DEFINITIVE HEALTHCARE
Discover opportunity

Information Security Program Overview

Introduction

Definitive Healthcare (DH) provides a SaaS platform that transforms data, analytics and expertise into intelligence that helps our customers achieve commercial success in the healthcare industry. The company was founded in 2011 and headquartered in Massachusetts with offices in North America, Europe and Asia. The security of data associated with our customers, employees, vendors and partners are all paramount. This document outlines how DH provides stewardships over this data.

Security Program Overview

Definitive Healthcare's Information Security Program includes effective administrative, technical and physical safeguards for the protection of confidential information maintained by Definitive Healthcare, including sensitive personal information pertaining to the employees and customers of Definitive Healthcare, as well as other confidential and sensitive institutional and third-party information.

Effective Security requires the participation of all employees within the Definitive Healthcare organization, including dedicated individuals who focus on developing security guidelines and executing best practices. In addition to internal expertise, DH partners with leading 3rd party vendors to provide guidance on policy creation, control auditing/validation and response/remediation.

The following categories provide a framework for the security program at DH. The DH framework is based upon ZeroTrust and SOC2, and is confirmed by internal testing.

- Risk and Compliance
- Data Protection and Management
- Identity and Access Management
- Privileged Access Management
- Infrastructure Security
- Crisis Management
- Resilience and Recovery
- Application Security
- Cyber Simulations
- Cyber Operations
- Asset Management
- Device Security and Health
- Incident Response and Forensics
- Security and Threat Modeling

492 Old Connecticut Path, Suite 401
Framingham, MA 01701

Security Framework

Risk and Compliance

DH has partnered with a leading 3rd party consulting firm to develop policies and standards to address the information security initiatives within the organization. The policies associated with these categories are reviewed on an ongoing basis with members of the Security and IT teams to ensure they continue to address the threat landscape.

All security risks within the organization are reviewed and either mitigated or accepted by the Security Services Team and VP of IT when necessary.

Compliance is achieved using various methods including reporting and internal/external auditing.

DH provides updates to the Audit Committee of the Board of Directors on a quarterly basis, highlighting the status of the Infosec Program and noting any issues or concerns which should be brought to the attention of the Board.

DH can report that there have been no breaches, and no expenses incurred as the result of a breach, over the previous three years.

Data Protection Management

Data Owners classify their data appropriately based on the contents. Any data classified as Confidential is to be encrypted in transit using industry standard algorithms and ciphers. This includes but is not limited to file transfers, e-mail, interactive sessions, and web-based applications.

Any data classified as Confidential is to be encrypted at rest using industry standard algorithms and ciphers. The encryption technique includes but is not limited to whole disk encryption, file encryption and backup data.

Identify and Access Management

DH operates under the principle of least privilege. Users are assigned permissions based on their job function and are not delegated permissions outside of their role to ensure segregation of duties. Stringent policies for onboarding and offboarding are in place along with auditing and oversight to ensure automation and processes are functioning as needed.

All applications used by DH employees that are capable of access via SSO are configured as such. Services not capable of using SSO use credentials stored in a password vault with role-based access control. All SSO configurations require MFA with authenticator app and logs are monitored for anomalous activity. Phone and email secondary forms of authentication are not considered secure and are not in use. Additionally, geographic restrictions are in place to aid credential theft prevention.

Privileged Access Management

Privileged accounts are those with access or abilities greater than that of a standard user. All accounts that are privileged are subject to higher standards of password policies. They are reviewed on a semi-annual basis and in the event any security event, employee termination or anomalous activity is observed. Service accounts are developed for a single purpose to conduct a specific action, task or process.

Privileged accounts are stored in a PAM solution with tight restrictions on accessibility. Passwords, configuration files, certificates, credentials and sensitive information is stored within the PAM system. PAM activity is logged locally and forwarded to a SIEM for long term retention and analysis.

Infrastructure Security

Multiple layers comprise the infrastructure security program including but not limited to, endpoint protection, layer 7 firewall inspections, e-mail security, secure remote access, physical security, secure file transfer, storage and patch management.

- DH leverages an enterprise leading EDR solution with vendor oversight which provides additional scrutiny to log data that fall outside of standard alerts. RMM and MDM provide additional control and visibility of assets to control software installation, reporting, device control, etc.
- Layer 7 firewalls provide SSL inspection, Intrusion Protection Services, network based anti-malware, sandboxing, file blocking and data filtering amongst other prevention and visibility functions.
- Our e-mail gateways provide SPAM, Malware and ATP scanning for all inbound and outbound email. Impersonation, account takeover protection and spear phishing protection is enabled for all users. In addition, DKIM DMARC and SPF records all help to secure the integrity of our email.
- All remote access connectivity to the DH network requires MFA and uses industry standard encryption for transport.
- Access control systems, alarm systems, video surveillance and environment monitoring all provide physical security for DH locations.
- All file transfers use industry standard encryption for transport both inside and outside of the DH network.

Crisis Management

Incident response processes are well documented and defined and can be activated in the event of a security related incident. DH has partnered with 3rd party vendors to provide response assistance when necessary. In addition, DH owns Cyber Insurance that provides coverage for a variety of categories including but not limited to, breach costs, income loss, extortion, system failures, reputational damage, social engineering, public relations and regulatory items.

Resilience and Recovery

Disaster Recover plans are in place in the event of a catastrophic event. Each year, DH conducts a DR exercise to ensure the recovery operation is successful. Any modifications required are documented thoroughly and implemented to ensure a successful recovery is possible. Capacity planning is an ongoing effort with items that are capable to scale their own resources along with periodic reviews and notifications associated with resource utilization. Backups are conducted regularly according to industry standards. Non fungible offline backups are also conducted on a regular basis. These are air gapped and replicated to geographically diverse locations.

Application Security

DH maintains a full Application Security Program for its externally facing applications, based upon OWASP standards. The program consists of multiple pillars. DH performs Static Application Security Testing (SAST) as part of all build and release pipelines. Code is analyzed for any potential security issues, which are identified and addressed as part of the development process and resolved before being deployed to test environments. DH also performs Dynamic Application Security Testing (DAST) for externally facing applications. DAST runs automated scans on a weekly against the deployed web applications to check for the existence of any new and emerging threats in the security landscape.

DH utilizes an industry leading tool for Software Composition Analysis (SCA) to scan for any new vulnerabilities in Open Source and Commercial Libraries which are utilized in the applications. SCA is conducted on every software build. DH also utilizes scanning tools for Infrastructure as Code (IaC) and for Container Security to ensure these systems are tested for new and emerging threats.

Finally, DH utilizes an independent third-party agency to perform Manual Penetration Testing (MPT) on externally facing applications to test for vulnerabilities using the same techniques attackers will utilize to compromise systems. MPT is performed annually and with remediation of any critical findings occurring no more than 90 days from discovery.

Vulnerability Management

A vulnerability framework exists that leverages multiple factors to aid in assessing risk within the organization. Vulnerabilities are prioritized and addressed based on risk scores with SLAs that define the timeliness of remediation. Scanning and agent deployments are used together to provide the most comprehensive posture. Weekly and bi-weekly scanning takes place across all DH infrastructure to maintain up to date vulnerability lists and asset information.

Cybersecurity Operations

Security related logs are forwarded to a centralized SIEM for ingestion and analysis. DH has partnered with multiple leading 3rd party vendors to analyze log data and notify the organization in the event of anything suspicious 24x7x365. Threat intelligence is provided by these vendors for consumption by the security team and correlation to the logs being forwarded to the SIEM. User behavior analytics, privileged user monitoring, systems and network are all monitored.

In addition, 3rd party penetration tests are performed annually. These include internal, external, directory services assessments and manual web application testing.

Asset Management

All assets including their device profiles and software inventory are stored in centralized locations. Combined with network scanning and NAC, all endpoints are inventoried to understand their presence within the DH network. Inventories are reviewed semi-monthly to identify any unauthorized devices or software installed in the network for remediation.

Incident Response and Forensics

Response plans have been created with the assistance of leading 3rd parties to address any security related incident. DH has also partnered with these organizations to provide incident response and forensics services in the event a security incident were to occur.

DH conducts an annual Incident Response Table-Top Exercise to test Incident Response procedures against real-world scenarios. Participants from across Technology, Business Operations, and Legal/Compliance are engaged in the exercise to ensure key personnel are aware of roles and responsibilities in the event of an incident.

Security and Threat Modeling

Threat and intelligence feeds are provided to internal DH security services to keep them apprised of the ever-evolving landscape. This intelligence is also included within the logic of the security applications in use by DH. This also includes the use of honeypots to create an element of deception to assist with identification of compromise.

Security Awareness and Training

All DH employees are required to participate in annual end user security awareness training to help them understand the threat landscape. In addition, phishing simulations are conducted on an ongoing basis with remedial training available for those who are susceptible to phishing based attacks. Additional training modules are offered for those who would like to extend their learning.

Data Privacy

At Definitive Healthcare, we strongly believe in the individuals' right to privacy and control over how their personal information is used. This privacy policy (the "Privacy Policy") explains what information we collect about you, our practices for handling the same and how you can exercise your rights. DH's Privacy Policy is available on our public website.

Wire Fraud Prevention

Our wire transfer procedures have been developed to minimize the risk of fraudulent wire transfers and changes to employee and supplier payment accounts.

Supply chain (Partner and Vendor Risk)

We conduct vendor risk assessments that include evaluating the risks each vendor poses to us and based on that assessment, outlining mitigation efforts on vendors that complete the process. We re-vet our critical suppliers on an annual basis and ensure that they have cyber insurance.

Certifications and Controls

Executive leaders of DH report on the operations and procedures of the security program at DH quarterly. This is to ensure executive alignment on the policies and strategies related ot security and their impact on the business.

DH is undergoing a SOC2 type II process, targeting certification by year-end 2023.

Contact Us

If you would like any additional information regarding our security program at DH we would like to hear from you. If you are already a client, please communicate with your Account Manager and your questions will be routed internally for addressing.

Last Updated: November 21, 20221

[1] All information set forth within this overview speaks only as of such date. DH undertakes no obligation to publicly update this information, except as may be required by law.