for AIS program ([CyberScoop](#))

--Forget your fingerprint: New concept lets people pick their own two-factor token ([CyberScoop](#))

--Malaysian Data Breach Could Affect Entire Population ([InfoSec](#))

--Tech industry outlines proposals for online ad disclosure legislation ([the Hill](#))

Contact us: follow @NHISAC and email at [bflatgard@nhisac.org](mailto:bflatgard@nhisac.org)