Epividian Privacy & Security
Standards and Procedures

Epividian is committed to the securitization and protection of Personally Identifiable Information (PII) and Protected Health Information (PHI) of our customers, their patients, and their clinics. Epividian has established and maintains a rigorous security and privacy posture that adopts industry best practices to minimize our attack surface and to safeguard our customer's data. Epividian's priority is ensuring that all patient data is handled properly and conforms to the highest ethical and regulatory standards while servicing clinicians, patients, and researchers.

Program Audits

- Continuous independent advisory services from Compliance Point, a leading a privacy and security firm with expertise in HIPAA compliance regulations, HITECH, and HITRUST certification frameworks, are being used to monitor and evaluate Epividian's privacy and security program. (See engagement letter at the end of this document)
- Yearly audit of the program to determine compliance and required updates for coverage, clarity, and regulation changes, alternating between internal and external results.

Privacy Policy & Ethical Use of Data

All U.S. medical practices contributing to the OPERA database are registered users of the CHORUMS™ clinical decision support system and reporting portal. All clinical data in CHORUS is PHI and thus managed according to HIPAA, HITECH, and relevant state regulations. The CHORUS portal, as a Quality Improvement activity, is accessed securely exclusively by clinic staff to view PHI for only those patients in the care of providers at the respective practice. These healthcare operations activities are disclosed to patients in their HIPAA disclosures and agreements with providers. All practices participating in CHORUS and OPERA are responsible for obtaining proper HIPAA consent for their patients.

Business Associate Agreements are executed between Epividian and each practice, in accordance with HIPAA guidelines. The HIPAA Privacy Rule states that:

1. For PHI data lawfully collected for healthcare operations (CHORUS), additional secondary uses of a de-identified form of that data are legal. Once properly de-identified, the clinical data is no longer PHI. Per HHS, "There are no restrictions on the use or disclosure of de-identified health information."
2. The HIPAA Privacy Rule provides for a Waiver of Patient Consent provided that an IRB has reviewed and approved of the research activities.

1. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
2. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/research/index.html

Privacy Safeguards

Epividian provides additional safeguards to protect patient privacy, which include:

- **IRB Oversight**. The ongoing OPERA observational research program has received Institutional Review Board (IRB) approval from Advarra, formerly Chesapeake. (See attached letters).
- **Data Masking**. All direct patient identifiers within CHORUS clinical data are removed prior to inclusion into OPERA such that no PII is available in the OPERA database.
- **External Oversight**. Epividian maintains an independent Epidemiology & Clinical Advisory Board (ECAB) that consists of researchers, treaters, and community members. This committee provides clinical and methodological review and oversight of scientific studies as well as the appropriateness of data practices related to both CHORUS and OPERA.
- **Opt-Out**. For patients who elect not to have their de-identified health data included in OPERA, they may request to do so, and their health records are subsequently excluded from OPERA, however any data collected prior to this election will remain in data archives corresponding to each analysis.
- **OPERA Data Is Not Shared**. The OPERA database is not shared outside of Epividian work-force members. The data is treated as PHI, including all privacy and security safeguards used in the storage and handling of each clinic's CHORUS database.

Interventions

No patient interventions will be conducted in OPERA. The OPERA database and research activities are exclusively observational.

The CHORUS service provides reporting of individual patients and the patient population, consisting of data gathered *from* the practice *to* the practice. There is no medical guidance offered to clinicians inside of CHORUS. Where reports and alerts are presented, they are based upon current published treatment protocols and standards of care.

There is no mandate to use the reports or the services to participate in either CHORUS or OPERA. Practices are not paid to use either but may elect to purchase premium healthcare analytics and other data management and reporting services offered by Epividian as part of CHORUS. Clinics are not required to purchase such services to maintain a CHORUS database with Epividian as a research partner.

Security Policy Executive Summary

Workforce Security

Background Checks
All Epividian employees must submit and pass a background check prior to being granted access to PHI. If discrepancies are found, Epividian engages with legal experts to perform a threat analysis to determine if PHI access may be granted.

Least Privileged Access
Each Epividian employee is granted access to resources, data or otherwise including PHI, only relevant to their assigned tasks and only when access is approved by their direct supervisor and Epividian's Security Officer. Access to PHI may only be granted for the timeframe necessary to complete the assigned task.

Password Complexity Requirements

- Employee passwords must meet a complexity requirement with passwords consisting of:
  - A minimum of 12 characters in length
  - A combination of upper-case and lower-case characters.
  - At least one (x1) numerical value [0-9]. Multiple are encouraged.
  - At least one (x1) special character. Multiple are encouraged.
- Employees are required to change their passwords every 90 days and may not reuse a password younger than 24 months.
- Use of generic, or shared, accounts by Epividian employees is strictly prohibited.
- Access to all system resources is logged and reviewed once per quarter, however random audits are completed more frequently.
- Continuous Security & Privacy training is required by all employees.
- Epividian maintains a strict sanctions policy with consequences ranging from re-training to termination, depending on the number and severity of the violations.

Remote Access
All employees telecommute. Additionally, Epividian is 100% virtualized and hosted with an IaaS provider. Obtaining access to internal resources is contingent upon completion of Epividian's Security & Privacy Training, as well as attestation of knowledge to all HIPAA compliance regulations and governance policies as outlined by the United States Government. We enforce multi-factor authentication when accessing VPN or any Microsoft Office 365 resources, including by not limited to SharePoint, OneDrive, Exchange (Email), DevOps, etc.

Additionally, Epividian prohibits the use of unsecured public Wi-Fi access points to connect to our infrastructure via VPN, or other resources containing sensitive information. Epividian discourages the use of any unsecured network. Exceptions may be granted per the discernment of the Security Officer and the employee's director supervisor.

Endpoint Security

Patch Management
Epividian leverages RMM technologies to ensure all external assets are scanned and patched weekly. All critical patches are downloaded and installed commencing at 5pm each Friday. Any endpoint that is offline during this time, scanning and/or patching will resume as soon as the endpoint establishes a connection with our RMM service. A reboot is often required to complete the patching process and logs are maintained per HIPAA compliance regulations.

Emergency patching is conducted as necessary and as determined by the current global security climate, which includes zero-day vulnerabilities.

SASE Architecture
Cisco Umbrella is a Secure Access Service Edge technology which is designed to converge basic network functionality (DNS) with cloud-hosted security functions (content filtering). All external Epividian assets have the Cisco Umbrella agent installed. All external requests are monitored and logged enforcing categorical web browsing restrictions and data obtained by Umbrella aids in building Epividian's Indicators of Compromise, or IOC, policies.

Encryption
Epividian-managed assets have BitLocker enabled. This is enforced through Group Policy and monitored via our RMM utility. All BitLocker keys are backed up to our local Active Directory domain.

Endpoint Detection and Response (EDR)
Epividian, Inc. has implemented Carbon Black, an industry-leading, next-generation anti-virus and real-time behavioral analysis solution to all external assets. Carbon Black is a cloud-based intrinsic, endpoint protection solution designed to deny/block behavioral anomalies when they occur, further solidifying Epividian's security posture to secure and protect our client's data.

Infrastructure-as-a-Service | Cloud Hosting

As of 2019, Epividian, Inc. has partnered with Armor, Inc. as our Infrastructure-as-a-Service solutions provider. Armor is SOC2/3, HIPAA, and PCI compliant, and carries HITRUST certifications on various services offered. Additionally, Armor has developed and matured an industry-known Security Information and Event Management (SIEM) suite and a year-round staffed Security Operations Center bringing best-in-breed security monitoring and management delivering:

- Host-Based Intrusion Detection & Prevention (IDS/IPS)
  - Epividian has enabled IPS on all systems.
- Next-Gen Firewall Services
  - Epividian regulates its own firewall policies to/from each server within Armor limiting access and communication to what is only required.
- Malware Protection
  - Trend Micro Deep Security agents are installed on each server providing:
    - Next-Generation Anti-Virus and Endpoint Detection and Response (EDR).
    - File Integrity Monitoring
    - Patch, Log, and Event Management
    - Intrusion Detection & Prevention
- Vulnerability Scanning
  - Detection and alerting of unmitigated risks and obsolete infrastructure or architecture.
- Patch, Log, and Event Management
  - Epividian meets HIPAA regulations with a minimum of one year log retention.

Extraction, Transfer & Load (ETL)

All client data transferred to and hosted within Epividian's infrastructure, whether in motion or at rest, is encrypted adhering to the latest HIPAA security compliance standards or industry best practice recommendations.

- Epividian-controlled data extracts executed within a client-managed system are encrypted using AES256, prior to the transmission to Epividian, Inc.
- All files are compressed and subsequently protected with a unique encryption password prior to transmission to Epividian.
- Files are securely transmitted using FIPS 140-2 compliant, 2048-bit RSA SFTP.
- SFTP access is both IP and Geo-Location restricted.
- Files are decrypted on secured, highly restricted resources during ETL processing.
- All databases containing PHI are encrypted using SQL Server Transparent Data Encryption methods, or TDE.

Application Security – CHORUS

The following section outlines security policies that are enforced as it relates to Epividian's CHORUS application and are applied to both web (browser) and mobile [app] versions.

Authentication

Epividian has developed a propriety authentication model using JWT built on Microsoft ASP.NET Core Identity.

Accounts

All CHORUS users must have a unique account. Zero exceptions. All login attempts, successful or failed, in addition to the data access are logged and reviewed regularly.

Password Complexity

CHORUS Portal accounts are subject to the following password complexity rules:

- A minimum of 12 characters
- A combination of upper and lower-case characters (A-Z, a-z)
- A minimum of two (2) numerical values (0-9)
- A minimum of two (2) special characters
- May not reuse any passwords newer than 24 months.
- Passwords must be changed every 90 days.

Multifactor & Biometric Authentication

Epividian requires multi-factor authentication or biometric authentication once the device has been enrolled. Each CHORUS user may enroll their device once successfully authenticated to CHORUS. Multi-factor authentication uses an OTP (one-time password) algorithm delivered through an authenticator app, such as Google or Microsoft, or pushed via SMS to the user's mobile device. Multi-factor authentication is required for all password changes. Biometric authentication may be used in lieu of a User ID/Password combination, but a user will required to create a numerical PIN to supplement the biometric authentication.

Application Session Timeouts

CHORUS sessions will automatically timeout after a period of 30 minutes of inactivity. A user is provided a warning with a one-minute timer prior to the session timeout so they may extend their session. Once the session has timed out, the user must re-authenticate to obtain access to CHORUS.

NAT Tracking

Epividian logs each session's originating, NAT'd IP address. This means if a CHORUS user stays within the same network, they may authenticate with biometrics only. If the user leaves the

network, say from a hospital or clinic, and beings using cellular data, the user must authenticate fully using biometrics with a PIN. Each user is required to fully authenticate to CHORUS weekly.

Vulnerability Testing

Epividian submits to scrutinous annual security application and penetration testing, both internal and external, by an accredited independent security assessor, adhering to the Open Web Application Security Project, or OWASP, framework to identify vulnerabilities, which are then processed through our Vulnerability and Risk Management process to reduce our overall attack surface. All CHORUS releases are evaluated against OWASP's top ten most critical web application security risks.

4400 River Green Parkway
Suite 100
Duluth, GA 30096
Main: (770) 255-1100
Fax: (770) 255-1025
www.compliancepoint.com

April 26, 2023

Subject: Epividian Engagement

To whom it may concern:

Epividian has engaged CompliancePoint, Inc., a certified HITRUST CSF Assessor Firm, to perform a HITRUST CSF Validation assessment to determine the current alignment of Clinical Softworks security controls as they relate to the HITRUST CSF Validated Assessment requirements as defined in HITRUST CSF. The HITRUST CSF framework is designed to help ensure the confidentially, integrity and resilience of the 360 Health Systems applications. The framework includes verification that the organization has effective controls over data transmission and storage and includes ISO, NIST, HIPAA and other regulatory requirements.

Additionally, Epividian has engaged CompliancePoint's cybersecurity services team to provide the following vulnerability and penetration testing services:

- External Penetration Testing
- Internal Penetration Testing
- Authenticated/unauthenticated Web Application Penetration Test
- Authenticated/unauthenticated Mobile Application Penetration Test
- Bi-Annual Web Application Scans

CompliancePoint is currently working with Epividian to verify the status of their controls as compared the HITRUST CSF requirements and to provide vulnerability and penetration testing services.

Regards,

Carol Amick, CPA, CCSFP, CHQP
Director of Health Care Services
CompliancePoint, Inc.

PROTOCOL APPROVAL

DATE:	20 Dec 2017
TO:	Gregory Fusco, MD, MPH Epividian, Inc.
PROTOCOL:	Epividian, Inc., OPERA (Observational Pharmaco-Epidemiology Research & Analysis) (Pro00023648)
APPROVAL DATE:	20 Dec 2017
EXPIRATION DATE:	20 Dec 2018

IRB APPROVED DOCUMENTATION:

Protocol Version:

- Research Protocol (Not Dated)

The IRB approved the above referenced protocol and your site on 20 Dec 2017.

On 20 Dec 2017, the IRB granted a waiver of Informed Consent and a waiver of HIPAA Authorization for the above referenced protocol.

Please review the IRB Handbook located in the "Reference Materials" section of CIRBI™ (www.cirbi.net). A copy of the most recent IRB roster is also available.

Thank you for selecting Chesapeake IRB to provide oversight for your research project.

6940 Columbia Gateway Drive | Suite 110 | Columbia, MD 21046
chesapeakeirb.com | Office: 410.884.2900 | Fax: 410.884.9190

CONTINUING REVIEW APPROVAL

CR00108957

DATE:	10 Dec 2018
TO:	Gregory Fusco, MD, MPH Epividian, Inc.
PROTOCOL:	Epividian, Inc. - OPERA (Observational Pharmaco-Epidemiology Research & Analysis) (Pro00023648)
CONTINUING REVIEW APPROVAL DATE:	10 Dec 2018
EXPIRATION DATE:	10 Dec 2019

Thank you for providing the information required for Advarra IRB to conduct continuing review of the protocol and your site.

In addition to the information you provided, the IRB reviewed the current protocol referenced above, the Consent Form(s) for the study, and other supporting information.

The IRB approved continuation of the above referenced protocol. The IRB determined changes to the Consent Form(s) were not necessary.

If the study is expected to last beyond the approval period, you must request and receive re-approval prior to the expiration date noted above. A report to the Board on the status of this study is due prior to the expiration date or at the time the study closes, whichever is earlier. It is recommended that you submit status reports at least 4 weeks prior to your expiration date to avoid any additional fees or lapses in approval.

Approved investigators and sites are required to submit to Advarra for review, and await a response prior to implementing, any amendments or changes in: the protocol; advertisements or recruitment materials ("study-related materials"); investigators; or sites (primary and additional).

Approved investigators and sites are required to notify Advarra of the following reportable events, including, but not limited to: unanticipated problems involving risks to subjects or others; unanticipated adverse device effects; protocol violations that may affect the subjects' rights, safety, or well-being and/or the completeness, accuracy and reliability of the study data; subject death; suspension of enrollment; or termination of the study.

Please review the IRB Handbook located in the "Reference Materials" section of Advarra CIRBI™ Platform (www.cirbi.net). A copy of the most recent IRB roster is also available.

We look forward to continuing to work with you on this project.

> 6940 Columbia Gateway Dr., Suite 110 410-884-2900 OFFICE ADVARRA.COM
Columbia, MD 21046

ADVARRA
advancing better research

CONTINUING REVIEW APPROVAL

CR00173408

DATE:	8 Dec 2019
TO:	Gregory Fusco, MD, MPH
PROTOCOL:	Epividian, Inc. - OPERA (Observational Pharmaco-Epidemiology Research & Analysis) (Pro00023648)
CONTINUING REVIEW APPROVAL DATE:	3 Dec 2019
EXPIRATION DATE:	3 Dec 2020

Thank you for providing the information required for Advarra IRB to conduct continuing review of the protocol and your site.

In addition to the information you provided, the IRB reviewed the current protocol referenced above, the Consent Form(s) for the study, and other supporting information.

The IRB approved continuation of the above referenced protocol. The IRB determined changes to the Consent Form(s) were not necessary.

If the study is expected to last beyond the approval period, you must request and receive re-approval prior to the expiration date noted above. A report to the Board on the status of this study is due prior to the expiration date or at the time the study closes, whichever is earlier. It is recommended that you submit status reports at least 4 weeks prior to your expiration date to avoid any additional fees or lapses in approval.

Approved investigators and sites are required to submit to Advarra for review, and await a response prior to implementing, any amendments or changes in: the protocol; advertisements or recruitment materials ("study-related materials"); investigators; or sites (primary and additional).

Approved investigators and sites are required to notify Advarra of the following reportable events, including, but not limited to: unanticipated problems involving risks to subjects or others; unanticipated adverse device effects; protocol violations that may affect the subjects' rights, safety, or well-being and/or the completeness, accuracy and reliability of the study data; subject death; suspension of enrollment; or termination of the study.

Please review the IRB Handbook located in the "Reference Materials" section of Advarra CIRBI™ Platform (www.cirbi.net). A copy of the most recent IRB roster is also available.

> 6940 Columbia Gateway Dr., Suite 110 410-884-2900 OFFICE ADVARRA.COM
Columbia, MD 21046

6100 Merriweather Dr., Suite 600
Columbia, MD 21044
410-884-2900

CONTINUING REVIEW APPROVAL

CR00308961

DATE:	29 Oct 2021
TO:	Gregory Fusco, MD, MPH
PROTOCOL:	Epividian, Inc. -, OPERA (Observational Pharmaco-Epidemiology Research & Analysis) (Pro00023648)
CONTINUING REVIEW APPROVAL DATE:	28 Oct 2021
EXPIRATION DATE:	28 Oct 2022

Thank you for providing the information required for Advarra IRB to conduct continuing review of the protocol and your site.

In addition to the information you provided, the IRB reviewed the current protocol referenced above, the Consent Form(s) for the study, and other supporting information.

The IRB approved continuation of the above referenced protocol. The IRB determined there were no changes required to the current Consent Form(s).

If the study is expected to last beyond the approval period, you must request and receive re-approval prior to the expiration date noted above. A report to the Board on the status of this study is due prior to the expiration date or at the time the study closes, whichever is earlier. It is recommended that you submit status reports at least 4 weeks prior to your expiration date to avoid any additional fees or lapses in approval.

Approved investigators and sites are required to submit to Advarra for review, and await a response prior to implementing, any amendments or changes in the protocol; advertisements or recruitment materials ("study-related materials"); investigators; or sites (primary and additional).

Approved investigators and sites are required to notify Advarra of the following reportable events, including, but not limited to: unanticipated problems involving risks to subjects or others; unanticipated adverse device effects; protocol violations that may affect the subjects' rights, safety, or well-being and/or the completeness, accuracy and reliability of the study data; subject death; suspension of enrollment; or termination of the study.

Please review the IRB Handbook located in the "Reference Materials" section of the Advarra CIRBI™ Platform (www.cirbi.net). A copy of the most recent IRB roster is also available.

Thank you for continuing to use Advarra IRB to provide oversight for your research project.

6100 Merriweather Dr., Suite 600
Columbia, MD 21044
410-884-2900

CONTINUING REVIEW APPROVAL

CR00397811

DATE:	5 Oct 2022
TO:	Gregory Fusco, MD, MPH
PROTOCOL:	Epividian, Inc. - OPERA (Observational Pharmaco-Epidemiology Research & Analysis) (Pro00023648)
CONTINUING REVIEW APPROVAL DATE:	5 Oct 2022
EXPIRATION DATE:	5 Oct 2023

Thank you for providing the information required for Advarra IRB to conduct continuing review of the protocol and your site.

In addition to the information you provided, the IRB reviewed the current protocol referenced above, the Consent Form(s) for the study, and other supporting information.

The IRB approved continuation of the above referenced protocol. The IRB determined there were no changes required to the current Consent Form(s).

If the study is expected to last beyond the approval period, you must request and receive re-approval prior to the expiration date noted above. A report to the Board on the status of this study is due prior to the expiration date or at the time the study closes, whichever is earlier. It is recommended that you submit status reports at least 4 weeks prior to your expiration date to avoid any additional fees or lapses in approval.

Approved investigators and sites are required to submit to Advarra for review, and await a response prior to implementing, any amendments or changes in the protocol; advertisements or recruitment materials ("study-related materials"); investigators; or sites (primary and additional).

Approved investigators and sites are required to notify Advarra of the following reportable events, including, but not limited to: unanticipated problems involving risks to subjects or others; unanticipated adverse device effects; protocol violations that may affect the subjects' rights, safety, or well-being and/or the completeness, accuracy and reliability of the study data; subject death; suspension of enrollment; or termination of the study.

Please review the IRB Handbook located in the "Reference Materials" section of the Advarra CIRBI™ Platform (www.cirbi.net). A copy of the most recent IRB roster is also available.

Thank you for continuing to use Advarra IRB to provide oversight for your research project.