Data Policy

Introduction

Association of Schools and Programs of Public Health (ASPPH) Data is defined as data acquired, analyzed, and reported by ASPPH in support of its overall mission. It is an essential asset of ASPPH, and as with all assets, it is important to identify an appropriate balance between maintaining the ability of authorized individuals to access and use the asset, while minimizing the risk that is inherent by making the asset available.

ASPPH data require appropriate maintenance and protection to assure quality and integrity. It further requires management, use, dissemination, and protection in a manner consistent with laws and regulations, along with the collective desires of the membership of ASPPH (ASPPH member institutions include member schools and programs of public health accredited by or in applicant status with the Council on Education for Public Health (CEPH), members of the ASPPH Undergraduate Network, and the Global Network for Academic Public Health (GNAPH). ASPPH data is also subject to risks and threats such as accidental loss or damage, unauthorized access, malicious misuse, and inadvertent alteration or disclosure.

The ASPPH Data Policy addresses four key aspects with respect to ASPPH data:

- Ownership of data
- Accountability of individuals with access to data
- Rules for use of ASPPH data
- Responding to a data security breach

The purpose of this Policy is to address the appropriate balance between protecting ASPPH data owned by or under the custody of ASPPH from accidental and/or intentional damage, unauthorized access, unauthorized disclosure, and/or alteration while also assuring that individuals authorized to use the data have appropriate access as required for their responsibilities and duties. This Policy is not intended as a complete statement of all policies related to ASPPH data, which may include, but are not limited to, privacy policies, release statements, and data use agreements.

Data Ownership

Data aggregated by ASPPH from information submitted by individuals and member institutions, or acquired through ASPPH processes, is owned by ASPPH and is used to produce analytics, reports, and publications and to conduct research. ASPPH assumes responsibility for the quality and integrity of the data to the extent that such aggregations present a true picture of the individual information submitted by individuals and/or members. ASPPH does not assume responsibility for the accuracy of the individual

information submitted by individuals and/or members used to create aggregated data.
Individual information submitted by individuals and/or ASPPH members are owned by the individuals and/or members that submitted the information. ASPPH shall take appropriate measures to prevent the unintentional loss or destruction of information under its custody; however, ASPPH does not assume responsibility or liability for any such loss or destruction that may occur.

Accountability

ASPPH is responsible for the direct management, use, and protection of data; gathering, analyzing, and coordinating the publication of data; interpreting and complying with laws, regulations, and ASPPH policies with respect to data; and developing and implementing access, security, and disaster recovery plans. ASPPH must ensure:

- All ASPPH staff with access to data are trained in data governance, use, and protection
- Data policies are communicated to users
- Access, security, and disaster recovery plans are implemented
- Data are protected by specific and enforced security plans
- Compliance with laws, regulations, and ASPPH policies
- Data breaches, disruptions, and threats receive appropriate responses

Data Custodians are responsible for operating and maintaining systems that collect, manage and provide access to data. Data Custodians may be either ASPPH staff or outside vendors contracted by ASPPH to serve as Data Custodians. Data Custodians maintain physical and system security of data including installation and maintenance of software, monitoring for security breaches, maintaining access logs, and setting file protection parameters; assign and revoke user access to data according to established policy; and implement procedures for data backup and recovery.

Institutional Reporting and Research Administrators are individuals from ASPPH member institutions who have been assigned by their institution's Primary Representative and are ASPPH's main contact regarding Institutional Reporting and Research. The Institutional Reporting and Research Administrator is responsible for managing their institutions' system users' access rights to My Institutional Reporting and restricted information and data.

System Users are individuals who have been granted access to My Institutional Reporting and/or Institutional Research in order to perform assigned duties, conduct research, or make other reasonable use of data. System users may include ASPPH staff, ASPPH members, or other affiliates of ASPPH. System users are expected to access data only through proper authorization and controls and disseminate data to others only when appropriately authorized. Access is provided to system users through the school or program's Primary Representative, the Membership Administrator, or the Institutional Reporting and Research Administrator.

Data Classification

Data is classified with respect to its sensitivity and confidentiality, and access varies according to the classification assigned to the data, as defined by law, regulation, ASPPH policy and/or general

expectations of the public and/or member institutions with respect to individual information. Data Trustees are responsible for assigning institutional data to these three classifications: public, limited access, or restricted.

Full Access data is not considered sensitive or confidential and access may be granted to any user who requests it. Full Access data, when published by ASPPH, is done so without restrictions. Examples of public ASPPH data include aggregate enrollment of ASPPH member institutions presented in publicly available reports; membership lists; and published research reports, white papers, and other documents in which aggregated or individual data appear.

Limited Access data are data that are not classified as restricted and are exclusively for use by ASPPH and its member institutions. Examples of limited access ASPPH data include all data published to the Institutional Research page of the MyASPPH web portal and published research reports, white papers, and other documents that are not published publicly and are for exclusive use by ASPPH and its member institutions.

*Restricted data i*s any confidential information or data that may be protected by statute, regulation or court order and/or which is considered confidential or highly sensitive by ASPPH. Examples of restricted data include but are not limited to financial data, individual salaries submitted by member institutions, information submitted by individual applicants through SOPHAS, consumer health data, biometric and genetic data, sensitive personal data, including but not limited to race, ethnic origin, religious beliefs, immigration status, etc.

ASPPH staff are expected to have policies in place that will protect confidentiality when restricted information is used in aggregate form to create reports and publications.

No restricted information or data shall be shared with other parties except through a signed data use agreement which provides that such information or data will be held confidential by the other party. A recipient of such restricted information or data may use such information or data only according to the terms and conditions set forth in a data use agreement between ASPPH and the other party.

Intellectual Property

ASPPH data are produced in various formats including, but not limited to, online dashboards and reports, printed publications, presentations, and web documents. These works are considered the intellectual property of ASPPH and shall be cited accordingly. The transfer of ASPPH data to another party shall be done by and through a data use agreement with such other party, which shall provide for terms of use of such data, the length of time such data may be used, and appropriate terms, conditions, and restrictions on who may use such data and for what such data may be used. Such transfer shall not be considered the sale of data to such other party unless specifically stated to be so. ASPPH data shall always be returned to ASPPH after another party, pursuant to contract, has finished using such data. In the case of electronic data, the party shall permanently delete data from all of its storage devices and confirm such deletion of data with ASPPH. ASPPH reserves the right to confirm the return and deletion

of all data upon completion of use and termination of the data use agreement.

If ASPPH data is co-owned by another party and ASPPH intends to transfer such data to a third party for a legitimate purpose, ASPPH shall always acquire written approval for such transfer from the data co-owner.

Safeguards

ASPPH shall require that all recipients of ASPPH data develop, implement and, use appropriate safeguards to prevent unauthorized use or disclosure of ASPPH data provided to them. Such recipients must store ASPPH data in their possession in a secure facility and electronic database that is password-protected. A recipient shall ensure that its employees, agents, and/or subcontractors will follow the same safeguards, restrictions, and conditions as the recipient is required to follow. ASPPH, at its sole discretion and at any time, may request proof from a recipient that it has developed and is using appropriate and useful safeguards. ASPPH staff shall have the rights to review the use of ASPPH data at any time to ensure that proper safeguards are implemented. ASPPH may require a recipient to provide ASPPH access to the recipient's facilities and devices to ensure that appropriate and effective safeguards have been implemented.

Data Use

System Users may use ASPPH data for their own internal purposes in accordance with this Policy. ASPPH requires that the use of ASPPH data be preapproved by ASPPH before such information is presented or published externally to the user's organization. In the event such information is intended to be published or become part of another publication, ASPPH shall have the right to monitor and control the use of such information. ASPPH shall have the right to question any System User as to the use of information acquired from ASPPH pursuant to this Policy. In the event that ASPPH data is used publicly or for publication by a System User in whole or in part, the System User shall note that such data was acquired from ASPPH through allowable access to published material or online resources, or through a Data Use Agreement, and that ASPPH has had no involvement regarding the conclusions reached in such publication. ASPPH shall require that such acknowledgement provides that ASPPH does not endorse or otherwise approve of the conclusions reached in such publication.

ASPPH is not responsible for the use of data reported to ASPPH that is used for accreditation reporting. It is the member institution's responsibility to assure that data reported for accreditation is valid and accurate.

Dealing with Data Security Breaches

A data security breach occurs when unauthorized individuals gain access to ASPPH data classified as limited use or restricted. When a data security breach is identified, the identifying parties, in partnership with ASPPH, should follow this procedure:

- **Notify ASPPH Institutional Reporting and Research Staff** immediately

- Identify the security gap that caused the breach and close the security gap
- Document the cause of breach and the solution
- Identify contacts who are statutorily required to be notified and notify them
- Identify contacts who, as a courtesy, should be notified about the breach, and notify them

Enforcement

Individuals who violate the terms of this policy may be denied access to ASPPH data by the appropriate ASPPH staff. Such an individual may be subject to penalties and disciplinary action by ASPPH. Allegations of violations of this Data Policy may be reported to administrators and officials who have supervisory control and jurisdiction over the individuals alleged to have committed violations. An alleged violator who works for or is otherwise under the control and supervision of ASPPH may be subject to ASPPH disciplinary action.

Changes

This policy is effective as of October 29, 2024. ASPPH reserves the right at its discretion to change, modify, add or remove portions of this Data Policy at any time. We will notify you of material changes by e-mail and/or by notice on the MyASPPH website. Your continued use of the service following any changes signifies your acceptance of these changes.