

Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare™

TLP:WHITE

Alert Id: 78f8309f

2023-06-08 15:09:20

This week, *Hacking Healthcare™* begins with a look at concerns over China's use of exit bans. We examine what they are, how they are being used by the Chinese government, and some considerations Health-ISAC members may wish to think about. Next, we take a look at an upcoming law in the U.S. state of Florida that is set to prohibit the offshoring of some healthcare data.

Welcome back to *Hacking Healthcare™*.

China and Exit Bans

While Hacking Healthcare focuses on the intersection of cybersecurity, healthcare, and global policy, sometimes it's worthwhile to break that mold by highlighting places where two of the three meet (healthcare, global policy in this case). You may be aware, but if not, it's worth paying close attention to recent developments in China related to "exit bans". This issue has impacted healthcare organizations in the past and may continue to do so in the future. As such, it is important to understand the issue and its data/security component.

What Are Exit Bans?

For those who are not as familiar with the term "exit bans", they are very much what they sound like – a government simply refuses to let an individual leave the country. While some exit bans may be imposed as a penalty for specific defined actions, the more concerning trend is the rise of opaque broad laws that allow for exit bans to be used.

In practice, vague laws that cite "national security concerns" could be used to justify any number of dubious applications, such as intimidation and coercion of individuals or organizations, control of certain groups, retaliation in business dealings, as leverage in international diplomacy/negotiations, or for any number of

other political needs.^[i] Importantly, while exit bans may primarily target a country's own citizens, they are used to target foreign nationals as well.

China's Use of Exit Bans

In China, exit bans are not a new phenomenon, but the non-governmental human rights group Safeguard Defenders has noted a significant increase in their use since 2012.^[ii] This uptick has appeared to coincide with a notable increase in the number of legal mechanisms that can make use of them.^[iii] The most significant of these new legal mechanisms is a recent update to a counter-espionage law.

This update reportedly allows "exit bans to be imposed on anyone, Chinese or foreign, who is under investigation."^[iv] The U.S. Chamber of Commerce responded to the update and to recent events in China with a statement that included noting that "In the context of China's new Counter Espionage Law, which casts a wide net over the range of documents, data or materials considered relevant to national security, the additional scrutiny of firms providing essential business services dramatically increases the uncertainties and risks of doing business in the People's Republic."^[v] The lack of clarity has concerned some over what kinds of business actions could be perceived as being problematic and could result in an exit ban.^[vi]

These concerns appear warranted given a number of cases over the past few years in which foreign nationals and executives have been refused exit and, in some cases, have been detained for extended periods of time. For example, just a few months ago, news reports detailed the detention of a well-known Japanese executive of Astellas Pharma who was accused of espionage.^[vii]

According to Safeguard Defenders, exit bans are increasingly being used and increasingly for political purposes.

Action & Analysis

****Included with Health-ISAC Membership****

Impending Florida Law Will Restrict “Offshore” Healthcare Record Storage

Sticking with a theme of healthcare, data, and China, a bill in the U.S. state of Florida that targets Chinese land ownership, investment, and other foreign interests appears set to prohibit healthcare organizations from storing some electronic health records outside the United States. This is an interesting development that appears to devolve issues generally addressed at the federal level, data localization, to the state level, and it raises interesting questions around data sharing and interoperability.

The last few pages of the Florida House Bill 1355 would amend the Florida Electronic Health Records Exchange Act to ensure that:

“A health care provider that utilizes certified electronic health record technology must ensure that all patient information stored in an offsite physical or virtual environment, including through a third-party or subcontracted computing facility or an entity providing cloud computing services, is physically maintained in the continental United States or its territories or Canada.”[\[xi\]](#)

The Act clarifies that it “applies to all qualified electronic health records that are stored using any technology that can allow information to be electronically retrieved, accessed, or transmitted.”[\[xii\]](#) It is set to go into effect on July 1st.

Action & Analysis

****Included with Health-ISAC Membership****

Congress

Tuesday, June 6

No relevant hearings

Wednesday, June 7

No relevant meetings

Thursday, June 8

No relevant hearings

International Hearings/Meetings

No relevant meetings

[i] <https://safeguarddefenders.com/sites/default/files/pdf/Trapped%20-%20China%E2%80%99s%20Expanding%20>

[ii] <https://www.reuters.com/world/china/chinas-exit-bans-multiply-political-control-tightens-under-xi-2023-05-02/>

[iii] <https://www.reuters.com/world/china/chinas-exit-bans-multiply-political-control-tightens-under-xi-2023-05-02/>

[iv] <https://www.reuters.com/world/china/chinas-exit-bans-multiply-political-control-tightens-under-xi-2023-05-02/>

[v] <https://www.uschamber.com/international/u-s-chamber-statement-on-concerns-over-prc-investment-climate>

[vi] <https://www.washingtonpost.com/world/2023/05/02/china-exit-bans-foreigners-business/>

[vii] <https://www.wsj.com/articles/in-china-a-detention-and-a-new-espionage-law-have-businesses-worried-78fc88b>

[viii] <https://www.washingtonpost.com/world/2023/05/02/china-exit-bans-foreigners-business/>

[ix] <https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories/china-travel-advisory.html>

[x] <https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories/china-travel-advisory.html>

[xi] <https://flsenate.gov/Session/Bill/2023/1355/BillText/c2/PDF>

[xii] <https://flsenate.gov/Session/Bill/2023/1355/BillText/c2/PDF>

[xiii] <https://static1.squarespace.com/static/5d7692c33cccf35926f4a98b/t/6446adee7a45703303541645/16823536>

Reference(s): [safeguarddefenders](#), [Reuters](#), [state](#), [Wall Street Journal](#), [Square Space](#), [flsenate](#), [uschamber](#), [Washington Post](#)

Report Source(s): Health-ISAC

Tags: Exit Bans, Hacking Healthcare, Health Records, EHR, Florida, China

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions and/or Comments:

Please email us at contact@h-isac.org

Conferences, Webinars, and Summits:

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

Hacking Healthcare:

Written by John Banghart, who served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.

Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.