January 26th, 2021

Hacking Healthcare

TLP White

This week, *Hacking Healthcare* begins with a brief overview of the HIPAA Journal's 2020 Healthcare Data Breach Report and zeros in on one particular vulnerability that the healthcare sector should look to address in 2021. Next, we update you on a German healthcare act that addresses the importance of security when it comes to IT modernization, and we consider how it might be a useful case study for appropriately crafted cybersecurity legislation going forward. Finally, another incident involving contact-tracing programs segues us into a broader discussion on remote work policies and their impact on IT security. Welcome back to *Hacking Healthcare*.

1. HIPAA Journal 2020 Healthcare Data Breach Report

The end of 2020 provides as good a marker as any to look back and assess the state of healthcare IT and security. Among a number of recently released end-of-year retrospectives is the HIPAA Journal's *2020 Healthcare Data Breach Report*, which helpfully collates the Department of Health and Human Services Office of Civil Rights' data breach information from the previous year.[1] This year's report provides some interesting figures to reflect on while also helpfully illustrating evidence of long-established security trends.

We've highlighted some of the key takeaways for you below:[2]

A 25% year-over-year increase in healthcare data breaches
According to the HIPAA Journal, healthcare data breaches have doubled since 2014, amounting to a 25% year-over-year increase.[3] What's more, the number of data breaches exposing more than 500 records in a year has been steadily climbing from 2010 to 2020.[4] While there were 199 such incidents in 2010, by 2019 that number had shot up to 512, and last year reached 642 reported incidents.[5]

Hacking/IT incidents accounted for 67% of data breaches and 92% of breached records
Hacking and IT incidents unsurprisingly led the way as the cause of data breaches at 67%. They also continued to solidify just how damaging they can be by representing nearly 92% of all breached records, a 5% increase over 2019.

Don’t Discount other Breach Causes

Unauthorized access/disclosure was the second most common cause of data breach at 22%, falling far behind hacking/IT incidents, but well ahead of theft at 6%, improper disposal at ~2.5%, and loss at ~2.5%. However, breaches defined as “loss” averaged twice the amount of records impacted as unauthorized access/disclosure and the median number of records breached as a result of loss (2,298) was second only to Hacking/IT incidents. Furthermore, while only sixteen improper disposal incidents were reported, they impacted nearly 585,000 records, an average of roughly 36,500 per incident.

Location, Location, Location

The location of breached healthcare data was primarily network servers and emails. Reminding us that not all security risks are cyber, coming in third was paper or film copies of PHI which were “were obtained by unauthorized individuals, lost, or disposed of in an insecure manner.”

HHS HIPAA Enforcement

According to the report, “More penalties were agreed with HIPAA covered entities and business associates in 2020 than in any other year since OCR started enforcing HIPAA compliance.” In total, $13,554,900 was reported to have been paid out. While the report acknowledges that investigations and settlements can run for years and may not accurately reflect the events of the year in which the penalties are reported, it also notes that “the large increase in financial penalties in 2020 is largely due to a HIPAA enforcement drive launched by OCR in late 2019 to tackle noncompliance with the HIPAA Right of Access.”

Action & Analysis

H-ISAC Membership Required

2. German Healthcare’s IT Security Booster Shot

Hospitals are among the more difficult entities to secure from an IT perspective. They need to operate a wide range of devices that can store or access highly sensitive and mission-critical data, while also allowing the continuous ingoing and outgoing of individuals, all while being a prime target for malicious cyber actors. Even so, finding the funding to invest in and maintain an ideal level of cybersecurity is no easy task. For German public hospitals, the government’s new Hospital Future Act (KHZG) may make this just a bit easier.

Coming into force in September 2020, the Act is designed to boost the digital maturity of the German healthcare sector “by improving patient care in hospitals, modernising IT structure, [and] improving cybersecurity measures.”[6] This modernization effort is backed by €4.3 billion in funding that could be allocated to public hospital projects such as “patient portals, electronic documentation of care and treatment services, digital medication management, IT security measures and cross-sectoral telemedical network structures. It can also be used to introduce or improve telemedicine, robotics, and high-tech medicine."[7]

Importantly, the Act would require that at least 15% of funding requested would be spent on improving IT security. However, public hospitals are not guaranteed to receive funding. Their requests appear to need approval from state authorities, and all plans must comply with the General Data Protection Regulation (GDPR)[8].

Action & Analysis
H-ISAC Membership Required

3. **COVID-19 Patient Data Has Been Sold Online for Months**

In what will likely add to skepticism and paranoia surrounding COVID-19 contact-tracing programs, two individuals were arrested late last week for allegedly selling patient information from the Dutch health ministry's COVID-19 contact-tracing system. While law enforcement authorities acted quickly in apprehending the two suspects, it was a news reporter who originally discovered the online advertisements for the data.[9]

According to the reporter, the ads for the stolen patient data were advertised on instant messaging apps such as Telegram and Snapchat. The ads included what appeared to be pictures taken from two separate Dutch Municipal Health Service applications that are part of their contact-tracing program. The records have allegedly been selling for between €30 to €50 per individual and contained "home addresses, emails, telephone numbers, dates of birth, and [the individual's national identification number]."[10]

More information will likely come to light as the court case against the alleged culprits proceeds. As of this moment, it is unknown exactly how long this information was made available, how many individuals may have been affected, or if this is a more widespread issue. What is known is that both suspects worked remotely for the Dutch Municipal Health Service call centers, which would have given them access to both systems.[11]

Action & Analysis
H-ISAC Membership Required

Congress –

Tuesday, January 26th:
- Senate – Homeland Security and Governmental Affairs: Business meeting to consider the nomination of Alejandro Nicholas Mayorkas, of the District of Columbia, to be Secretary of Homeland Security.

Wednesday, January 27th:
- No relevant hearings

Thursday, January 28th:
- No relevant hearings

International Hearings/Meetings –

- No relevant hearings

EU –

- No relevant hearings

Sundries –

Agencies Name Additional Biden Appointees with Tech Expertise

https://www.nextgov.com/cio-briefing/2021/01/agencies-name-additional-biden-appointees-tech-expertise/171621/

New AI model can predict length of COVID-19 hospitalization

https://www.healthcareitnews.com/news/new-ai-model-can-predict-length-covid-19-hospitalization

Conferences, Webinars, and Summits –

https://h-isac.org/events/

Contact us: follow @HealthISAC, and email at contact@h-isac.org

[1] https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/

[2] https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/

[3] https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/

[4] https://www.hipaajournal.com/wp-content/uploads/2021/01/us-healthcare-data-breaches-2009-2020.jpg

[5] https://www.hipaajournal.com/wp-content/uploads/2021/01/us-healthcare-data-breaches-2009-2020.jpg

[6] https://www.healthcareitnews.com/news/emea/german-hospitals-receive-digital-health-boost

[7] https://www.healthcareitnews.com/news/emea/german-hospitals-receive-digital-health-boost

[8] https://gdpr-info.eu/

[9] https://www.zdnet.com/article/dutch-covid-19-patient-data-sold-on-the-criminal-underground/

[10] https://www.zdnet.com/article/dutch-covid-19-patient-data-sold-on-the-criminal-underground/

[11] https://www.zdnet.com/article/dutch-covid-19-patient-data-sold-on-the-criminal-underground/