

# UNIVERSITY OF HAWAI‘I SYSTEM REPORT



REPORT TO THE 2026 LEGISLATURE

Report on Data Exposure at the  
University of Hawai'i – Cancer Center

HRS 487N-4

December 2025

**Subject: Report to the Legislature on Data Exposure at the University of Hawai'i – Cancer Center**

Discovery of Data Exposure: December 2025  
Location of the Data Exposure: University of Hawai'i – Cancer Center – Research Operations  
Nature of the Exposure: Ransomware attack on Certain IT Systems

**Incident Description:**

On or about August 31, 2025, University of Hawai'i ("UH") identified a cybersecurity incident isolated to specific servers that support the research operations at the Cancer Center. There has been no impact on clinical operations or patient care at the Cancer Center. The affected data was contained in research files and was not part of the medical records for patients treated at or in conjunction with the Cancer Center.

UH promptly disconnected affected systems and took steps to terminate the unauthorized access and mitigate risk to data. Experts were immediately engaged to investigate and determine the nature and scope of the incident.

During the course of the investigation, it was determined that an unauthorized third party had access to and the opportunity to exfiltrate a subset of research files on the servers supporting the research operations at the Cancer Center. Due to the extensiveness of the encryption by the threat actors, it took some time for UH to restore the affected systems and be in a position to assess the impact to data. Once the affected systems became accessible, UH promptly began identifying potentially impacted files to conduct an e-discovery review.

While the investigation was underway, UH made the difficult decision to engage with the threat actors in order to protect the individuals whose sensitive information may have been compromised. Keeping external stakeholders informed UH worked with an external team of cybersecurity experts to obtain a decryption tool and to secure destruction of the information the threat actors illegally obtained.

Initially, the review identified a majority of the files related to a specific cancer study and largely contained only research data with no Personal Information about the research subjects. UH engaged a third party vendor to conduct a formal electronic review of the affected files. As the third-party review got underway, UH confirmed the existence of a set of files dating back to the 1990s containing Social Security numbers for study participants. These Social Security numbers were used in the 1990s to identify research participants before UH began using a different convention for identifying research subjects.

After making this discovery, UH started the process of submitting this notice in accordance with §487N-4 of the Hawai'i Revised Statutes. UH is currently working to compile the names and mailing addresses for potentially-affected individuals. The notice to affected individuals will include an offer of credit monitoring and identity theft protection services where applicable. UH is also simultaneously continuing an electronic review of the remaining files for any

additional sensitive information. UH will supplement this report and provide a sample notice once it has confirmed the number of individuals to be notified.

UH has taken the following steps to remediate the event and further bolster the security of the affected systems:

- Installed endpoint protection software with 24/7 monitoring.
- Retained third party experts to contain and remediate the event.
- Created replacement accounts for any compromised user accounts.
- Reset passwords.
- Rebuilt compromised systems to ensure that all malware has been eliminated and created new accounts/passwords to ensure that attackers no longer have access.
- Replaced existing firewall and rebuilt network utilizing new firewall that includes additional security controls.
- Conducted a third-party assessment to validate the security controls of the entire Cancer Center.