University of Virginia
Administrative Data Access Policy

Approved June 24, 1994
President's Cabinet
Revised September 1996
Revised October 2001

TABLE OF CONTENTS

1.0: Philosophy
2.0: Definition of Administrative Data
3.0: Roles and Responsibilities
4.0: Requests for Access to University Administrative Data
   4.1: Legally Restricted or Limited-Access Data
   4.2: Exceptions
   4.3: Denial
   4.4: Appeal
5.0: Responsibility of Data Users
   5.1: Use of Administrative Data only in the Conduct of University Business
   5.2: Maintenance of Confidentiality and Privacy
   5.3: Protection of Data
   5.4: Accurate Presentation of Data
   5.5: Maintenance of Data Quality

Definitions of Important Terms

1.0: Philosophy

Information maintained by the University is a vital asset that will be available to all
employees who have a legitimate need for it, consistent with the University's responsibility to preserve and protect such information by all appropriate means. The University is the owner of all administrative data; individual units or departments may have stewardship responsibilities for portions of that data. The University intends that the volume of freely accessible data be as great as possible, given limitations of budget.

The value of data as an institutional resource is increased through its widespread and appropriate use; its value is diminished through misuse, misinterpretation, unnecessary restrictions to its access, or failure to maintain quality. The University expressly forbids the use of administrative data for anything but the conduct of University business. Employees accessing data must observe requirements for confidentiality and privacy, must comply with protection and control procedures, and must accurately present the data in any use. In addition, the University and its employees do comply with applicable state and federal laws and regulations, including state ITRM standards and guidelines.

The University determines levels of access to administrative data according to principles drawn from various sources. State and federal law provides clear description of some types of information to which access must be restricted. In an academic community, ethical considerations are another important factor in determining access to administrative data (see Appendix A).

2.0: Definition of Administrative Data

The University's data base consists of information critical to the success of the University as a whole. The University data base is shared data, managed within a conceptual framework. It is likely that the University data base will be distributed across processing units both within and outside the University. Specific types of data, such as research data and electronic mail "boxes," may be covered by specially tailored policies.

Data may be digital text, graphics, images, sound, or video. The University regards data that are maintained in support of a functional unit's operation as part of the University's administrative data base if they meet at least one of the following criteria:

- if at least two administrative operations of the University use the data and consider the data essential;
- if integration of related information requires the data;
- if the University must ensure the quality of the data to comply with legal and administrative requirements for supporting statistical and historical information externally;
- if a broad cross section of University employees refers to or maintains the data; or
- if the University needs the data to plan.

Some examples of administrative data include student course grades, patient records, employee salary information, vendor payments, and the University's annual Data Digest. Administrative data does not include personal electronic calendar information and similar material.

3.0 Roles and Responsibilities

As part of their jobs, University employees take on various roles and responsibilities (see Appendix B) with respect to University administrative data. Under the guidance of various University leaders, especially the chief information officers of the University and the Health System, individuals may fill the roles of data stewards, data security contacts, data users, data,
processors, and system sponsors. In addition, various individuals and groups provide data-related services, especially the agency information security officers, data administrators and data security administrators in the Department of Information Technology and Communication and in Health System Computing Services.

4.0: Requests for Access to University Administrative Data

4.1: Legally Restricted or Limited-Access Data

Access to legally restricted or limited-access data (for definitions of the three categories of University administrative data, see Appendix A) by University employees, employees of University-related foundations, or non-U.Va. employees sponsored by a University manager requires that a formal request be made to the appropriate data security contact.

4.2: Exceptions

All requests for exceptions to data access policies must be made in writing to the data security contact. E-mail requests are acceptable. The request must specify the data desired and their intended use.

4.3: Denial

The data security contact must provide a written record of the reasons for denial of any request to access University administrative data. E-mail records are acceptable.

4.4: Appeal

Members of the University community may appeal any decision that denies access to University administrative data. Appeals may be made to the appropriate data steward.

5.0: Responsibilities of Data Users

5.1: Use of administrative data only in the conduct of University business

The University expressly forbids the disclosure of unpublished administrative data or the distribution of such data in any medium, except as required by an employee's job responsibilities and approved in advance by the data custodian. In this context, disclosure means giving the data to persons not previously authorized to have any type of access to it. The University also forbids the use of any administrative data for one's own personal gain or profit, for the personal gain or profit of others, or to
satisfy personal curiosity.

5.2: Maintenance of confidentiality and privacy

Users will respect the confidentiality and privacy of individuals whose records they access, observe any ethical restrictions that apply to data they access, and abide by applicable laws and policies with respect to accessing, using, or disclosing information. All data users having any access to legally restricted or limited-access data will formally acknowledge (by signed statement or some other means) their understanding of the level of access provided and their responsibility to maintain the confidentiality of data. Each data user will be responsible for the consequences of any misuse.

5.3: Protection of data

Users will comply with all reasonable protection and control procedures for administrative data to which they have been granted the ability to view, copy or download.

5.4: Accurate presentation of data

Users will be responsible for the accurate presentation of administrative data, and will be responsible for the consequences of any intentional misrepresentation of that data.

5.5: Maintenance of data quality

Users are responsible for notifying data stewards or data security contacts when they recognize that data is in error, incomplete, obsolete or missing.

Definition of Important Terms

Access (to data): either (a) the capacity for data processors to enter, modify or delete data or (b) the capacity for data users to view, copy or download data.

Categories (of data): see Appendix A

- General administrative -- see Appendix A
- Legally restricted -- see Appendix A
- Limited-access -- see Appendix A

Domain (of data): The entire collection of data for which a University employee functioning as a data steward or data security contact (see roles in Appendix B) is responsible. The data domain also includes rules and processes related to the data.
Quality of data: In this context, quality is a collective characteristic that encompasses utility, objectivity, integrity, accuracy and completeness. Data quality is supported by presentation in an accurate, clear, complete, and unbiased manner, with sources identified in appropriate fashion, with potential sources of error identified, and with disclosure of the degree to which the data has been protected from unauthorized access or revision, from compromise through corruption, and from falsification.

Roles and Responsibilities: See Appendix B

Help

- Help Desk
- Request Help
- ITC How-to Guides
- Computer Terms Glossary

About

- ITC Services Directory
- Contact Us • Send Feedback
- Site Info • Page Updated: 2005-09-28 EDT
- © 2006 by the Rector and Visitors of the University of Virginia

Standards & Policy

- Disclaimer
- P3P Privacy Policy
- Accessibility: WAI • 508
- Web Standards: XHTML • CSS

University of Virginia
Information Technology and Communication
108 Cresap Road
P.O. Box 400217
Charlottesville, Virginia, 22904-4217 USA

© 2006 by the Rector and Visitors of the University of Virginia.

The information contained on the University of Virginia’s Department of Information Technology and Communication (ITC) website is provided as a public service with the understanding that ITC makes no representations or warranties, either expressed or implied, concerning the accuracy, completeness, reliability or suitability of the information, including warrantees of title, non-infringement of copyright or patent rights of others. These pages are expected to represent the University of Virginia community and the State of Virginia in a professional manner in accordance with the University of Virginia’s Computing Policies.