COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 21, Number 10. October 14, 2021 FBI: More Awareness, Due Diligence Needed To Fight China in New 'Space Race' for Data

By Theresa Defino

Conducting a risk analysis is a basic tenet of security compliance, with the overarching goal of understanding where protected health information (PHI) "lives" in an organization, where it moves, where it resides—and then imposing safeguards. Would China be an acceptable final resting place? And would covered entities (CEs) or business associates (BAs), with their often murky subcontractors, even know if the Chinese government was tapping into it?

This isn't as far-fetched as it may sound. Recent reporting by *Reuters* has uncovered alleged ties between what it calls a Chinese gene company and the Chinese military. "A prenatal test taken by millions of pregnant women globally was developed by Chinese gene company BGI Group in collaboration with the Chinese military and is being used by the firm to collect genetic data," *Reuters* reported in July.[1]

"What *Reuters* discovered was that, although you sign a consent form as a patient, the identified genetic data from mothers all around the world was getting sent back to Hong Kong and China," according to Edward You, a supervisory special agent in the FBI's Weapons of Mass Destruction Directorate. "And yes, they get their results back, but what it means is that as the data resides in China, the Chinese national government [has] laws in place where they can access that data, based on a determination if there's a national security need."

You, who recently completed a two-year detail as the FBI's liaison officer to HHS, made his observations during a podcast with John Riggi, senior advisor for cybersecurity and risk for the American Hospital Association (AHA).[2]

As Riggi explained at the start of the podcast, AHA has been providing resources to its members and the health care industry generally by interviewing individuals such as You to help address threats to cybersecurity and discuss "best practices to help identify and reduce the risk posed by those threats."

You "worked for six years in graduate research focusing on retrovirology and human gene therapy at the University of Southern California, Keck School of Medicine. He subsequently worked for three years at the biotechnology firm AMGEN Inc. in cancer research," according to Texas A&M University, where You is a senior fellow for the Scowcroft Institute of International Affairs at the Bush School of Government and Public Service.[3]

According to Texas A&M, You's "overall goal is to safeguard the scientific community, the life science research enterprise, and the U.S. bioeconomy."

Before beginning the discussion, Riggi asked You to define what is meant by the bioeconomy. You said this term is acknowledging "advances that we're seeing in biotech" are heavily dependent upon data.

"Data is going to become the new critical resource, or the new oil, that is really going to fuel the ability to leverage biotech," said You. He added that data, "beyond the traditional cybersecurity issue, is really going to be the focal point of priority, not only for the U.S. but for around the world."

Riggi asked You to define "the greatest threats to the bioeconomy" and where they originate.

You responded that America is at risk of biological threats, such as "dangerous bacteria, viruses and toxins." He added that the United States is the only country that has been the victim of "bioterrorism," referring to "anthrax mailings on the heels of the 9/11 attacks."

Noting the ongoing pandemic, You said that the "dangerous pathogens or emerging and re-emerging infectious disease [are] still a big threat."

But, he added compliance officials and others "really need to start thinking about what does security look like for our data. And I'm not talking about privacy. I'm not talking about ransomware."

There may not be a true appreciation "for the value of the data," You said, nor an appropriate assessment. Officials may not be "understanding the consequences of what happens when we lose that data, or it gets co-opted or accessed by others or either state or nonstate actors."

As far as the source of threats to data, it is China. You named the Chinese Communist party, saying it "has put in strategies in place to gain access to the data."

In response to *Reuters*' reports, BGI has maintained that it is operating appropriately and complying with various laws.

In a statement following the *Reuters* coverage, BGI officials said the firm "is committed to improving health outcomes worldwide. That is and always has been the company's mission. Assertions that BGI is motivated by anything other than the advancement of health outcomes are both deeply disappointing and factually incorrect. ... Wherever BGI undertakes research, the company strictly comply with local laws, guidelines, and protocols, while adhering to internationally recognized ethical standards."[4]

Bigger Fear Than Breach: Data Misuse

More common concerns remain. Referring to cyber intrusions, You said "the hacks that we've seen in health care and health insurance, the huge exfiltration of data [are] ongoing around the world."

But, said You, "here's the problem...what I classify as the covert or criminal acquisition of data. And even in those instances, I don't think we're assessing the actual threat." In You's view, "predominantly the focus has been on the loss of personal identifiable information, the possibility for identity theft or for fraud."

Yet this is short-sighted, once "you layer on the fact that data is going to fuel the future of precision health," You said, noting the quick development of COVID-19 vaccines. This demonstrates the "power" of the data, You said.

Hacking of insurance data and the "potential loss of data of individuals," including billing codes and medical information, "is really valuable data," especially when it concerns "millions of individuals," said You. The data "can be interpreted [revealing patients] their current or prior medical conditions, what treatments have been provided, what drugs have been administered, what the drug course over time may have looked like."

He called this "incredibly valuable data that, over time, will just gain more value as a more [is] aggregated, or as we develop the tools to analyze that data."

Some May be CEs, CLIA Certified

You maintained that health care entities are "giving away" the data through contracts, collaborations or partnerships.

China, You said, has "heavily invested, for example, in [the] DNA sequencing market" and has "established institutions" that are HIPAA CEs and are accredited under the Clinical Laboratory Improvement Amendments (CLIA).

Given these organizations "meet all of our existing U.S. requirements for privacy and even for clinical compliance…we may be sending specimens and our data for analysis for clinical testing, and may not be realizing the vulnerability" of the data, said You.

If data is being sent "overseas," asked You, "who is going to have access to the data and how is that data potentially going to be utilized?"

Riggi clarified that You's remarks refer to "the Chinese government, not the Chinese people [and] the many, good [Chinese-born] U.S. citizens and researchers that we have here that contribute to the advancement of medical research and science every day."

You continued that "there's a disparity here, a lack of reciprocity, in that we send our data overseas to institutions that, on paper, look like they meet all of our existing criteria."

Organizations in the United States are conducting "due diligence in assessing [whether] they are a HIPAA" CE or BA "based on the regulations," said You.

But, what they may not be assessing is "once the data goes over there, what are the regulatory and legal requirements [in China]? And so there is a lack of understanding of what the risks and the vulnerabilities are once our data leaves our shores," You said.

Share Population Data 'Cautiously'

You maintained that "China has established themselves to be able to tap into data from all around the world through…strategic partnerships for collaborations through contracts" but that firms in the United States "don't get to see any of their data."

He added that, "from a bioeconomy standpoint, that gives them a tremendous strategic advantage" in the development of "artificial intelligence, high-performance computing, machine learning, quantum computing," and then Chinese officials could "turn that loose on that data."

Officials in U.S. health care organizations, Riggi concurred, must be "really cautious on who they provide the data to [for] population health studies" and "even what may seem as fairly routine data exchanges provided to third parties for billing and coding purposes."

Data "could be used as building blocks for the development of precision medicine," said Riggi. U.S. health care organizations must perform their own reviews, even "on what you believe to be a U.S.-based third party [to] understand precisely if they are, in fact, using subcontractors for that service, which may be located in China or some other foreign nation."

If so, "data that you provided them here in the U.S. [could be] transferred to the subcontractor," Riggi said.

Riggi also asked You for his thoughts on the "strategic implications of China becoming dominant economically and scientifically in the development of precision medicine." Riggi added that "as we've seen in the pandemic, health security equals economic security, and economic security equals national security."

Fear of Supply Chain Dominance by China

Since President Biden took office, "overall Chinese investments in the U.S. has decreased, [but government officials] have absolutely concentrated more heavily in health care and pharmaceutical and biotech industry sectors. So that should be kind of a wake-up call for us," You said.

"This potentially can translate into a win-win-win for China…that if they win the bioeconomy 'space race,' they will get improved health care, better food security, [which] will translate into more employment opportunities for their own citizenry," he added.

This could make "the rest of the world…beholden to them…dependent upon a foreign supply chain for our health care needs," You said.

Riggi asked You how health care organizations can respond "to mitigate these threats, especially given there may not be viable commercial, cost-effective alternatives for the U.S." for services provided by Chinese firms.

You said the first response is to raise awareness, and "having the wherewithal to start improving your risk assessment, doing due diligence as you establish contracts—or those business partnerships and collaborations, asking about those contractors or subcontractors."

Organizations can be "doing a better job and understanding where the data might be going…to conduct a more robust risk assessment," he said.

In addition to raising awareness, You suggested "doing that gut check and looking at your business model and business operations." He added that health care organizations should know they are "not alone in this" and can contact their local FBI field office for support and expertise.

Reach Out for Help

The FBI has "coordinators to assist in cybersecurity matters and private sector coordinators to help with potential [intellectual property] theft or espionage issues as well," You said, adding the FBI also can "provide assistance with threat assessments" and officials are "there to help" in response to a criminal event. "We also have our other federal partners like the National Counterintelligence Security Center," he added. For a list of free federal resources, see companion article in this issue.[5]

"The fact is that there [is the] potential for public/private partnerships to be able to identify and mitigate the risks," said You.

He said that AHA members and others could alert the FBI to vulnerabilities and "unhealthy dependencies in our health care system" to help develop countermeasures and "inform policy."

You added that there are "policies in the works right now, both in the White House and Congress, looking at how do we better reinforce and improve the U.S.'s bioeconomy. To me, the fact that that's happening is a huge home run. So, it's raise awareness, get more eyes on the problem, establish those partnerships with the FBI and others, and get your voices heard in…helping us—even within the FBI—to understand what is happening on the ground."

Contact Riggi at jriggi@aha.org.

1 Kirsty Needham and Clare Baldwin, "Prenatal test developed with Chinese military stores gene data," *Reuters,* July 7, 2021, https://reut.rs/3uhdECJ.
2 American Hospital Association, "National Threats to the Bio-Economy with SSA Edward You," *Advancing*

Health Podcast, September 23, 2021, https://bit.ly/39IaAWP.
3 "Senior Fellows," Bush School of Government and Public Service, Texas A&M University, accessed October 11, 2021, https://bit.ly/3luZsmH.
4 BGI, "BGI Statement in Response to Reuters Report," news release, July 9, 2021, https://prn.to/3BvED0c.
5 Theresa Defino, "List of Federal Cybersecurity Resources," *Report on Patient Privacy* 21, no. 10 (October 2021).