



TLP White

This week, *Hacking Healthcare* begins by examining some early conversations amongst policymakers on the topic of vaccine cards and passports, specifically drawing attention to the security and privacy concerns of such credentialing. Next, we check-in on the progress being made on a US-EU Privacy Shield replacement and make the case for tempering expectations. Finally, we conclude by breaking down a new healthcare data risk report that suggests healthcare data overexposure is a global issue. Welcome back to *Hacking Healthcare*.

## 1. Vaccine Cards & Passports: Security and Privacy Issues

As the COVID-19 vaccine rollout continues and more restrictions ease, a concept that has been discussed since the beginning of the pandemic is taking shape – vaccine certification or passports to prove vaccination. This effort is not unique to the United States. Countries around the world are creating their own means for citizens to prove vaccination, and from country to country it varies if the public or private sector is trailblazing the effort.

There are also multinational efforts such as the World Health Organization’s “Smart Vaccination Certificate.” In the U.S., the private sector is largely driving the effort, albeit with strong support from the government. Jeff Zients, Biden administration COVID-19 “czar,” spoke on the concept of vaccination certification at a March 12 briefing:<sup>1</sup>

*“Also, as we increase the number of people vaccinated, we know some people may have a need to demonstrate that they are vaccinated. The private sector and not-for-profit coalitions are already beginning to work on this. Our role is to help ensure that any solutions in this area should be simple, free, open source, accessible to people both digitally and on paper, and designed from the start to protect people’s privacy.”*

Last week, New York launched the digital Excelsior Pass, which can be stored in the wallet app on phones. Businesses and venues can scan the QR code in the pass to verify that the individual has had a COVID-19 vaccine or a negative test result.<sup>2</sup> The Excelsior Pass is built on IBM’s digital health pass platform and uses blockchain technology to ensure neither IBM nor the business scanning the pass will have access to individuals’ personal and medical information.<sup>3</sup>

April 6th, 2021

Looking internationally, in March, the European Union launched “digital green certificates,” which will be a vaccination passport for the EU’s 440 million citizens and residents. The hope is that the certificates will be ready for use by June to encourage tourism in Europe over the summer months. The digital green certificate is expected to be available as both digital and paper documents. Unlike in the U.S., in Europe, national authorities such as hospitals, test centers, and health authorities will be responsible for issuing the certificates.<sup>4</sup>

In Israel, there is the “green pass,” which validates vaccination or COVID-19 recovery date to enter restaurants, gyms, and other venues. However, there have been privacy concerns with Israel’s green pass. Privacy experts in Israel claim that the pass reveals information to those checking the pass that they don’t need to know, uses an outdated encryption library that is more vulnerable to security breaches, and is easy to forge.<sup>5</sup> While an official at Israel’s Ministry of Health said that some of those issues have been fixed, the green pass problems raise a larger conversation about security in vaccine certification, passes, and passports, both in Israel and elsewhere.

#### ***Action & Analysis***

\*H-ISAC Membership Required\*

## **2. Biden Win May Signal Improved Prospects for New Data Privacy Agreement with EU**

It wasn’t altogether surprising when the Court of Justice of the European Union (“CJEU”) struck down the US-EU Privacy Shield last July, but the lack of an immediate replacement and slow progress towards a new agreement has left many organizations that operate in both markets in a confusing legal limbo. However, there is some sense that a Biden administration, being closer aligned to the EU in both policy and temperament than the previous administration, will improve the chances of a new deal being struck.

As we covered before, the Privacy Shield was created in 2016 and was designed to “provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data.”<sup>6</sup> It came together in the wake of the invalidation of its predecessor, the Safe Harbor, the year prior.<sup>7</sup> However, even before its adoption, critics believed that the Privacy Shield was flawed and was unlikely to survive legal scrutiny. Last July, that prediction was confirmed in a case brought by the same individual who invalidated the Safe Harbor, Max Schrems.

The CJEU’s ruling essentially held that data privacy and protection standards within the United States do not meet the legal requirements of the European Union, and the Privacy Shield does not effectively mitigate the differences in required protections.<sup>8</sup> In effect, CJEU noted that the surveillance laws within the United States are too overbearing and are in direct conflict with EU law. Despite this decision in *Schrems II*, there is some cause for optimism.

April 6th, 2021

According to the Agence France-Presse, EU Justice Commissioner Didier Reynders recently relayed that "[f]inding [a] solution is a priority in Brussels and in Washington DC."<sup>9</sup> He referred to the EU and US as like-minded partners and stated that it should be possible "to find appropriate solutions on principles that are cherished on both sides of the Atlantic."<sup>10</sup>

**Action & Analysis**

\*H-ISAC Membership Required\*

**3. New Healthcare Data Risk Report Highlights Concerns**

A new report from Varonis that "focuses on data security in the healthcare industry," including hospitals, pharmaceutical firms, and biotechnology companies, highlights a number of data-related concerns and considerations that healthcare organizations should be aware of, not least of which is the possibility of overexposure due to the number of accessible files open to employees and the prevalence of less than stellar password policies.

Varonis' *2021 Data Risk Report: Healthcare, Pharmaceutical & Biotech* was released last week and was compiled from data analysis of 3 billion files from 58 healthcare organizations of various sizes and specific industries globally.<sup>11</sup> Some of the more important takeaways included:<sup>12</sup>

- Nearly 20% of files are open to every employee in healthcare organizations (on average);
- On their first day, new employees at small companies have instant access to over 11,000 exposed files, and nearly half of them contain sensitive data;
- Larger organizations tended to have the most problems in their permissions structures, increasing the risk of data breaches stemming from cyberattacks;
- One-third of organizations evaluated had 10,000 files open to every employee; and
- 77% of the companies surveyed had 501 or more accounts with passwords that never expire, while 79% had more than 1,000 ghost users still enabled.

**Action & Analysis**

\*H-ISAC Membership Required\*

**Congress –**

Tuesday, April 4th:

- No relevant hearings

Wednesday, April 5th:

- No relevant hearings

Thursday, April 6th:

- No relevant hearings

April 6th, 2021

## ***International Hearings/Meetings –***

- No relevant hearings

## ***EU –***

- No relevant hearings

## ***Conferences, Webinars, and Summits –***

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

**Contact us: follow @HealthISAC, and email at [contact@h-isac.org](mailto:contact@h-isac.org)**

---

<sup>1</sup> <https://www.whitehouse.gov/briefing-room/press-briefings/2021/03/12/press-briefing-by-white-house-covid-19-response-team-and-public-health-officials-14/>

<sup>2</sup> <https://covid19vaccine.health.ny.gov/excelsior-pass>

<sup>3</sup> <https://www.usatoday.com/story/news/health/2021/03/26/covid-vaccine-passports-new-york-first-vaccination-proof-system/6976009002/>

<sup>4</sup> [https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/covid-19-digital-green-certificates\\_en](https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/covid-19-digital-green-certificates_en)

<sup>5</sup> <https://www.technologyreview.com/2021/03/01/1020154/israels-green-pass-is-an-early-vision-of-how-we-leave-lockdown/>

<sup>6</sup> <https://www.privacyshield.gov/welcome>

<sup>7</sup> <https://arstechnica.com/tech-policy/2020/07/court-tosses-us-eu-data-sharing-agreement-amid-us-surveillance-concerns/>

<sup>8</sup> <https://techcrunch.com/2020/07/16/europes-top-court-strikes-down-flagship-eu-us-data-transfer-mechanism/>

<sup>9</sup> <https://www.securityweek.com/eu-us-make-new-attempt-data-privacy-deal>

<sup>10</sup> <https://www.securityweek.com/eu-us-make-new-attempt-data-privacy-deal>

<sup>11</sup> [https://info.varonis.com/hubfs/Files/docs/research\\_reports/2021-Healthcare-Data-Risk-Report.pdf](https://info.varonis.com/hubfs/Files/docs/research_reports/2021-Healthcare-Data-Risk-Report.pdf)

<sup>12</sup> [https://info.varonis.com/hubfs/Files/docs/research\\_reports/2021-Healthcare-Data-Risk-Report.pdf](https://info.varonis.com/hubfs/Files/docs/research_reports/2021-Healthcare-Data-Risk-Report.pdf)