

Connected College Health Network Data Governance Policy

This Data Governance policy was written by a subgroup of the CCHN Data Governance Committee, including Mel Fenner (University of Illinois, Urbana-Champaign), Kat Lindsey (University of Florida), Amy McLaughlin (Oregon State University), Kevin Readdean (Rensselaer Polytechnic Institute), and Data Governance Committee co-leads Brian Mistler (Humboldt State University) and Sharon McMullen (University of Notre Dame).

I. Purpose

Overview

The American College Health Association (ACHA) is committed to improving the health and well-being of college students. ACHA recognizes that the availability of information will enable the organization to achieve its goals in advocacy, education and research. College health professionals also need information to advance the health of college students at their institutions and enable policy makers and other stakeholders to make informed decisions about the health and well-being of the college student population.

Effective, efficient and strategic use of robust data for decision-making is an essential cornerstone of college health and of system improvement. Stakeholders at all levels of decision-making require timely, useful, and accurate data to most effectively support student achievement. To that end, ACHA has developed the Connected College Health Network (CCHN), a data warehouse supported by a Data Governance Committee, in order to meet the information needs of its stakeholders.

Participating institutions of higher education will submit information regarding their infrastructure for supporting

- health promoting practices,
- mental health and well-being, and
- physical health,

as well as campus characteristics, wellness programs and policies, etc. through the annual Institutional Profile Survey. Sources of data may include:

- Member institutions' electronic health record (EHR) systems
- Student demographics
- Administrative data
- Health and environmental factors
- Other relevant college health databases (e.g. such as the National College Health Assessment (NCHA)
- Integrated Postsecondary Education Data System (IPEDS)
- Other Government data sources.

Goals and Objectives

A goal of the CCHN is to provide meaningful, accurate insights that support data-driven decision-making. With data made accessible by the CCHN, stakeholders should be able to assess, monitor, and promote student health and well-being. CCHN objectives include:

- **Integrating** existing ACHA data and other data sources through the creation of a surveillance network across college campuses
- **Empowering** institutions to monitor data trends in student health & well-being
- **Providing** access to de-identified student health data to college health leaders to improve college health and well-being center quality and efficiency through enhanced benchmarking tools and the sharing of the results of data-driven interventions.
- **Enabling** data-driven decision-making by measuring health status and outcomes against academic performance and retention

CCHN considers a broad range of interests in decision-making and values community consensus. As such, a Data Governance Committee is appointed by the ACHA Board of Directors and supported by the ACHA national office staff. The Data Governance Committee is drawn from ACHA membership and is subject to ACHA bylaws and committee guidelines. CCHN leaders serve as Data Sponsors/Trustees of the Data Warehouse and the Data Governance Committee acts in an advisory capacity to CCHN leadership. Selected responsibilities of the committee include:

- Articulate the requirements for safe and effective input, access, retrieval, exchange, reporting, management and storage of data
- Inform rules to control the usage, security, quality and integrity of data during its lifecycle
- Recommend compliance with applicable laws, regulations, exchanges and standards
- Articulate responsibilities for data stewardship by defining data owners, roles, responsibilities and accountabilities
- Serve in the escalation path process (as defined below)
- Advise ACHA regarding the process by which changes to the CCHN will be made, ensuring changes are carried out in a logical manner that is mindful of potential impact on data quality
- Conduct operations with ethics, integrity, openness and transparency, supporting the shared interests of CCHN and the ACHA membership

II. **Scope**

This policy applies to all data imported into the CCHN system including the Institutional Profile Survey (IPS), Clinical Data Transfer (CDT), Cross-framework Analytic Capabilities (CAC), and other such components, and covers data in any form, including print, electronic, audio-visual, and backup and archived data, regardless of the system in which the data originated or are stored.

This policy applies to anyone approved to engage with data housed within the CCHN on behalf of ACHA.

III. Ownership

Data gathered by a member institution is owned by that institution. Upon submission to CCHN, ACHA will have a perpetual, irrevocable license to the data, including the authority to further license all data provided to institutions hereunder, and any other analyses, reports, or other intellectual property used, developed, created, or disclosed by ACHA under the Data Use and Transfer Agreement. In addition, ACHA may own the copyright in the organization, selection, and display of data within the CCHN. Further, to the extent that data users develop any rights to data through their authorized use users will assign all such rights to ACHA and agree to cooperate with ACHA in protecting and effectuating such rights. Data users shall give proper attribution to ACHA for any permissible use, dissemination, reproduction, or disclosure of the data or reports provided through CCHN.

IV. Usage

Data Privacy

Data submitted to CCHN is protected and will be released to data users only in de-identified, aggregate form, with the exception of limited data elements submitted through the IPS that are publicly available and marked as open.

ACHA members (including institutional, individual and sustaining) will have different levels of access to CCHN. Non-members will not be granted direct access to CCHN datasets or reporting tools. Access to data is permissions-based and will be requested using the Data Use Agreement (see Appendix). Data may also be accessed by Data Stewards and other employees of ACHA and its CCHN vendor whose job responsibilities require it. These data recipients are subject to the data privacy policies of their organizations. Data access security will be managed by the vendor.

Conditions under which individuals or institutions may submit data

Data may only be submitted by designated representatives of ACHA member institutions using the Data Transfer Agreement. Each institution will identify staff members who are approved to contribute data on its behalf. The name and contact information of the person making the submission is required and will not be made available to data users.

It is essential that data submitted must not be able to identify a single individual student. The primary methods used by the U.S. Department of Education for disclosure avoidance for tabular data include defining a minimum cell size. Data contributors are expected to submit data in alignment with both its institution's and CCHN's security practices around cell size. In the event that those rules are not consistent, data contributors should follow the most restrictive rule.

Data Transfer Agreement

Member institutions that contribute data to the CCHN do so with the expectation that ACHA will handle that data in accordance with all relevant, industry-standard rules and regulations. See Data Transfer Agreement in Appendix.

Protection of Data

Participant Data will be contributed from the electronic health records, billing systems, and registration systems of students treated at the Participant's student health center or counseling center without any personally identifiable information. It will be stored securely and shared only in aggregate in keeping with the Data Use Agreement. Identification of individuals is never possible. The association between information and institutions is protected consistent with CCHN security practices.

Escalation Path

Access to, or use of, the CCHN that is not contemplated by this and other relevant CCHN guidance will be managed according to the following escalation path.

1. Member institutions will take steps to resolve the issue at the local level. For example, an institution that finds it has inadvertently submitted inaccurate data should contact CCHN staff for assistance in submitting corrected data.
2. If an issue cannot be resolved by CCHN staff, or rises to a level that would benefit from input of the Data Governance Committee, such as novel or unanticipated use, either the CCHN staff or the member institution can escalate the issue to the ACHA Chief Executive Officer, who will charge Data Governance Committee leadership with forming a 3-member Investigating Committee comprised of Data Governance Committee members to evaluate the issue and provide an opinion to the CCHN Executive Committee, as follows.
 - a. Details of the issue and supporting documentation will be sent to the Investigating Committee within 10 working days of the receipt of the request. The Investigating Committee will review the information provided, and consult with whoever it deems necessary, to determine if the request is in keeping with the tenets of data governance. It will render an opinion within 30 days to the ACHA Chief Executive Officer, who will then place the issue as an agenda item on a CCHN Executive Committee meeting within the next 60 days. The CCHN Executive Committee will consider the opinion of the Investigating Committee and make a determination, which is final. The ACHA Chief Executive Officer will notify the member institution of the outcome in writing.
3. In the event of a breach of the data transfer agreement, violation of this Policy or other improper conduct, the process set forth in ACHA's [Sanctions Procedure](#) will be followed and the institution's data submission and access will be suspended until the issue is resolved.

V. Security

CCHN data is de-identified and therefore not considered personal health information, although transmission and handling of data is consistent with both HIPAA and FERPA. ACHA contracts with a Data Warehouse vendor to manage data within industry standard processes, tools, and security standards to ensure safety of data in all phases including storage, access and transmission. See details in Appendix.

VI. Quality and Integrity

Both data quality (i.e., accuracy, validity, reliability, timeliness and completeness) and data integrity (i.e., consistency over the data's life-cycle) are essential to meet the goals of CCHN. The CCHN vendor is responsible for implementing appropriate procedures consistent with industry standards to ensure data quality (e.g., data quality assurance, standardization, monitoring, etc.) and data integrity (e.g., data validation, maintenance, retention, etc.). Data shall be retained and disposed of in an appropriate manner in accordance with the vendor's policies noted in the Security section, above.

VII. Definitions

American College Health Association (ACHA): Standing at the forefront of issues that impact the health and wellness of college students, ACHA represents over 1,100 institutions of higher education, and the collective health and wellness needs of 10 million college students through advocacy, research and education. ACHA national headquarters is located at 8455 Colesville Road, Suite 740, Silver Spring, MD 20910.

ACHA-National College Health Assessment (ACHA-NCHA): a nationally recognized research survey administered to over 1.5 million college students that provides robust national information about college student health status, health risk behaviors and health attitudes

Clinical Data Transfer (CDT): the capture and transmission of de-identified clinical data, such as ICD-10 and CPT codes, by institutions' EHR vendors

Connected College Health Network (CCHN): A national college health data warehouse to advance educational achievement and health equity among students by integrating with existing ACHA systems and other data sources, enabling data-driven decision-making, providing access to de-identified student health data to college health leaders, and delivering a platform of informed healthcare for improved student health outcomes. ACHA is the coordinating center and central repository for data received by CCHN Participants.

CCHN Data Warehouse: the de-identified aggregate data repository ("CCHN Data") provided by ACHA, as the CCHN data coordinating center, to CCHN Participants for use in Projects

CCHN Participant: an organization participating in the CCHN that has signed a Multicenter Connected College Health Network Data Use Agreement

CCHN FAQ: provides answers to frequently asked questions about the Connected College Health Network

CCHN vendor: a private company contracted by ACHA to provide technical support of CCHN

Cross-framework Analytic Capabilities (CAC): a system by which institutions and organizations agree to allow ACHA to facilitate research across various data sources

Data: facts and figures submitted by an institution including, but not limited to, profile information regarding facilities and services as well as de-identified health information

Data contributors: those individuals who are approved by their member institutions to contribute data to CCHN

Data corruption: unintentional changes to data; prevented by data maintenance processes

Data Governance Committee: an advisory committee to CCHN that is comprised of ACHA members who are appointed by ACHA Board of Directors

Data integrity: the consistent accuracy, or lack of unintentional changes to or deterioration of, data over its entire life-cycle

Data quality: the state of accuracy, validity, reliability, timeliness and completeness that makes data appropriate for a specific use

Data sponsors/trustees: high-level ACHA executive leadership

Data stewards: ACHA staff or vendor responsible for daily management of data

Data Use Agreement: used with any entity (profit, nonprofit) or person that wants access to the CCHN data.

Data Transfer Agreement: used with schools that are giving data to ACHA for use in the CCHN database

Data users: those individuals who are approved by CCHN to access CCHN data

Data Admin User: can create and view reports, execute all features, and create users and assign roles and rights to users (i.e., create/read/update/delete)

Data End User: can view reports and execute certain features (i.e., read-only)

Data Power User: can create and view reports, and execute all features (i.e., create/read/update)

Data warehouse vendor: a private company contracted by ACHA to provide technical support to CCHN

De-identified records and information: shall be defined as set forth in 34 CFR §99.31(b)(1) and shall constitute education records or information from education records that may be released without the

consent required under FERPA after the removal of all personally identifiable information provided that Participant has made a reasonable determination that a student's identity is not personally identifiable, whether through single or multiple releases and taking into account other reasonably available information.

Disclosure: shall be defined as set forth in 34 CFR §99.3 and shall mean to permit access to or the release, transfer or other communication of personally identifiable information contained in education records by any means, including oral, written, or electronic means, to any party except the party identified as the party that provided or created the record.

EOM: The Family Educational Rights and Privacy Act of 1974, as amended, 20 U.S.C. 1232g and regulations promulgated thereunder, 34 CFR Part 99

Electronic Health Record (EHR): a digital version of a patient's paper chart. EHRs are real-time, patient-centered records that make information available instantly and securely to authorized users. While an EHR does contain the medical and treatment histories of patients, an EHR system is built to go beyond standard clinical data collected in a provider's office and can be inclusive of a broader view of a patient's care.

EHR vendor: a private company contracted by an institution to provide EHR services

FERPA: The Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g, affords postsecondary students the right to have access to their own education records, the right to seek to have the records amended, and the right to have some control over the disclosure of personally identifiable information from the education records.

HIPAA: The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, is intended to improve the efficiency and effectiveness of the health care system through national standards for electronic health care transactions and code sets, unique health identifiers, security and protections for individually identifiable health information.

Institutional Profile Survey (IPS): an annual survey that captures data from institutions of higher education regarding the nature of their health and wellness infrastructures and on their health promoting practices on campuses

Integrated Postsecondary Education Data System (IPEDS): a system of interrelated surveys conducted annually by the U.S. Department of Education. IPEDS gathers information from every college, university, and technical and vocational institution that participates in federal student financial aid programs.

Member institution: an educational entity such as a college or university that is an ACHA member

Outside entity: an organization not related to an ACHA member institution

Participant data: The de-identified data provided by Participant to ACHA for inclusion in the CCHN Data Warehouse. Participant Data will be obtained from the electronic health records, billing systems, and registration systems of students treated at the student health center or counseling center of Participant and shall contain no Personally Identifiable information.

Personally Identifiable Information ("PII"): as defined in 34 CFR §99.3, the term includes, but is not limited to--

- (a) The student's or other individual's name;
- (b) The name of the individual/student's parent or other family members;
- (c) The address of the individual/student or their family;
- (d) A unique identifier, such as social security number, student number, or biometric record;
- (e) Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
- (f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
- (g) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.