ACCESS
Community Health & Research Center

Policy Name: Policy Section/ Number:	Created By:	Initial Date:	Current Date:	Pages:
Data Breach Policy Section __/# ____	Ana Dutcher Quality Assurance Manager	11/23/2020	4/4/2022	Page **1** of **4**

Approved By: Mohamad Khraizat	Title: Health Operations Manager
Signature: Mohamad Khraizat	Date: 4-4-22

I. POLICY

This policy aims to help ACCESS Community Health and Research Center (CHRC) manage data breaches effectively. ACCESS CHRC holds data about our clients, survivors of domestic and sexual violence, legal clients, employees, and other individuals for a variety of programmatic and logistical purposes. ACCESS CHRC is committed not only to the letter of the law but also to the spirit of the law and places a high premium on the correct, lawful and fair handling of all personal data with utmost respect for the privacy and trust of all individuals with whom it deals.

II. PURPOSE

The purpose of this policy is to document the organization's response to breaches involving electronically stored information.

III. APPLICATION

This policy applies to all ACCESS employees, interns and volunteers who that have access to client data. The data covered by this policy pertains to personally identifiable information (PII) and protected health information (PHI). Parties with access to this data can include ACCESS staff as well as vendors responsible for maintaining data in cloud-hosted applications.

IV. DEFINITIONS

1. PHI: Any information pertaining to health status, heath care, or payment for health care that can be linked to an individual.
2. PII: Any information that can be linked to and identify a specific individual.
3. Breach: Any incident of unauthorized access to data containing PII or PHI.

V. PROCEDURES

A. Action Plan:

In the event of a suspected breach, the following protocol is adhered to:

1. Notification:

   ACCESS IT must be notified as soon as a breach is suspected. ACCESS actively utilizes monitoring solutions to proactively identify accounts engaging in unusual activity and deactivates accounts as necessary to allow for an investigation to confirm if a breach has taken place. ACCESS staff must

alert IT in the event a breach is suspected as a result of any situation where proactive monitoring tools have no visibility (e.g. misplaced removable storage, exposure of PII/PHI as a result of mishandling of data, stolen hardware, etc.).

2. Identification:

   Upon notification (either by staff or through monitoring), ACCESS IT identifies the credentials utilized to exfiltrate data and blocks access. Once access is eliminated, audit logs are examined to identify what was accessed and how. In the event the unauthorized access was the result of leaked credentials, the account is disabled. In the event the unauthorized access was a result of an environmental security issue, the infrastructure is taken offline while the security issue is addressed. External resources including, but not limited to, IT security vendors, cybersecurity insurance vendor, and law enforcement may be brought in if warranted for additional forensic analysis.

3. Classification:

   As part of the identification process, ACCESS IT (and if necessary, 3rd party vendors), identify all information accessed during the breach to determine if client PII or PHI has been exposed. In the event PII or PHI was assessed as part of the breach, the incident is classified as a breach and the client notification process begins. If PII/PHI was not accessed (e.g. user credentials were phished and the account was used for malicious purposes outside of the context of data exfiltration, and the account in question did not have access to PII/PHI, the incident is not classified as a breach). If determined to be a breach, DVS will be notified within 24 hours of the incident.

4. Client Notification:

   Once an incident is classified as a breach, ACCESS IT will provide the Director of Human Resources information pertaining to the clients and staff affected, and the nature of the data that was exfiltrated. Human Resources will direct departmental stakeholders to notify affected individuals in accordance with any applicable state and federal laws, and in a timely manner.

5. Per Office of Justice Programs ACCESS CHRC Programs who receive VOCA or VAWA funds (VOCA, STOP-L, STOP-V, STOP-C, CSU, SASP, DV COMP, SA COMP, SH/JFF, ICJR) and who create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information must have written policies and procedures in place to:

   a. Respond in the event of actual or imminent breach of personally identifiable information,
   b. Report the actual or imminent breach of PII to the grantee's Division of Victim Services contract analyst(s) within 24 hours after the occurrence of an actual breach, or detection of an imminent breach.

B. Involved Staff:

1. Information Technology Director and Information Technology Team:

   The Information Technology Director is responsible for managing and maintaining the security of all data collected within the organization. The Information Technology team proactively utilizes technologies to prevent breaches, but in the event a breach occurs, initial analysis is conducted by the team internally to determine how the exfiltration occurred, which data and clients/staff were affected, and if warranted, IT is tasked with engaging 3rd party vendors.

2. Departmental Stakeholders:

   ACCESS is a multifaceted organization with differing levels of access and compliance requirements. In the event of a breach, the stakeholders in any affected department(s) will be notified and included as part of the response.

3. Human Resources Director and Human Resources Team:

   The Human Resources Director will be responsible for managing the breach response regarding client and staff notification. Additionally, the Human Resources Director will be responsible for ensuring the organization adheres to all legal requirements.

4. Directly Responsible Staff:

   In the event a staff member is responsible for the breach due to the non-malicious mishandling of information or Information Technology assets, they will be included for remediation and training purposes.

C. Enforcement:

1. ACCESS staff members found in violation of this policy may be subject to disciplinary action.

D. Existing Proactive Threat Mitigations:

1. Encryption:

   All storage on ACCESS laptops is encrypted to mitigate data exfiltration as the result of theft. The encryption keys are stored on a TPM (Trusted Platform Module), and in the event unauthorized tampering of the system, the TPMs are configured to delete the encryption keys to ensure all data on the endpoint is unusable. Communication with all applications that store/access sensitive is encrypted in transit. Data is not stored directly on ACCESS desktops and all data is inaccessible upon disconnection from the local network.

2. Conditional Access:

   ACCESS utilizes conditional access to preemptively block remote logins based on multiple criteria, including but not limited to geolocation, unusual and/or impossible login activity (e.g. login from multiple physical locations in a short period of time), etc.

3. Intrusion Prevention Signature:

   ACCESS utilizes IPS packet inspection on all traffic entering and exiting the network. This is helpful to preemptively and automatically block traffic participating in an attack or data exfiltration activities.

4. Geolocation Blocking:

   ACCESS utilizes geolocation blocking to block traffic to and from all countries we don't actively need to communicate with.

5. Log Servers:

   ACCESS actively utilizes log servers to retain logs pertaining to network access to ensure a thorough and complete investigation can be conducted in the event of a breach.

VI. QUALITY ASSURANCE/IMPROVEMENT

ACCESS Quality Assurance Manager shall review and monitor adherence to this policy.

VII. COMPLIANCE WITH ALL APPLICABLE LAWS

ACCESS Employees, interns and volunteers are bound by all applicable local, state, and federal laws, rules, regulations, and policies, all federal waiver requirements, state, and county contractual requirements, policies, and administrative directives in effect and as amended.

I. LEGAL AUTHORITY AND REFERENCES

1. HITECH Act Enforcement Interim Final Rule Section 13410(d) of the HITECH Act, which became effective on February 18, 2009, revised section 1176(a) of the Social Security Act (the Act)

2. Omnibus HiTECH Compliance with Electronic Health Information enacted as part of the American Recovery and Reinvestment Act of 2009, to strengthen the privacy and security protections for health information established under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).