CHORDS Data Incident and Response Plan

A **data incident** is a situation in which CHORDS data are released, shared, and/or accessed in a way that is inconsistent with processes approved by COMIRB/IRB of record or executed data use agreements.

Should a data incident occur, this Response Plan will be followed along with appropriate mitigative actions to address the incident. All CHORDS data partners will be notified, within one business day, by the CHORDS board chairperson if a data incident occurs so they can follow their local sites' policies and procedures for reporting and mitigation, if required. A data incident may occur at a data partner site, data user site, CORHIO, or the University of Colorado's Anschutz Medical Campus (CU Anschutz).

Depending on the severity of the data incident (as determined by the Executive Committee in consultation with the CORHIO or CU Anschutz Privacy Officer or others as required), procedures implemented can range from communication/education in the case of a low risk incident; up to contacting CHORDS Network staff to shut down the CHORDS instance of PopMedNet™ in the case of a request that was submitted through PopMedNet™ and resulted in a very high-risk incident.

For data incidents occurring at a data partner site:
a. A DataMart Administrator is responsible for executing all CHORDS queries. Queries will be sent through PopMedNet™ (PMN). Administrators have accountability for returning the query results to the the PMN client. If a data incident occurs at a participating site, the Data Mart Administrator will follow all applicable local policies and procedures for reporting and mitigation of the data incident (i.e., notifying their institution's Privacy Officer, local IRB, and other institutional officials as appropriate). The Data Mart Administrator will also contact the CHORDS Network Administrator as soon as possible or within one business day of the incident occurring.

For data incidents occurring at a data user site:
b. After notifying their local IRB, privacy officer or others as required, the data user will, within one business day, notify the chair of the CHORDS Network Operations Work Group of the data incident issue and the Executive Committee of any mitigative actions taken at their institution including the final resolution of the data incident. The Executive Committee will be responsible for reporting the data incident with all relevant information and within one business day to data partners and COMIRB.

CHORDS also adheres to the following security guidelines of CORHIO (https://www.corhio.org/library/documents/PDF_Collateral/HIE_Privacy_and_Security_Controls.pdf) and the University of Colorado Anschutz Medical Campus (https://www.cu.edu/ois/system-wide-incident-response-procedure-data-breaches) regarding data incidents.

Security

- 9.1 Security Incidents

CHORDS will adhere to CORHIO and CU Anschutz existing policies regarding security incidents and as outlined in this Chapter.

- 9.2 Auditing

Audit Control and Review Plan:

1. Systems and applications to be logged: CHORDS activity is logged for the central portal (web application) hosted at CORHIO on a cloud-based server.
2. Information logged in each system: All data requests submitted through the CHORDS Network are fully logged.
3. Activity reports for each system: CHORDS logs are accessible to CU Anschutz' server network administrators. CHORDS staff request these logs and review them on a quarterly schedule; logs are also available upon request.
4. Procedures to review all audit logs and activity reports, including workforce member responsible for performing the audit, the frequency the audit is to be performed, and escalation procedures if suspicious activity is detected: CHORDS Network Administrators are responsible for regular audits of available logs and activity reports. These audits will be performed quarterly and following any security incidents. If suspicious activity is detected, staff members will report the activity to CHORDS Network Administrators who will report the activity to the University's OIT and adhere to University Incidence Report policies as described in this Chapter's Section 9.3.C.

Audit Trail and Audit Trail Mechanisms

1. Logs contain the information outlined in Chapter 9.2, including user login, login date/time, and activity time.

Workforce Accountability

1. Users are trained on HIPAA accountability through university mandated HIPAA training. Additionally, users agree to adhere to CHORDS and university policies when submitting user access request forms. The policies are located and/or referenced on each form and serve as documentation that staff are trained on these policies.

- 9.4 Workforce Security
  1. Access to Electronic Protected Health Information (ePHI): All individuals accessing ePHI through CHORDS will have the appropriate permission through their project to access ePHI. Each site contributing data to CHORDS must have a DUA in place (or other agreement as required by the institution); each project requesting data from CHORDS must receive IRB approval or exemption and acquire any necessary DUAs from sites (or other agreement as required by the institutions). All individuals accessing CHORDS will be confirmed by their supervisor and by CHORDS administrators as being authorized members of an approved project before being granted access.

     Individuals shall only be granted access to the minimum necessary ePHI that they require to perform their duties.

All individuals will complete a CHORDS access request form (see Appendix 3). CHORDS adheres to all University policies regarding granting, modifying, and terminating access. Supervisors of approved CHORDS projects will inform CHORDS administrators of any changes in staffing. Individuals no longer associated with an approved project will have their account disabled within one week of termination. In addition, CHORDS requires password changes on a regular basis (6 months); individuals who lose their access to their institutional email account will be unable to change their password and will therefore be locked out of their CHORDS account.

2. Workstation Use and Security
   Individuals accessing ePHI through CHORDS agree to adhere to all policies regarding workstation use and security. CHORDS requires strong passwords and unique user names. Individuals agree to ensure that their workstation settings for all computers used to access ePHI through CHORDS adhere to OIT policy (including regular security patches, standard anti-virus product use, using workstations located in areas with controlled access, etc.). Users agree to use recommended security practices where possible, including encrypting computers used to connect to CUPID; and physically securing computers by working in access-controlled or locked areas and using automatic screen-saver time outs.

- 9.5 Facility and Device Security

Data is stored in New Cloud Data Center, 160 Inverness Dr W #100, Englewood, CO 80112. Access to the office requires that a NewCloud Employee allows you entrance. Once in the office, physical access to the CORHIO Rack is through an authorized permission list controlled by CORHIO Infrastructure department. The Rack is locked and the key is controlled by NewCloud.

Information is stored on virtual servers running Windows Server 2012. Application runs on the app servers running Microsoft IIS, and the data is stored on the SQL servers running SQL Server 2012. Access is granted to the CHORDS Administrators at CORHIO and UCH

University data is stored in a SQL server and files in the file server at New Cloud Networks/CORHIO. The servers sit behind the New Cloud Firewall and a CORHIO Firewall with New Cloud and CORHIO's security protections.

Backup of the system is preformed through VEEAM Backup and data is retained for 2 weeks. In case of data loss and the need to restore data, these backups would be used to re-populate CHORDS data. CHORDS data is not used for clinical treatment and therefore loss of access to data would not pose an urgent emergency nor a threat to patient safety or wellbeing.

- 9.6 Transmission Security

1. Transmission Security: CHORDS securely transmits data from client datamarts at each data site to a central portal for access by an approved researcher. Only approved projects will receive data through CHORDS transmission. Human review takes place

at each site when each query is received and when data is ready for transmission to the researcher. An individual's access to data is limited to the approved project and the minimum necessary data for that individual's role on the project. CHORDS data is accessed via secure file transfer and remote login protocols. CHORDS data is never transmitted via fax.

2. Transmission Security Measures: All transmissions of ePHI from CHORDS to a recipient outside the CHORDS network (e.g. over the Internet) utilize an encryption mechanism. Files containing ePHI are transferred using a secure file transfer protocol. CHORDS does not send e-Mail messages containing ePHI for transmission outside the CHORDS network. See the Secure E-Mail Transmission policy.
3. Integrity Controls: CHORDS has implemented transmission security measures to ensure that ePHI is not improperly modified during transmission. EPHI integrity is sustained using approved mechanisms in transmission from data partners (checksums, hashing algorithms) and to researchers (checksums and hashing algorithms) whenever available and feasible to protect against unauthorized alteration, tampering, corruption, or falsification of the ePHI.

- 9.7 Contingency Plan
  1. Data Backup and Storage Plan: Data contained within CHORDS is not used for patient treatment and therefore immediate recovery of the data is not required in case of an emergency. SQL server data is backed up every 15 minutes. CORHIO performs a full SQL backup nightly, differential backups every hour, and log backups every 15 minutes. This allows CORHIO to restore to any point in time. Full server backups are performed nightly. CORHIO takes a copy of the VM in a consistent state and then have the ability to restore the entire VM, individual disks, or specific files as needed. Backups are performed from a snapshot of the VM while the VM is running.
  2. Disaster Recovery Plan: CHORDS information is not critical for patient treatment and loss of access for a given period of time would not hinder operations. The physical equipment hosting CHORDS is in the NewCloud Networks Office. CHORDS will adhere to the CORHIO disaster recovery plan and provide assistance for CHORDS project-specific needs in the event of an emergency.
  3. Emergency Mode Operation Plan: CHORDS does not provide critical business operations or functions and therefore this Plan is not necessary.
  4. Testing and Revision Plan: This is not a real-time system and therefore a contingency plan in case of emergency and loss of system access is not necessary. CHORDS users would be able to go several weeks without access to the system without impeding business operations.
  5. Applications and Data Criticality Plan: Does not apply, CHORDS functions as one system.
  6. Emergency Access Controls: Does not apply, CHORDS functions as one system with several administrators who can provide access in case of absence of one administrator.

- 9.8 Data Integrity

1. Integrity Controls: CHORDS uses several standard integrity controls, including:
    a. Firewalls: University data is stored in a SQL server and web application server. The servers sit within CORHIO rack behind the NewCloud and CORHIO firewall.
    b. Password protection: Strong password requirements, user authentication through access request form.
    c. Multi-Factor- Access to the server, requires MFA.
    d. Anti-virus software: All users adhere to CORHIO policies and update anti-virus software as requested.
    e. Standards for change control, testing, documentation, approval, and rollback: Software is developed on a development system. Deployment packages for versions are created and turned over to the administrators to be run on the test system. They run regression testing before deploying a new version to the production server. Extensive documentation of the software development and additional documentation of this process exists.
2. Data Authentication Controls:
    a. Database integrity: SQL server data is backed up every 15 minutes. We perform a full SQL backup nightly, differential backup every hour, and log backups every 15 minutes. This allows us to restore to any point in time. Backups are performed from a snapshot of the VM while the VM is running. This data is then stored both on local disks for fast restore as well as offsite for long-term archival and DR. No backup data, or any data for that matter, is stored in the cloud.
    b. Message integrity: CHORDS will only transmit ePHI using https connections.
    c. Procedure integrity: The CHORDS servers are stored in NewCloud Networks Datacenter. It has redundant cooling and power. The room is monitored by cameras and the door is protected by badge and key. CORHIO Racks are only accessible by authorized personnel.
3. Software Controls: SQL server meets the requirements as defined in this Chapter. CHORDS does not allow for the modification of ePHI. Further, the original ePHI remains at its proprietary source and is not accessed at all through CHORDS. No modifications are possible for the ePHI stored in the EHRs at each source institution. Therefore, no modifications can be made which would impact patient treatment or alter a patient's original record.

- 9.9 Person or Entity Authentication

CHORDS uses unique user logins and passwords (which are encrypted when stored). CHORDS users agree to adhere to all policies outlined in this Chapter. CHORDS administrators will ensure prompt deletion of terminated users as outlined in this Chapter.

- 9.10 Device and Media Controls

All ePHI stored on hardware or electronic media will be destroyed prior to the decommissioning of the hardware or media itself in accordance with the policies and methods outlined in this Chapter. Prior to device or media re-use, all ePHI stored on a device or media will be securely removed. While CHORDS does not currently use hardware or electronic media to store ePHI (as ePHI is not transmitted through our system), once these practices are initiated CHORDS will keep a written inventory of hardware and electronic media used to store ePHI as outlined in this Chapter. All research projects using CHORDS data will need to have additional IRB and DUA documentation of the project's procedures and policies around data storage.

- 9.11 Portable Media Security

All CHORDS users agree to adhere to the policies outlined in this Chapter. ePHI will only be stored on portable media devices when necessary. All devices will have security controls in place in accordance with the University's policies, and only minimum necessary data will be stored. Data will be deleted/wiped and/or the device destroyed when the ePHI storage is no longer necessary.

- 9.12 Secure E-Mail Transmission

No ePHI is currently transmitted over email in the CHORDS system. In the future CHORDS will only transmit ePHI using https connections.

- 9.13 Security of ePHI on Home Computers

Initially, CHORDS users will not be accessing ePHI in the data and reports. When ePHI becomes accessible, all CHORDS users agree to adhere to University policies regarding anti-virus software, security patches, anti-spyware software, firewalls, etc. as outlined in this Chapter when using home computers. Each research project using CHORDS will need to document their data storage policies and procedures in study-specific IRB documents and Data Use Agreements. Additionally, CHORDS recommends that access from home computers take place only using a VPN connection to the University.

Chapter 10 Report a Breach

- 10.1 HIPAA Privacy Incident Notice
    - CHORDS team members will use the appropriate forms and processes from CORHIO and CU Anschutz to notify relevant parties of potential HIPAA privacy incidents
- 10.2 Complaint Notification Form
    - CHORDS team members will use the appropriate forms and processes from CORHIO and CU Anschutz to notify relevant parties of HIPAA Complaint Notifications.