INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:38 UTC

Albemarle County, VA Ransomware Attack Results in PHI and PII Data Breach

DATA BREACH | HIGH

SCC Item ID	SCC-DBR-2026-0047
Type	Data Breach
Severity	HIGH
Affected Products	Albemarle County, Virginia, county government IT systems (specific platforms not publicly disclosed)
Published	2025-12-17

Executive Summary

In June 2024, Albemarle County, Virginia suffered a ransomware attack that resulted in the confirmed exfiltration of PII and PHI belonging to county residents and individuals who had conducted business with the county. The breach was confirmed following a completed investigation, with official notifications issued to affected individuals per applicable breach notification requirements. The primary business risks are regulatory exposure under HIPAA and state privacy law, reputational damage with constituents, and potential litigation from affected individuals whose health and personal records were compromised.

Technical Analysis

The Albemarle County incident involved ransomware deployment against county government IT systems, resulting in data exfiltration prior to or concurrent with encryption. No CVE has been publicly associated with the initial access vector. Mapped CWE is CWE-693 (Protection Mechanism Failure), indicating a control gap that permitted the attack chain to complete. MITRE ATT&CK techniques identified in available disclosures: T1566 (Phishing, likely initial access vector), T1078 (Valid Accounts, possible credential abuse for lateral movement or persistence), T1041 (Exfiltration Over C2 Channel, data theft prior to encryption), and T1486 (Data Encrypted for Impact, ransomware payload execution). No ransomware family, specific threat actor group, or technical IOCs have been publicly disclosed by the county or attributed by a credible threat intelligence source. Affected systems and platforms have not been publicly named. PHI involvement triggers HIPAA Breach Notification Rule obligations; PII involvement triggers Virginia Consumer Data Protection Act (VCDPA) and applicable state breach notification statutes. Source quality is T3 (local news, county press releases, HIPAA Journal); no primary-tier threat intelligence sourcing is available.

Action Checklist

1. Step 1, Immediate: If your organization operates county-adjacent systems, shared infrastructure, or data-sharing agreements with Albemarle County, assess whether any connected systems or shared credentials could have been exposed; isolate pending review.
2. Step 2, Detection: Review endpoint and SIEM logs for TTPs aligned to T1566 (phishing delivery), T1078 (anomalous account use or credential reuse), T1041 (unusual outbound data transfers), and T1486 (volume shadow copy deletion, rapid file encryption activity); baseline deviations in these categories warrant escalation.
3. Step 3, Assessment: Inventory all systems that store or process PHI and PII; confirm encryption at rest and in transit controls are active; verify backup integrity and isolation from primary network segments.
4. Step 4, Communication: If your organization stores PHI or PII for a similar constituent base (local government, healthcare-adjacent), confirm your breach notification runbook is current and legal counsel has reviewed HIPAA and state notification timelines; do not wait for breach confirmation to verify readiness.
5. Step 5, Long-term: Conduct a tabletop exercise simulating ransomware with exfiltration against a government or regulated-data environment; review CIS Benchmark controls for email security (phishing prevention), privileged access management (T1078 mitigation), and data loss prevention; evaluate whether PHI and PII datasets are segmented and access-controlled to limit blast radius in a future incident.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to external IR firm or legal counsel immediately if any active data exfiltration is confirmed, if your organization lacks on-site IR capability, or if affected PHI/PII volume exceeds your breach notification resource capacity.
Recovery Notes	Post-containment recovery requires: (1) verified eradication of ransomware artifacts and persistence mechanisms before restoring from backups; (2) credential rotation for all accounts accessed during containment phase; (3) network segmentation validation to prevent re-compromise. Test restore on isolated network segment before production restoration. Coordinate with legal counsel on breach notification timelines (HIPAA 60-day requirement begins from discovery date, not containment date).
Forensic Artifacts	Windows Security Event Log (Event IDs 4624, 4625, 4688, 4698, 4720, 4722, 4732) | Exchange/mail server transaction logs and quarantine records (SMTP logs, IIS W3C logs for OWA/ActiveSync) | Firewall connection logs with source, destination, ports, bytes transferred (syslog format or native exports) | Volume Shadow Copy metadata and MFT (Master File Table) snapshots showing file modification timestamps and deletion patterns | PowerShell transcript logs (Event ID 4103) and command-line history (/var/log/auth.log for Linux service account activity)

Per-Action IR Details

Step 1 — Immediate: If your organization operates county-adjacent systems, shared infrastructure, or data-sharing agreements with Albemarle County, assess whether any connected systems or shared

credentials could have been exposed; isolate pending review.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (organization preparation) and §3.2.1 (detection and analysis — scope determination)

Controls: NIST 800-53 IR-4(1) — incident handling with automated tools; SI-4 — information system monitoring; AC-2(1) — account management and privileged access controls

Compensating: Document all data-sharing agreements and interconnected systems manually; query DNS logs and firewall rules for outbound connections to county IP ranges using grep and awk on syslog or firewall exports; identify service accounts and shared credential repositories (e.g., shared password files, config files with embedded credentials) using 'find' with permission audits; isolate by disabling firewall rules or physically disconnecting network segments if tools unavailable.

Evidence: Capture firewall logs (last 90 days minimum) showing all traffic to/from Albemarle County IP ranges; export DNS query logs for county domain names; collect all active network connections (netstat -an output from all servers with timestamp); preserve credential management logs or password manager audit trails if shared credentials exist; take filesystem snapshots of config files containing account credentials before any isolation action.

Step 2 — Detection: Review endpoint and SIEM logs for TTPs aligned to T1566 (phishing delivery), T1078 (anomalous account use or credential reuse), T1041 (unusual outbound data transfers), and T1486 (volume shadow copy deletion, rapid file encryption activity); baseline deviations in these categories warrant escalation.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.2 (analysis — identifying indicators); §3.2.3 (containment strategy selection based on attack vector)

Controls: NIST 800-53 SI-4(1) — system monitoring with automated tools; AU-2 — audit events; AU-6 — audit review, analysis, and reporting; NIST 800-53 AU-12(1) — audit generation for account logon events

Compensating: For T1566: Export mail server logs (Exchange, Postfix, Sendmail) and search for sender reputation blacklist hits, SPF/DKIM/DMARC failures, unusual attachment types (.exe, .scr, .ps1, .bat) using grep; cross-reference with user complaint tickets. For T1078: Query Windows Event Log 4624 (logon), 4625 (failed logon), 4688 (process creation) via 'Get-EventLog' or 'wevtutil' on endpoints; search for logons outside business hours or from anomalous IPs using scripts. For T1041: Monitor 'netstat -an' and firewall logs for large sustained data transfers to non-business IPs; use tcpdump to capture packet headers. For T1486: Search System Event Log for Event ID 7034 (service stopped), 7035 (service started); scan for deleted shadow copies using 'vssadmin list shadows' and MFT records; look for rapid file modifications using 'find' with '-mmin' filters.

Evidence: Preserve email gateway logs and headers (SMTP transaction logs, quarantine records); export full Windows Security Event Log (4624, 4625, 4688, 4698, 4720 events) from all domain-connected systems; capture firewall connection logs with source, destination, bytes transferred; collect MFT snapshots from affected volumes; preserve command history (.bash_history, PowerShell transcript logs, Event ID 4103) for all service and administrative accounts; take network packet captures (tcpdump, Wireshark) during log review window.

Step 3 — Assessment: Inventory all systems that store or process PHI and PII; confirm encryption at rest and in transit controls are active; verify backup integrity and isolation from primary network segments.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (organization preparation — tools and resources); NIST 800-53 SC-28 (protection of information at rest); SC-7 (boundary protection) and CP-9 (information system backup)

Controls: NIST 800-53 SC-28(1) — encryption of information at rest; SC-7(3) — managed interfaces; CP-9(1) — system backup with offline copies; CP-10 — information system recovery and reconstitution

Compensating: Manually audit database and file server configurations: run 'cryptsetup status' on Linux volumes, 'Get-BitLockerVolume' on Windows, and query MSSQL 'sys.dm_database_encryption_keys' for TDE status; verify in-transit encryption by inspecting application config files and SSL certificate stores using 'openssl s_client' for TLS version and cipher validation. For backups: query backup software logs (Veeam, Acronis, native tools) to confirm daily execution; test restore of a non-critical dataset to verify integrity; physically inspect offline backup media (tape, external

drives) for storage location away from production network; document backup schedule and retention in a shared runbook.

Evidence: Capture configuration exports from all database servers (MSSQL, PostgreSQL, MySQL configuration files); export filesystem encryption status (BitLocker, LUKS configuration); preserve SSL/TLS certificate inventories with expiration dates; document current backup schedule with logs from last 30 days; take snapshots of network segmentation rules (firewall rules, VLAN configs) showing backup network isolation; preserve backup media location documentation and access control logs.

Step 4 — Communication: If your organization stores PHI or PII for a similar constituent base (local government, healthcare-adjacent), confirm your breach notification runbook is current and legal counsel has reviewed HIPAA and state notification timelines; do not wait for breach confirmation to verify readiness.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.2 (mitigation strategies including communication protocols); NIST 800-53 IR-4(2) — incident handling with automated tools and IR-2 — incident response training

Controls: NIST 800-53 IR-4 — incident handling; IR-2 — incident response training; SI-4 — information system monitoring; AC-4(20) — information flow enforcement with auditing for data transmissions

Compensating: Create a manually maintained breach notification decision tree document: chart notification requirements by data type (PHI, PII, financial data) and state; reference HIPAA 45 CFR §164.400-414, state AG offices' published guidance, and FTC timeline rules (60 days for HIPAA); establish a communication template repository (email drafts, media statements, regulatory notification letters) reviewed by in-house counsel quarterly; assign notification roles to specific personnel with backup designees and contact lists (state AG, media, affected individuals database); store runbook on shared drive with version history.

Evidence: Preserve current breach notification runbook with approval signatures from legal counsel; capture screenshots of notification decision logic and timeline charts; document internal communication contact list with email/phone; preserve template library with legal review dates; keep records of any prior breach notification drills or incidents for reference.

Step 5 — Long-term: Conduct a tabletop exercise simulating ransomware with exfiltration against a government or regulated-data environment; review CIS Benchmark controls for email security (phishing prevention), privileged access management (T1078 mitigation), and data loss prevention; evaluate whether PHI and PII datasets are segmented and access-controlled to limit blast radius in a future incident.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §3.4 (post-incident activities — lessons learned); NIST 800-53 AU-4(1) — audit storage capacity and CA-7(1) — continuous monitoring

Controls: NIST 800-53 CA-8 — security and privacy assessment; IR-3 — incident response testing; AC-6(3) — least privilege with privileged access management; SC-7(8) — denied egress traffic monitoring; SI-4(5) — system monitoring with security event correlation

Compensating: Host a 2-hour tabletop exercise using free/open-source tools: simulate phishing email delivery → credential compromise → privilege escalation → data exfiltration using a documented attack narrative; assign roles (IR lead, SOC analyst, backup admin, legal/PR); manually walk through detection at each stage using your actual log sources; document where tooling gaps blocked detection and design manual compensating controls (e.g., manual log review schedules, email approval workflows). For CIS hardening: download CIS Benchmarks (free tier available at cisecurity.org); audit your current configuration state against controls 6.1 (phishing filters), 5.4 (privileged access removal), 13.3 (data loss prevention on network traffic); prioritize gaps by cost-benefit and document 90-day remediation plan.

Evidence: Preserve tabletop exercise scenario document, attendance log, and role assignments; record or transcribe detection timeline gaps identified during exercise; capture current state audit findings against CIS controls (spreadsheet or report format); document remediation recommendations with business case justification; preserve meeting notes and action item tracking.

Detection Guidance

No public IOCs (IPs, domains, hashes, or file indicators) have been released by Albemarle County or attributed by a credible threat intelligence source. Detection should focus on behavioral indicators aligned to the confirmed MITRE techniques. For T1566: review email gateway logs for high-volume attachment or link delivery, particularly targeting government or HR roles. For T1078: alert on logins from new geographies, off-hours access to sensitive systems, or service accounts authenticating interactively. For T1041: monitor for sustained outbound transfers to unknown external destinations, particularly over encrypted channels or non-standard ports, during off-hours. For T1486: watch for Volume Shadow Copy deletion (vssadmin delete shadows), rapid sequential file rename or extension changes, and sudden spikes in disk write activity, all strong ransomware pre-detonation or detonation signals. Organizations using a SIEM should confirm detection rules for these techniques are active and tuned. CISA provides ransomware detection guidance in advisory AA23-061A and related threat alerts, with detection rule templates applicable to this TTP profile; see https://www.cisa.gov/resources for current advisories.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`none-publicly-disclosed`	No IOCs have been released by Albemarle County or attributed by a credible public threat intelligence source as of available reporting. Do not fabricate or assume indicators.	LOW

Framework Mappings

MITRE-ATTACK

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

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-2** — Account Management

- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **IR-4** — Incident Handling

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **RS.CO-03** — Recovery activities and progress communicated

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

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

SOC2-TSC

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1566	Phishing	Initial-Access
T1041	Exfiltration Over C2 Channel	Exfiltration
T1486	Data Encrypted for Impact	Impact
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
	https://cvillerightnow.com/news/208802-albemarle-county-has-release...	T3
Albemarle County Cybersecurity Incident Update | County News	https://www.albemarle.org/Home/Components/News/News/1327/1681	T3
Albemarle County, VA, Confirms PHI Stolen in June Ransomware ...	https://www.hipaajournal.com/albemarle-county-va-ransomware-data-br...	T3

Source	URL	Tier
Albemarle County concludes investigation into June ransomware ...	https://www.cbs19news.com/news/albemarle-county-concludes-investiga...	T3
UPDATE: Cybersecurity Incident | County News	https://www.albemarle.org/Home/Components/News/News/1135/1681	T3

Generated 2026-03-29 18:38 UTC by TJS Security Command Center