College of Health and Human Sciences Information Security Policy

Introduction

Colorado State University collects information of a sensitive nature to facilitate and enable its business/academic functions. Unauthorized access to such information may have many severe negative consequences, including adversely affecting the reputation of the University. Protection of such personally identifiable information from unauthorized access is required by various private sector, federal and state mandates, including among others the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the Family Educational Rights and Privacy Act (FERPA), Colorado House Bills 03-1175 and 06-1157, and the Payment Card Industry Data Security Standard. Sensitive information is stored on a variety of computer systems in the decentralized information technology (IT) environment at the University. As such systems are being subjected to increasing numbers and types of attempted unauthorized access, the adoption of these information security policies will aid in the protection of such information.

Definitions

Personal computers are comprised of desktops, laptops, tablets, personal digital assistants and other such devices of all brands, used principally by one individual at a time. This category includes laboratory computers.

The College of Health and Human Sciences at Colorado State University is referred to as "the College" as well as the acronym "CHHS" in this document.

Sensitive information includes, but is not limited to, social security numbers, personally identifiable health information, personally identifiable financial information including credit card information, driver's license information, personnel employment and student performance information, proprietary research and academic information, third-party proprietary information, FERPA protected non-directory information and any other information that through disclosure would adversely affect an individual or besmirch the reputation of the University.

Please note that the above list may change over time. Furthermore, information such as date of birth may not be considered "sensitive" by itself. However, when combined with other information about an individual (name, address and phone number, for example), may ultimately contribute to identity theft. Reasonable care should be taken to protect all information about faculty, staff, and students even if it is not itself considered to be "sensitive".

Resources

For other College and University IT Policies, please visit our website.

Information Security Policies

1. Files and File Storage

In general, users are responsible for their own files, including the information contained in those files, and ensuring that files containing critical data are stored on CSU-central (such as ARIES) or CHHS-central (such as CHHS file servers, including those that house the CHHS m: and p: drives) systems.

Sensitive information in individuals' files should be kept to a minimum, and reasonable and prudent protection of those files shall be implemented by CHHS system administrators (herein referred to as the

CHHS IT Group). It is the responsibility of the owner of the files containing sensitive data that are transmitted via the network to ensure that the files are reasonably protected against unauthorized access.

- In the College of Health and Human Sciences, all electronic data containing sensitive information shall be stored on either CSU-central (such as ARIES) or CHHS-central systems to ensure that the information remains as secure as possible.
- It is the responsibility of the CHHS IT Group to ensure that CHHS-central systems are kept as secure as possible. The CHHS IT Group will also ensure that these College-central systems are regularly backed up and that the backed up data is stored in a secure location.
- It is the responsibility of the department to contact the CHHS IT Group to ensure that access to sensitive information on CHHS-central systems is restricted to necessary personnel only. The CHHS IT Group can limit access to any set of files or folders on CHHS-central systems to a group of people chosen by the department.
- Sensitive information shall not be stored on desktops, laptops, or removable media. If the storage of sensitive information on these types of systems or media is necessary, the department is responsible for contacting the CHHS IT Group to ensure that the media is adequately and properly encrypted.

2. Social Security Numbers

After September 30, 2006, social security numbers (SSNs) shall not be stored on University or College Systems unless written authorization for doing so has been obtained from the Vice President for Information Technology.

3. Credit Card Information

Under no circumstances shall credit card information (including credit card numbers, expiration dates, and security codes) be stored on any personal computer or server managed by the College of Health and Human Sciences.