Gittleman J, Hasty K, Schachter S & Payne D. Health Data Security in Clinical R&D: An International Security Blindspot? *Global Biosecurity, 2022; 4(1).*

RAPID REPORTS AND PERSPETIVES FROM THE FIELD

Health Data Security in Clinical R&D: An International Security Blindspot?

Janie Gittleman[1], Katherine Hasty[2], Steven Schachter[3] & Daniel Payne[1]

[1] ManTech International Corporation, United States

[2] Future Warfare, United States

[3] Harvard Medical School, United States

Keywords: Health, Data Security, Cybersecurity, Surveillance, Clinical Research and Development

The targeted theft of Pfizer/BioNTech vaccine data from the European Medicines Agency (EMA)" is the most recent wake-up call that cybersecurity, economic security, and public health are increasingly intertwined in complex ways that have pressing national security implications. In fact, Health Care IT News reported a "'global phishing campaign' against organizations responsible for the transport and sub-zero storage of the vaccine, supposedly in an attempt to gain unauthorized access to private credentials and sensitive information regarding the vaccine's distribution." (1) A critical and often overlooked target area for malicious activity is clinical R&D leading to new drugs, medical treatments, and devices. Actors in academia, government and the private sector are increasingly at risk from remote cyber intrusions and espionage through insider threats targeting intellectual property. Theft and manipulation of this health data threaten to undermine private sector investments and slow progress towards positive health outcomes. Compromised data can be leveraged to harm vulnerable populations or subvert medical responses to public health crises. The ability to hold a population's health at risk is essentially a biowarfare effect achieved through the cyber domain. It's time to think seriously about what defense in this space looks like, especially at a time when the clinical R&D landscape itself is changing rapidly with increased connectivity and automation.

Health data are vulnerable to malicious actors who seek economic advantage, strategic competitive advantage, and leverage over U.S. and global public health outcomes. American companies, labs, and agencies have already lost extensive data to actors backed by Beijing. (2) China's strategy of using stolen digital resources to advance its civilian and military capabilities (3) clearly applies to the biopharma and advanced medical products in their top-10 technologies for development under the "Made in China 2025" initiative. There is a particular urgency to this topic now, as governments around the world are investing in new avenues of clinical R&D, research support, regulatory compliance, and translational science (4) (turning observations in the lab, clinic and community into interventions that improve the health of individuals and the public).

Securing the data analysis pipeline (the people) and networks (infrastructure) of the medical and pharmaceutical sectors – across private industry, academia, and government – shares much in common with current practices in other sensitive fields. Companies, labs, and agencies need better intrusion detection, including digital twins and intrusion simulations to keep systems and human teams sharp. They need better defenses against insider threats, including better screening processes for employees, contractors, and research trialists with access to sensitive proprietary pharmaceutical R&D information. The insider threat is real: the US Department of Justice has successfully prosecuted individuals at such institutions as Harvard University (5) and Nationwide Children's Hospital's Research Institute for theft of health-related scientific research (6). Entities involved in critical research should consider a rigorous background investigation process that combines a traditional investigation and one related to mission-specific risks. This should go beyond screening principal investigators to encompass others with access to critical data, such as data analysts and lab support engaged in global collaboration at an accelerated pace. They should improve systems to spot the theft or removal of sensitive proprietary information from company networks. Organizations must better train their people, particularly academic and research institutions, whose experts work closely with outside entities and benefit from rich collaboration. Training must emphasize practical measures that individuals can take to protect themselves and their electronic devices from malicious actors during travel (at hotels, airports, restaurants, etc.) and at partner-provided facilities. Basic cyber hygiene measures have not been standardized or benchmarked as best practices across the community of interest.

The health industry also has unique requirements and challenges, all of which are in the midst of rapid

evolution. Growth in team-based translational science is bringing research scientists, systems thinkers, analytic boundary crossers, and business developers together across global communications architectures faster than ever. The increasing breadth and variety of global stakeholders and exploding dataset sizes are critical to rapid innovation but drive special security needs. Currently the health sector is highly vulnerable: ransomware attacks on hospitals and healthcare facilities have increased worldwide (7) spurring the need for enhanced prevention, detection, and mitigation measures to counter the barrage of threat actors and tactics. (8)

Data provenance must be a top priority for research institutions and industry partners. Government agencies have work to do as well. The Defense Counterintelligence and Security Agency should update controlled unclassified information (CUI) (9) standards and practices. The Cybersecurity and Infrastructure Security Agency should overhaul the public health sector of our critical infrastructure (10) planning. The USG must act on the recommendations put forward by the 2015 Bipartisan Commission on Biodefense; a 2021 study titled "Biodefense in Crisis – Immediate Action Needed to Address National Vulnerabilities" (11) found that little progress has been made in implementing the Commission's recommendations. The community of interest is fragmented because fast-tracked scientific research – developing proposals, recruiting study subjects, collecting data, developing results, and reporting – is global and often outsourced. New standards are required to create accountability and transparency without restricting innovation across this unique landscape.

Finally, security must become an integral part of conversations driving the field's development. A 2019 workshop (12) conducted by National Institutes of Health (NIH) and National Science Foundation (NSF) examined strategies to use health data and considered the future of models for delivery of drugs, devices, treatments, and health systems interventions. Forums like these must move beyond recognizing cybersecurity as a challenge and work to stimulate collaborative engagement on emerging threats, rapid impact assessment, and process improvement.

To begin, participants need to simply acknowledge that they are coming from different places in terms of their historical approach to security. Common security terminology, such as "zero trust," may be alienating or confusing to research alliances that rely on trust, collaboration, and rigorous external validation for success. Security procedures must therefore be developed through the coordinated efforts of clinical trialists, digital technologists, and security subject matter experts. Moreover, security solutions must span all involved organizations so that implementation facilitates interoperability (information sharing) across projects and programs and is not stifled by organizational silos.

We are in the infancy of responding to a crucial set of challenges driven by our fast-tracked innovation partnerships and dispersed remote workforce. A cross-organizational discussion on national security implications, ethical imperatives, and human rights considerations of securing clinical trial data across academia, government, and pharma is required for this new era of highly funded, networked clinical R&D.

References

1. Porter S. Pfizer. COVID-19 vaccine data leaked by hackers. Healthcare IT News. (14 January 2022). https://www.healthcareitnews.com/news/emea/pfizer-covid-19-vaccine-data-leaked-hackers (accessed 29 January 2022).
2. U.S. National Counterintelligence and Security Center. China's Collection of Genomic and Other Healthcare Data from America: Risks to Privacy and U.S. Economic and National Security. February 2021. https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/NCSC_China_Genomics_Fact_Sheet_2021revision20210203.pdf (accessed 24 February 2022).
3. Puglisi A. Testimony before the U.S. Senate Select Committee on Intelligence. (4 August 2021). https://www.intelligence.senate.gov/sites/default/files/documents/os-apuglisi-080421.pdf (accessed 29 January 2022).
4. U.S. Department of Health and Human Services. National Institutes of Health. National Center for Advancing of Translational Research. (20 January 2022). https://ncats.nih.gov/training-education/skills. (accessed 29 January 2022).
5. U.S. Department of Justice. Office of Public Affairs. Harvard University Professors and Two Chinese Nationals Charged in Three Separate China Related Cases. Justice News. (28 January 2020). https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related. (accessed 29 January 2022).
6. The United States Department of Justice. Office of Public Affairs. Hospital Researcher Sentenced to Prison for Conspiring to Steal Trade Secrets and sell to China. Justice News. Press Release #21-344. Researcher Sentenced to Prison for Conspiring to Steal Trade Secrets and Sell to China. Justice News. https://www.justice.gov/opa/pr/hospital-researcher-sentenced-prison-conspiring-steal-trade-secrets-and-sell-china. (20 April 2021). (accessed 29 January 2022).
7. Offner K.L. Sitnikova E., Joiner K.,MacIntyre C.R. Towards understanding cybersecurity capability in Australian healthcare organizations: a systematic review of recent

trends, threats, and mitigation. https://www.tandfonline.com/doi/full/10.1080/02684527.2020.1752459.
8. Ayala L. Cybersecurity for Hospitals and Healthcare Facilities A Guide to Detection and Prevention. A Press. 2016.
9. Defense Counterintelligence and Security Agency. Controlled Unclassified Information. DCSA Office of Communications and Congressional Affairs. https://www.dcsa.mil/mc/ctp/cui/. (accessed 29 January 2022).
10. United States Department of Homeland Security Healthcare and Pubic Health Sector-Specific Plan. (CISA.gov). (May 2016). (accessed 29 January 2022).
11. Bipartisan Commission on Biodefense. Biodefense in Crisis: Immediate Action Required to Address National Vulnerabilities. (March 2021). https://biodefensecommission.org/. (accessed 29 January 2022).
12. Inan O.T., Tenaerts P., Prindville S.A., Reyonolds H.R., Dizon D.S., Cooper-Arnold K., Turrakhia M., Pletcher M.J.,Preston K.L, Krumholtz H.M., Martin B.M., Mandl B.M., Klasnja P.,Spring B., Iturraga E., Campo R., Desvigne-Nickens P., Rosenberg Y., Steinhubl R.,and Califf R.M. Digitizing Clinical Trials. Nature Publishing Group. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7395804/. (accessed 29 January 2022).

How to cite this article: Gittleman J, Hasty K, Schachter S & Payne D. Health Data Security in Clinical R&D: An International Security Blindspot? *Global Biosecurity, 2022; 4(1).*

Published: March 2022