American Association of Colleges of Pharmacy
Institutional Data Policy Statement

Introduction

Institutional data is defined as data gathered, analyzed and published by AACP in support of its overall mission to serve its member colleges and schools and their respective faculties, by acting as their advocate at the national level, by providing forums for interaction and exchange of information among its members, by recognizing outstanding performance among its member educators, and by assisting member colleges and schools in meeting their mission of educating and training pharmacists and pharmaceutical scientists.

Institutional data is an essential asset of AACP. As with all assets, it is important to find an appropriate balance between maintaining the ability of authorized individuals to access and use the asset, while minimizing the exposure to the risk that is inherent by making the asset available.

AACP is an owner of institutional data and a custodian of data owned by and gathered from its members. Institutional data requires appropriate maintenance and protection to assure quality and integrity. It further requires management, usage, dissemination and protection in a manner consistent with laws and regulations as well as with the collective desires of the membership of AACP. Institutional data is also subject to risks and threats such as accidental loss or damage, unauthorized access, malicious misuse, and inadvertent alteration or disclosure.

The policies described herein are intended to address three key aspects with respect to institutional data: the ownership of data, the nature of data with respect to sensitivity and confidentiality, and the roles and responsibilities of individuals with access to data. The purpose of these policies is to set forth a balance between protecting institutional data owned by or under the custodianship of AACP from accidental and/or intentional damage and unauthorized access, disclosure or alteration while also assuring that individuals authorized to use the data have appropriate access as required for their responsibilities and duties. The policies presented here are not intended as a complete statement of all policies related to AACP institutional data. As described below Data Trustees, Data Stewards and Data Custodians are expected to establish and/or implement specific policies with respect to data as it relates to their responsibilities and functional roles.

Ownership and Custodianship

Data aggregated by AACP from information submitted by individuals, member colleges and schools is owned by AACP and is used to produce reports and publications and conduct research. AACP assumes responsibility for the quality and integrity of the data to the extent that such aggregations present a true picture of the individual data submitted by individuals and/or member colleges and schools. AACP does not assume responsibility for the accuracy of the individual data submitted by individuals and/or member colleges and schools used to create aggregated data. Individual data submitted by individuals and/or member colleges and schools are owned by the individuals and/or member colleges and schools that submitted the data. AACP serves as a custodian of this data. AACP shall take all appropriate measures to prevent the unintentional and/or intentional loss or destruction of data under its custodianship; however, the Association does not assume responsibility or liability in the event that this takes place.

Data Roles and Responsibilities

Data Trustees are AACP staff who have policy and planning responsibility with respect to institutional data and have ultimate responsibility for data within their area of duties and control. Data Trustees establish policies and ensure their implementation with respect to management, use and protection of data; determine

whether data is public, limited access or restricted; and oversee the data with respect to accuracy and integrity.

Data Trustees must ensure:
- All individuals with access to data are trained in data management, use and protection;
- Data policies are communicated to users;
- Access, security and disaster recovery plans are implemented;
- Restricted data is protected by specific and enforced security plans;
- Compliance with laws, regulations and AACP policies;
- Data breaches, disruptions and threats receive appropriate responses.

Data Stewards are AACP staff with operational responsibility with respect to institutional data. Data Stewards implement policies and are responsible for the direct management, use and protection of data; gather, analyze and coordinate the publication of data; interpret and comply with laws, regulations and AACP policies with respect to data; coordinate training of individuals with access to data; and, in concert with Data Custodians, develop and implement access, security and disaster recovery plans.

Data Custodians are responsible for operating and maintaining systems that collect, manage and provide access to data. Data Custodians may be either AACP staff or outside vendors contracted by AACP 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.

Data Users are individuals who have been granted access to institutional data in order to perform assigned duties, conduct research, or make other reasonable use of data. Data Users may include AACP staff, AACP members and other volunteers, vendors, contractors, or other affiliates of AACP. Data Users are expected to access data only through proper authorization and controls; access only the data on a need to know basis with respect to authorized use; disseminate data to others only when appropriately authorized; report access privileges inappropriate to their authorization; be knowledgeable of AACP security procedures and confidentiality procedures; and perform the role of a Data Custodian when data is place on a personally owned or managed system or device.

Data Classification
Data classification is used to define data with respect to its sensitivity and confidentiality and access varies according to its sensitivity and confidentiality requirements as they may be defined by law, regulation, AACP policy and/or general expectations of the public and/or member colleges and schools with respect to individual data. Data Trustees assign institutional data to one of three categories: public, limited access or restricted.

Public data is not considered sensitive or confidential and access may be granted to any user who requests it. Public data, when published, is done so without restrictions. Examples of public data under AACP ownership and/or custodianship include aggregated enrollment, financial and salary data of member colleges and schools presented in publicly published reports; membership rosters and directories; enrollments of students, tuitions, and curricula at individual member colleges and schools; and published research reports, white papers and other documents in which aggregated or individual data appear.

Limited Access data must be requested from, and authorized by, the Data Trustee and/or Data Steward who is responsible for the requested data. Limited data generally is not considered sensitive or confidential but access is granted only to users who have an express and appropriate need for the data as determined by the Data Trustee and/or Data Steward. Restrictions are usually applied to users with respect to further use of the data. Examples of limited access data under AACP ownership and/or custodianship are peer comparison reports prepared at the request of member colleges and schools and mailing lists of individual members. As examples of possible restrictions placed on the use of limited access data, colleges and

schools may be requested to not publish requested peer comparison reports and mailing lists may be limited to a one-time use by purchasers.

Restricted data is information that may be protected by law and/or regulation or considered confidential or highly sensitive by AACP policy. Access to restricted data is limited to Data Trustees and Data Stewards that have responsibility for the data within their area of duties and control and to users who are the owners of data that is under AACP custodianship. Examples of restricted data include financial data and individual faculty salaries submitted by member schools and colleges and data and information submitted by and gathered from individual applicants through PharmCAS. Data Trustees and Data Stewards are expected to have policies in place that will protect confidentiality when restricted data is utilized in aggregate form to create reports and publications. For example AACP does not report mean salaries unless more than four values are used in the calculation and does not report mean data gathered from financial surveys of member colleges and schools unless more than three values are used in the calculation. For peer comparison reports requested by member colleges and schools AACP requires a minimum of five peers schools to perform the comparison analysis. Individual-specific and school-specific salary data and school-specific financial information is only provided to the member college or school that owns and originally reported the data to AACP. Requests for this information will only be released with the explicit approval by the CEO dean of that institution.

Intellectual Property
AACP reports and publications are produced in various formats including, but not limited to, printed publication, paper reports, and web documents. These works are considered the intellectual property of the Association and should be cited appropriately.

Enforcement
Individuals who violate policy described herein may be denied access to institutional data and may be subject to penalties and disciplinary action, both by AACP and by other authorities such as governmental officials when policy violations are also in violation of laws and regulations. Allegations of violations should be reported to administrators and officials who have supervisory jurisdiction over the individuals alleged to have committed violations. An alleged violator will be subject to AACP disciplinary action.