USING COMPLIANCE AUDITS TO MONITOR DATA RECIPIENT COMPLIANCE WITH CONDITIONS OF DATA RELEASE

August 2020

William Bailey, Chief Privacy Officer

Scott Curley, Manager of Privacy & Compliance

CENTER FOR HEALTH INFORMATION AND ANALYSIS

CHIA.

Why Consider a Data Recipient Audit Program?

Are the data recipients protecting CHIA Data? How would CHIA even know?

- CHIA has been releasing confidential and sensitive health data to approved data recipients for several years.
- CHIA has signed DUAs with over 100 data recipient organizations covering 300+ Data Applications, and nearly 1,000 individual data extracts.
- Historically DUAs were filed away and rarely followed up on.
- CHIA felt is was appropriate to determine how well our data recipients were doing in complying with their obligations under the CHIA DUA.

Data Use Agreement Obligations

1. **Data Privacy**
   - Confidentiality Agreements
   - Data Access Logs
2. **Permitted Use**
   - Describe purpose as identified in the approved Data Application.
   - Approved data linkages
3. **Publication**
   - Aggregation and cell suppression
   - Publication must be consistent with the CHIA-approved research purpose
4. **Data Security**
   - Data may not change physical location without prior CHIA review and approval, or be transmitted by unsecure means
5. **Data Destruction**
   - Upon completion of research use, data recipient must destroy all CHIA Data must be destroyed and then certify in writing to that destruction

Audit Design

In 2016 CHIA began to conduct audits. Audits have been in written form designed to get essential information to ensure compliance while minimizing the burdens on data recipients. Recipients use a one-page reply form in order to simplify the audit response process.

1. **Phase 1 (2016)**
   - “Check box” style survey, with no signatures required
2. **Phase 2 “Expanded Audits”(2018/2019)**
   - Supporting documentation
     - Signed confidentiality agreements
     - Corresponding data access logs
     - Citations for all publications using CHIA Data
   - Organization-wide response from multiple roles
     - Lead researcher
     - Information Security representative
     - Institutional representative

Data Audit Results

Audit Data (MM/YYYY)	Number of Audits	Formal Correction	Informal Correction	Datasets Destroyed
2016*	67	1	0	14
2018**	18	3	0	5
2019**	48	5	10	11
Total	133	9	10	30

*Phase 1 “Check Box Audit”
**Phase 2 “Expanded Audit”

Observations

Phase 1 “Check Box”

- High level of reported compliance and low level of reported non-compliance.
- Yielded destructions of data
- Late response suggests noncompliance

Phase 2 “Expanded Audit”

- Reported non-compliance rates increased when documentation was required
- Reported non-compliance rates increased when an organization-wide response was required
- Yielded destruction of data
- Late response suggests noncompliance

What were common areas of Data Recipient noncompliance?

1. **Timeliness**
   - Strong correlation between late responses and non-compliance.
   - CHIA Data not destroyed within 30 days of project completion.
2. **Data Privacy**
   - Confidentiality Agreements often not signed prior to data access or at all
   - Data Access Logs, which could alert project leaders of compliance issues, were not kept and/or updated.
3. **Permitted Use**
   - Proliferation of use into areas outside of approved project
   - Unapproved data linkage
4. **Publication**
   - Without appropriate cell suppression
   - On topics outside of the approved research purpose
5. **Data Security**
   - Disconnect between data users and data security lead to data movement and migration without prior CHIA approval, sometimes in an non-secure manner.

Repercussions for Noncompliance

1. **Connect with Office of Sponsored Programs and/or Compliance Officer**
2. **Corrective Action Plans**
3. **Suspension of Data Release**
4. **Suspension of unapproved research/projects**
5. **Withdrawal of publications**

What lessons has CHIA learned through data recipient audits?

- Data Recipient Audits are a valuable tool for assessing Data Recipient compliance
- Audits are much more robust when supporting documentation is required
- Audits are more forthcoming when signed by responsible parties
- Audits are particularly more revealing when signatures are required from institutional representatives and data custodians, not merely research staff
- Student use represents a data migration/exposure risk that mitigates in favor of limiting data release to supervising institutional faculty and not individual students
- Data recipients may assume all DUA documents are alike, and as a consequence be insensitive to agency-specific restrictions and obligations
- Data recipient refresher training may be useful to head off inadvertent noncompliance, and as a reminder of ongoing obligations under the DUA

Suggested goals for Data Recipient Audits

- Use Data Recipient Audits as an assessment tool to determine how well your agency and its data recipients are doing in protecting privacy and security interests
- Keep the audit scope and response process at a reasonable level absent evidence of significant noncompliance
- Focus on the responsibility of the organization approved to receive the data, rather than solely with the individual researcher or research teams
- Be prepared to work with institutions in order to promptly and reasonably remedy any noncompliance you may find
- Share your experiences with other APCD compliance staff!

Contact Information

For questions, please contact:

- William Bailey, Chief Privacy Officer
- William.Bailey@state.ma.us (617) 701-8134
- Scott.Curley@state.ma.us (617) 701-8255