INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:37 UTC

University of Hawaii Cancer Center Ransomware Attack Exposes 1.2 Million Records

DATA BREACH | HIGH | CVSS 8.1

SCC Item ID	SCC-DBR-2026-0061
Type	Data Breach
Severity	HIGH
CVSS Base Score	8.1
Affected Products	University of Hawaii Cancer Center, internal IT systems and research data repositories
Published	2026-03-05
Discovery Source	Serper

Executive Summary

The University of Hawaii Cancer Center disclosed a ransomware attack that exposed personal and health-related information for approximately 1.2 million individuals connected to cancer research programs. Compromised data includes names, Social Security numbers, dates of birth, contact details, and research health data, creating significant regulatory exposure under HIPAA and state breach notification laws. Organizations in healthcare research should treat this as a pattern indicator: ransomware groups are actively targeting academic medical institutions where research data repositories combine high sensitivity with historically weaker security controls.

Technical Analysis

The incident follows a multi-stage ransomware intrusion pattern mapped to five MITRE ATT&CK techniques: T1566 (Phishing, likely initial access vector), T1078 (Valid Accounts, enabling persistence and lateral movement), T1071 (Application Layer Protocol, C2 communications), T1041 (Exfiltration Over C2 Channel, pre-encryption data theft), and T1486 (Data Encrypted for Impact, ransomware payload deployment). CWE-693 (Protection Mechanism Failure) applies broadly, indicating defensive controls failed to interrupt the kill chain at multiple stages. No specific CVE has been publicly attributed. No patch is applicable, this is an operational security failure, not a software vulnerability exploit. Threat actor identity has not been confirmed as of available reporting. The breach affected internal IT systems and research data repositories, suggesting the ransomware reached beyond clinical or administrative networks into research infrastructure. No public IOCs have been released by the organization or law enforcement.

Action Checklist

1. Step 1, Immediate: Audit privileged and service account usage across research data systems and repositories; reset and rotate credentials immediately for any accounts with access to sensitive research or PII datastores.
2. Step 2, Detection: Review email gateway logs and endpoint telemetry for phishing delivery indicators (T1566); search SIEM for anomalous authentication events using valid accounts outside business hours or from unusual source IPs (T1078).
3. Step 3, Assessment: Inventory all systems holding research data, PII, or PHI; confirm network segmentation between research infrastructure and clinical or administrative environments; identify any repositories with broad internal access.
4. Step 4, Communication: If your organization holds similar research data populations, brief legal and compliance on HIPAA breach notification obligations and applicable state notification timelines; notify institutional leadership of exposure pattern relevance.
5. Step 5, Long-term: Conduct a tabletop exercise simulating ransomware lateral movement from an initial phishing compromise into research data stores; review and enforce least-privilege access controls on research repositories; validate backup integrity and test restoration procedures for research data environments.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to external IR firm immediately if initial containment reveals evidence of persistent backdoors, multi-stage payload deployment, or data exfiltration to attacker-controlled infrastructure; escalate to legal within 24 hours if organization discovers it holds similar healthcare research data populations, as HIPAA notification obligations begin from discovery date.
Recovery Notes	After threat eradication, conduct a full restore of research data from verified clean backups to a segmented, air-gapped environment; validate data integrity (row counts, checksums, database consistency checks) before reconnecting to production networks. Implement network micro-segmentation isolating research repositories behind a firewall rule set permitting only documented research workflows; require all research data access to be authenticated via domain accounts with audit logging to Sysmon/auditd. Maintain an incident log documenting all systems affected, remediation completion dates, and re-baseline dates for 12 months post-incident to detect re-compromise or data staging.

Forensic Artifacts	Windows Event Log Security (Event ID 4688 — Process Creation, Event ID 4624 — Successful Logon, Event ID 4625 — Failed Logon) spanning minimum 60 days pre-incident discovery | Windows Event Log System (Event ID 7045 — Service Installation, Event ID 1102 — Audit Log Cleared) and Sysmon operational log (Event ID 1 — Process Creation, Event ID 3 — Network Connection, Event ID 11 — File Created/Modified) for evidence of malware execution and lateral movement | Master File Table (MFT) entries and NTFS change journal ($LogFile, $UsnJrnl:$J) from affected file servers showing file encryption timestamps and creator account identifiers | Email gateway quarantine logs, message tracking logs, SMTP server logs, and email headers for phishing delivery evidence; browser download/cache history on researcher endpoints showing malware payload origins | Network-based evidence: DNS query logs showing suspicious domain resolution patterns, NetFlow/sFlow records documenting unusual outbound connections during attack window, and packet captures of lateral movement traffic (SMB, RDP, WinRM sessions) | /var/log/auth.log and /var/log/audit/ (Linux) for SSH/sudo abuse; database audit logs from affected repositories (SQL Server error log, MySQL general query log if available, PostgreSQL pg_log); backup metadata and integrity logs proving backup systems were not compromised

Per-Action IR Details

Step 1 — Immediate: Audit privileged and service account usage across research data systems and repositories; rotate credentials for any accounts with access to sensitive research or PII datastores.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.2.3 (Containment Phase) — credential compromise is a containment priority; service account abuse is common in research environment lateral movement.

Controls: NIST 800-53 AC-2(1) Account Management — Privileged Access, NIST 800-53 IA-4(e) Identifier Management, CIS Control 5.3 — Account Monitoring and Controlling

Compensating: Use native OS tools: `Get-LocalUser | Where-Object {$_.Enabled -eq $true}` (Windows); `getent passwd | awk -F: '$3 >= 1000 {print $1}'` (Linux). Export account metadata to CSV; cross-reference against HR/research systems list to identify service accounts with no owner. For credential rotation without central vault: generate new passwords using `openssl rand -base64 32`, document in encrypted, air-gapped spreadsheet, execute password changes in a defined maintenance window with before/after logging.

Evidence: Capture BEFORE credential rotation: Windows Event Log 4688 (Process Creation) filtered for privileged account usage in past 30 days; `lastlog -t 30` output (Linux); SIEM login/authentication records (if available) for all privileged accounts; any available endpoint process logs showing service account execution context (e.g., Sysmon Event 1 or /var/log/audit/ on Linux). Document baseline account list with creation date, last password change date, and authorized use case. These artifacts prove which accounts were compromised and when lateral movement occurred.

Step 2 — Detection: Review email gateway logs and endpoint telemetry for phishing delivery indicators (T1566); search SIEM for anomalous authentication events using valid accounts outside business hours or from unusual source IPs (T1078).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §2 (Preparation) and §3.1 (Detection and Analysis) — reconnaissance of initial compromise vector and account misuse patterns.

Controls: NIST 800-53 SI-4 Information System Monitoring, NIST 800-53 CA-7 Continuous Monitoring, CIS Control 8.1 — Email and Web Browser Protections

Compensating: Email: if no gateway appliance, parse mail server logs directly. Exchange: `Get-MessageTrackingLog -ResultSize unlimited -Start (Get-Date).AddDays(-30) | Where-Object {$_.EventID -eq 'FailedToDeliver'}` or check IIS logs in `%windir%\System32\LogFiles\HTTPSYS` for suspicious domains in User-Agent or Referer fields. Endpoint: examine Windows Security Event Log (Event ID 4625 for failed logins, 4624 for successes); filter for logons outside 06:00–22:00 or from non-corporate subnets using `wevtutil qe Security '/q:*[System[(EventID=4624)]] and *[EventData[Data[@Name="IpAddress"]!="10.0.0.0/8" and @Name="IpAddress"]!="172.16.0.0/12"]]' /f:text`. Linux:

`grep 'Failed password' /var/log/auth.log | awk '{print $11}' | sort | uniq -c | sort -rn` to identify brute-force source IPs.

Evidence: Capture immediately: all email gateway reject/quarantine logs for past 60 days (export as CSV/JSON); full email headers for any messages with suspicious sender domains, shortened URLs, or macro-enabled attachments; Windows Event Log 4625 (failed authentication) and 4624 (successful authentication) for past 30 days filtered by source IP outside corporate ranges; endpoint process creation logs (Sysmon Event 1) showing email client or browser execution with suspicious child processes (e.g., cmd.exe, powershell.exe); DNS query logs showing resolution of malicious domains. Preserve email artifacts in forensic-grade format (PST or EML) before deletion policies execute.

Step 3 — Assessment: Inventory all systems holding research data, PII, or PHI; confirm network segmentation between research infrastructure and clinical or administrative environments; identify any repositories with broad internal access.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Tools and Resources for Incident Handling); NIST 800-53 SC-7(a) Boundary Protection — network architecture assessment.

Controls: NIST 800-53 IA-4 Identifier Management, NIST 800-53 SC-7 Boundary Protection, NIST 800-53 SC-32 Information System Partitioning, CIS Control 1.1 — Asset Inventory and Management

Compensating: Inventory: use native directory tools (LDAP queries, `dsquery` on Windows domain, `ldapsearch` on Linux) to enumerate file shares, databases, and mounted volumes; parse export into spreadsheet with system name, IP, data classification, current owner, and access permissions. Network segmentation: perform network mapping using free tools (nmap, Wireshark, arp-scan); document subnets and routing rules; use `netstat -an | grep LISTEN` on each server to identify listening ports and compare against documented baselines. Access audit: export file share permissions using `icacls [path] /save aclfile.txt` (Windows) or `getfacl -R /path` (Linux); search for group access (research_users, domain_users, everyone) on sensitive paths. Output all findings into a single access matrix (system | data type | current access group | required access group).

Evidence: Document baseline state BEFORE any remediation: current network diagram (physical or logical topology); a complete export of all file share ACLs and NTFS permissions on systems containing research data; database user/role definitions from each research repository (SQL Server: `SELECT name, type_desc FROM sys.database_principals`; MySQL: `SELECT user, host, select_priv, insert_priv FROM mysql.user`); firewall rule exports showing allowed traffic between research, clinical, and administrative subnets; DHCP server scope listings to confirm IP address allocation and subnet assignments. These artifacts establish the compromise scope and baseline for recovery validation.

Step 4 — Communication: If your organization holds similar research data populations, brief legal and compliance on HIPAA breach notification obligations and applicable state notification timelines; notify institutional leadership of exposure pattern relevance.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.1.4 (Notification) — regulatory communication is part of incident response lifecycle; timing is material.

Controls: NIST 800-53 IR-4(1) Incident Handling — Coordination, NIST 800-53 IR-6 Incident Reporting, CIS Control 17.1 — Incident Response Program

Compensating: Create a communication timeline document listing: (a) HIPAA breach notification deadline (60 calendar days from discovery per 45 CFR §164.404); (b) state AG notification requirements (varies by state; California requires notice without unreasonable delay, others require within 30–60 days); (c) media notification trigger (in most states, if >500 individuals affected, HHS and major media must be notified simultaneously). Prepare a one-page breach summary for legal/compliance and executive stakeholders containing: affected data types, number of individuals, preliminary compromised systems, current containment status, estimated notification scope. Schedule daily incident briefings with IR, legal, compliance, and privacy officers for first 14 days post-discovery, then move to 3x weekly. Document all communications in a shared log with date, attendees, decisions, and assigned owners.

Evidence: Preserve all incident discovery documentation: initial detection alert/report with timestamp; discovery notification to IR team with chain of custody; preliminary scope assessment (affected systems, data types, record count); any correspondence with external parties (hosting providers, backup vendors, law enforcement). These

establish the incident timeline required for breach notification letters and regulatory inquiries. Create a communication registry tracking all notifications sent, recipients, method, and timestamp.

Step 5 — Long-term: Conduct a tabletop exercise simulating ransomware lateral movement from an initial phishing compromise into research data stores; review and enforce least-privilege access controls on research repositories; validate backup integrity and test restoration procedures for research data environments.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §3.4 (Post-Incident Activity) — tabletop exercises and control validation are post-incident hardening practices.

Controls: NIST 800-53 AC-2(7) Least Privilege, NIST 800-53 AC-3 Access Enforcement, NIST 800-53 CP-4 Contingency Plan Testing, NIST 800-53 IR-3 Incident Response Training, CIS Control 5.1 — Establish and Maintain Asset Accounts

Compensating: Tabletop: schedule 2-hour workshop with IT ops, security, research leadership, and legal; walk through a scenario: phishing email → compromised researcher account → lateral movement to file server → ransomware encryption. At each step, pause and ask: 'What would we detect? What would we do?' Document gaps (missing logs, unclear ownership, slow approval chain). Use MITRE ATT&CK mapping to structure the scenario (T1566 → T1078 → T1570 → T1486). Least privilege: create a 'research data access' role matrix (researcher | analyst | data admin | pi | external collaborator) and assign only necessary permissions per role (e.g., analysts can read/query but not delete; PIs can manage team access but not system backups). Enforce via file share ACL and database role assignment; require manager sign-off for any exceptions. Backup validation: weekly restore tests of a sample dataset from backups to isolated test environment; document restore time, completeness, and data integrity; maintain a log of successful restores to prove backup viability. For low-budget environments, use `rsync` with checksums (`rsync -av --checksum source/ backup/`) and periodic SHA256 verification (`find backup/ -type f -exec sha256sum {} \; > manifest.txt`).

Evidence: Post-incident: document the tabletop exercise results (attendees, scenario timeline, gaps identified, remediation actions); update IR playbooks with new detection thresholds discovered during the exercise. Archive baseline access control configurations BEFORE enforcement changes (export current ACLs, database roles, firewall rules) to establish audit trail. Capture first successful backup restoration report with timestamp, dataset size, restore duration, and integrity verification results. These artifacts prove the organization has tested and validated recovery procedures.

Detection Guidance

No confirmed, publicly disclosed IOCs are available for this incident. Detection should focus on behavioral indicators consistent with the mapped MITRE techniques. For T1566 (Phishing): query email gateway logs for messages with credential-harvesting links or macro-enabled attachments delivered to research staff. For T1078 (Valid Accounts): alert on authentication events outside normal user baselines, particularly service accounts or privileged users accessing research file shares or databases at anomalous hours. For T1071 (Application Layer Protocol C2): look for sustained beaconing patterns to external IPs over HTTP/HTTPS, especially from research workstations or servers not typically generating outbound web traffic. For T1041 (Exfiltration over C2): monitor for large outbound data transfers to non-organizational destinations, particularly from systems hosting research datasets. For T1486 (Ransomware Encryption): endpoint detection rules should flag mass file rename or extension-change events; backup systems should alert on sudden inaccessibility of previously replicated data. Healthcare and academic research environments should also confirm that HIPAA-required audit logging is active on all systems processing research PHI, as log gaps will impede any post-incident forensic review.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`No confirmed IOCs publicly available`	No threat actor has been identified and no IOCs have been released by UH Cancer Center, law enforcement, or reporting sources as of available information.	LOW

Framework Mappings

MITRE-ATTACK

- **T1041** — Exfiltration Over C2 Channel
- **T1078** — Valid Accounts
- **T1071** — Application Layer Protocol
- **T1486** — Data Encrypted for Impact
- **T1566** — Phishing

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AT-2** — Literacy Training and Awareness
- **SI-3** — Malicious Code Protection
- **SI-8** — Spam Protection
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection

NIST-CSF-2

- **RS.MI-01** — Incidents are contained

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.308(a)(6)(ii)** — Response and Reporting
- **164.312(e)(1)** — Transmission Security

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.34** — Privacy and protection of personal information
- **A.8.24** — Use of cryptography

SOC2-TSC

- **CC7.4** — Responds to identified security incidents

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1041	Exfiltration Over C2 Channel	Exfiltration
T1078	Valid Accounts	Defense-Evasion
T1071	Application Layer Protocol	Command-And-Control
T1486	Data Encrypted for Impact	Impact
T1566	Phishing	Initial-Access

Sources

Source	URL	Tier
	https://www.securityweek.com/1-2-million-affected-by-university-of-...	T3
1.2 million affected in UH Cancer Center ransomware data breach	https://www.paubox.com/blog/1.2-million-affected-in-uh-cancer-cente...	T3
Notice of UH Cancer Center cyberattack affecting personal information	https://uhcancercenter.org/about-us/newsroom/1189-notice-of-uh-canc...	T3
Data breach at University of Hawai■i Cancer Center impacts 1.2 ...	https://securityaffairs.com/188876/data-breach/data-breach-at-unive...	T3
Cancer Center Research Study Hack Affects 1.2M - GovInfoSecurity	https://www.govinfosecurity.com/cancer-center-research-study-hack-a...	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-03-29 18:37 UTC by TJS Security Command Center