January 19th, 2021

TLP White

This week, *Hacking Healthcare* takes a look at a court ruling that could impact the Department of Health and Human Services (HHS) Office of Civil Rights' (OCR) imposition of penalties relating to HIPAA violations. Next, we briefly analyze some new data that suggests healthcare web applications are increasingly being targeted by malicious cyber actors, and we explore why a return to normalcy for healthcare cybersecurity may be a bit further down the line than we might hope. We then jump into the disturbing news that stolen documents related to COVID-19 vaccines were manipulated and leaked on the Internet and discuss their potential to stoke public mistrust. Finally, we quickly acknowledge the positives associated with HHS' apparent decision to appoint its first ever Chief Artificial Intelligence Officer. Welcome back to *Hacking Healthcare*.

1. **Major OCR Penalty Overturned by Appeals Court**

   Last Thursday, the U.S. Court of Appeals for the Fifth Circuit sided with the University of Texas M.D. Anderson Cancer Center over HHS in an appeal against a $4,348,000 judgment resulting from a HIPAA violation.[1] The decision represents a major win for M.D. Anderson, and it has potentially significant implications for civil monetary penalties in the context of HIPAA violations going forward.

   The appeal stems from an OCR investigation into three reported data breaches between 2012 and 2013. All three incidents involved electronic protected health information (ePHI) and included a stolen employee laptop, which was unencrypted and lacked password protections, and two unencrypted USB thumb drives which went missing.[2] OCR determined that these incidents, which affected roughly 35,000 patients, violated both the HIPAA privacy and security rule, with OCR charging that M.D. Anderson failed to implement an encryption mechanism for ePHI (protected health information) and improperly disclosed ePHI.[3]

   At the time of the original fine, the roughly $4.3 million penalty that HHS attempted to impose was reported to be the third largest HIPAA penalty to ever have been levied against a single covered entity.[4] M.D. Anderson twice contested OCR's determination, before finally petitioning the Fifth Circuit Court of Appeals.[5] The Fifth Circuit Court's decision ultimately determined that "[t]he Government's decision was arbitrary,

capricious, and contrary to law," with HHS conceding that it could not defend a fine in excess of $450,000.[6]

Action & Analysis
H-ISAC Membership Required

2. New Research Suggests Significant Rise in Health Web App Attacks

As malicious cyber actors continue to hammer the healthcare sector, new research from Imperva suggests they are continuing to evolve their tactics. In a post published last week, Imperva noted a 51% increase in web application attacks on healthcare targets and announced that the healthcare industry saw roughly 187 million of such attacks globally throughout 2020, which would amount to a 10% year-over-year increase.[7] The data available suggests that the United States, United Kingdom, Brazil, and Canada were the four countries most targeted.[8]

While these attacks have risen significantly in terms of volume over the past month, Imperva also reports that the number of reported breaches has declined. Rather than celebrating this point, however, Imperva posited that this lack of reported breaches is more likely due to organizations not yet recognizing the potential impacts of the attacks. They reason that in a year as challenging as 2020, many resources traditionally allocated toward threat research, incident response, and incident analysis have been needed elsewhere to shore up remote work and other issues.[9] Imperva supports this theory by noting a 43% increase in data leakage in the opening days of 2021.[10]

Action & Analysis
H-ISAC Membership Required

3. Stolen Vaccine Data Manipulated to Misinform

Back in December, we briefly covered how the European Medicines Agency (EMA) released a short and vague statement alerting the public to the fact that they had been "the subject of a cyberattack," but that they "[could not] provide additional details whilst the investigation was ongoing."[11] Since the initial press release, a series of updates have gradually clarified the situation, leading to the recent reveal of disturbing news that some amount of stolen documents and data related to COVID-19 vaccines were altered and posted to the Internet.

The cyberattack was originally disclosed on December 9th and prompted the EMA to quickly launch a full investigation "in close cooperation with law enforcement and other relevant entities."[12] Immediate updates in the wake of the attack suggested that "a limited number of documents belonging to third parties were unlawfully accessed," but the agency's operations were unaffected and the attack would not affect any evaluation or approval for COVID-19 vaccines or treatments.[13] However, a further update on January 12th revealed that some of the unlawfully accessed documents had been leaked to the Internet.

The twist to this story came on January 15th, when the EMA's 5th update revealed that the leaked documents, which "included internal/confidential email correspondence dating from November, relating to evaluation processes for COVID-19 vaccines," had been "manipulated by the perpetrators prior to publication in a way which could undermine trust in vaccines."[14] The EMA has not elaborated where the information was leaked or exactly how the documents were manipulated, but has promised further updates when appropriate.

Action & Analysis
H-ISAC Membership Required

4. HHS Names Chief Artificial Intelligence Officer

Earlier this month, reports surfaced that HHS was set to name Oki Mek to the newly created position of HHS Chief Artificial Intelligence Officer (CAIO). Oki Mek will come into the position with roughly two decades of experience related to "federal, technology-centered work."[15] He will be no stranger to HHS' work, having previously been a Senior Advisor to the Chief Information Officer and the Chief Technology Officer/Chief Product Officer in the Division of Acquisition at HHS.[16]

According to Nextgov, current HHS Chief Information Officer Perryn Ashmore made the decision to select Mek for the new position under the acknowledgement that "AI is playing and will continue to play a significant role in overall technology modernization."[17] Ashmore elaborated that the position will be responsible for coordinating the Office of the CIO's pursuits to implement the AI principles established in the Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government executive order.[18]

Details regarding specific projects and initiatives to be undertaken by the CAIO are still scarce at the time of writing, but the creation of the position is a positive. Artificial intelligence and machine learning have been highly touted in the healthcare sector for their ability to drive a wide range of administrative and clinical improvements, and having a dedicated position in HHS to support them reiterates HHS' commitment to this emerging technology. We will look to provide further updates as this position becomes settled.

Action & Analysis
H-ISAC Membership Required

January 19th, 2021

Congress –

Tuesday, January 19th:

- Senate – Committee on Homeland Security and Governmental Affairs: Hearings to examine the expected nomination of Alejandro N. Mayorkas, to be Secretary of Homeland Security.

Wednesday, January 20th:

- No relevant hearings

Thursday, January 21st:

- No relevant hearings

International Hearings/Meetings –

- No relevant hearings

EU –

Friday, January 22nd:

- European Commission – EU4Health Programme 2021-2027

Sundries –

CISA Warns of Vulnerabilities in Cloud Use, Shares Solutions List

https://www.nextgov.com/cybersecurity/2021/01/cisa-warns-vulnerabilities-cloud-use-shares-solutions-list/171427/

NSA warns against using DoH inside enterprise networks

https://www.zdnet.com/article/nsa-warns-against-using-doh-inside-enterprise-networks/

Conferences, Webinars, and Summits –

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

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

---

[1] https://www.ca5.uscourts.gov/opinions/pub/19/19-60226-CV0.pdf
[2] https://www.ca5.uscourts.gov/opinions/pub/19/19-60226-CV0.pdf
[3] https://www.natlawreview.com/article/fifth-circuit-court-appeals-vacates-md-anderson-hipaa-penalty
[4] https://www.hipaajournal.com/m-d-anderson-cancer-center-has-4-3-million-ocr-hipaa-fine-overturned-on-appeal/
[5] https://www.hipaajournal.com/m-d-anderson-cancer-center-has-4-3-million-ocr-hipaa-fine-overturned-on-appeal/
[6] https://www.ca5.uscourts.gov/opinions/pub/19/19-60226-CV0.pdf
[7] https://www.imperva.com/blog/web-application-attacks-on-healthcare-spike-51-as-covid-19-vaccines-are-introduced/
[8] https://www.hipaajournal.com/healthcare-industry-web-application-attacks-increased-by-51-in-december/
[9] https://www.imperva.com/blog/web-application-attacks-on-healthcare-spike-51-as-covid-19-vaccines-are-introduced/
[10] https://www.imperva.com/blog/web-application-attacks-on-healthcare-spike-51-as-covid-19-vaccines-are-introduced/
[11] https://www.ema.europa.eu/en/news/cyberattack-european-medicines-agency

[12] https://www.ema.europa.eu/en/news/cyberattack-ema-update-1
[13] https://www.ema.europa.eu/en/news/cyberattack-ema-update-1
[14] https://www.ema.europa.eu/en/news/cyberattack-ema-update-5
[15] https://www.nextgov.com/emerging-tech/2021/01/hhs-names-first-ever-chief-artificial-intelligence-officer/171439/
[16] https://www.g2xchange.com/statics/hhs-taps-oki-mek-to-serve-as-chief-artificial-intelligence-officer-caio/
[17] https://www.nextgov.com/emerging-tech/2021/01/hhs-names-first-ever-chief-artificial-intelligence-officer/171439/
[18] https://www.nextgov.com/emerging-tech/2021/01/hhs-names-first-ever-chief-artificial-intelligence-officer/171439/