Important Information for Non-Governmental Requests for APCD and Case Mix Data

Thank you for your interest in the Massachusetts All Payer Claims Database ("MA APCD") and Case Mix data. The Center for Health Information and Analysis ("CHIA") is implementing revised data application materials to create a more streamlined, predictable process for those seeking access to CHIA data.

Revised Application Process and Requirements

CHIA is implementing a new request process, modeled on the process used by the Centers for Medicare and Medicaid Services ("CMS") that includes three key components:

1) A Data Request
2) A Data Management Plan (for applicants seeking Level 2 data or above)
3) A Data Use Agreement

The Data Request:

The Data Request is the core of the application and includes information about your organization and your intended uses of CHIA data. CHIA will assist you in developing a request that seeks the minimum amount of data necessary to achieve your objectives and poses the least amount of risk to the privacy of individuals.

The Data Management Plan:

Non-governmental applicants will be required to submit a Data Management Plan that describes the physical, administrative and technical safeguards in place to protect any protected health information provided by CHIA. A comprehensive data management plan is critical to the approval of any non-governmental request for access to CHIA data that contains protected health information. The CHIA-approved Data Management Plan also will be used as the basis for future auditing by CHIA of data recipient's compliance with the Data Use Agreement. CHIA is adopting the process currently used by CMS to review applications for Research Identifiable Files ("RIFs"). CHIA encourages applicants to review the materials describing Data Management Plans, which is available on the ResDAC (CMS's Research Data Assistance Center) website. Information about the federal program is available at www.resdac.org/cms-data/request/research-identifiable-files.

In addition, CHIA is implementing mandatory minimum data security requirements, described below, for applicants seeking data that includes protected health information.

The Data Use Agreement:

Prior to receipt of any CHIA data, each applicant will be required to sign a Data Use Agreement that limits the applicant's use of the data to only those uses approved by CHIA. The Data Use Agreement further imposes various requirements on data recipients regarding data privacy and data security that must be met for recipients to receive or continue to hold CHIA data. The Data Use Agreement further allows CHIA to audit data recipients to confirm compliance with both the Data Use Agreement and the CHIA-approved Data Management Plan submitted by the applicant.

Minimum Security Requirements for Non-Governmental Applicants

Non-governmental applicants must meet the following minimum security requirements before receiving any CHIA data that includes protected health information (Case Mix Level 2 and above and MA APCD data):

- Encryption of any media containing CHIA data;
- Anti-virus software on any server containing CHIA data; and
- Physical access controls, e.g., confidential data must be stored behind locked doors with access to the data limited to the fewest number of people required to achieve the purpose for which such access was granted.

Or

- õ An attestation by your organization's chief legal officer, or another attorney or officer authorized to bind your organization, that your organization complies with HIPAA privacy and security requirements or, if not a HIPAA-covered entity, has privacy and security practices and policies in place such that the organization is substantially compliant with HIPAA privacy and security rules;

  or

- õ Documentation sufficient to show that your organization's information security and privacy program has been subject to an independent third-party audit in the last two years and the outside auditor determined that your organization is HIPAA-compliant.

All non-governmental applicants also must submit a Data Management Plan completed by the applicant's Chief Information Security Officer, Chief Privacy Officer, legal counsel or an officer with sufficient knowledge or experience of the organization's data privacy and security practices and authority to bind the organization.