

Policy:	Security
Date Introduced:	08/24/01
Date Revised:	08/26/02, 12/09/02, 04/03/03, 08/15/03, 09/11/03, 02/28/05, 03/01/05, 04/12/05
Author:	Tim McCain

Colorado Immunization Information System
Security Policies and Procedures Manual

Colorado Immunization Information System
Colorado Dept Public Health and Environment
DCEED-IMM-A3
4300 Cherry Creek Drive South
Denver, CO 80246-1530
Main Line (303) 692-2700
Fax (303) 758-3640

By receipt of this document, you acknowledge that you understand that information contained within this document is confidential or proprietary information of The Colorado Immunization Information System. Any knowledge gained in the use of this document is to be kept confidential, and this confidentiality is a condition of the acceptance of this document. This information shall not be used or disclosed to anyone unless specifically authorized by The Colorado Immunization Information System. The unauthorized use or disclosure information contained in this document is possible grounds for legal action and/or a duty to mitigate damages.

No part of this document in part or whole, may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written consent of The Colorado Immunization Information System (CIIS). Inclusion of this document, in part or whole, into any published work either in verbal, electronic, or written form, is prohibited without express written consent from CIIS. This document contains present policies, standards, and procedures for securement of data maintained by CIIS and its facility, as such this document may be changed, or revoked, at any time and without notice. Your request and use of this document and related information constitutes your agreement to all aforementioned terms, conditions, and notices.

Table of Contents

Definition of the CIIS		Page 4
Section 1	Terms Used in Policy	Page 5
Section 2	Confidentiality Statement	Page 6
Section 3	Modification of security policy	Page 7
Section 4	Physical and environmental controls	Page 7
	4.1 Server controls	Page 7
	4.2 Server facility controls	Page 7
	4.3 Workstation controls	Page 9
	4.4 UCHSC confidentiality	Page 10
	4.5 Employee awareness	Page 10
Section 5	User access controls	Page 10
	5.1 User account policy	Page 10
	5.2 User database review	Page 13
	5.3 CIIS employee termination	Page 13
	5.4 Termination Procedure	Page 13
Section 6	Receipt/removal of components	Page 14
	6.1 Hardware installation	Page 14
	6.2 Suspicion of breach	Page 14
	6.3 Inventory and tracking	Page 15
	6.4 Component documentation	Page 15
	6.5 Mobile components	Page 15
	6.6 Component life cycle	Page 15
Section 7	Software standards	Page 16
	7.1 Data encryption	Page 16
	7.2 Database standard	Page 16
	7.3 Operating system standard	Page 17
	7.4 Web server standard	Page 17
	7.5 Local authentication	Page 17
	7.6 Virus protection	Page 18
	7.7 Logs and reports	Page 18
Section 8	Contingency policy	Page 20
	8.1 Physical and virtual controls	Page 20
	8.2 Removable media storage	Page 20
	8.3 Backup policy	Page 21

Section 9	Security breach policy	Page 23
	9.1 Security breach definition	Page 23
	9.2 Risk analysis and management	Page 23
Section 10	Data transmission policy	Page 26
	10.1 Transmission standard	Page 26
	10.2 SSL standard	Page 27
Section 11	User education and training	Page 27
	11.1 Initial education	Page 28
	11.2 Ongoing education	Page 28
	11.3 Virus protection	Page 30
	11.4 Patch management	Page 30
	11.5 Email policy	Page 30
Section 12	Third party employees	Page 31
	12.1 Definition	Page 31
	12.2 Policy compliance	Page 31
	12.3 Policy violation	Page 31
	12.4 Access assessment	Page 31
	12.5 Physical access	Page 31
	12.6 PHI securement	Page 31
Section 13	Future considerations	Page 32
Appendix A	CIIS Session Diagram	Page 33
Appendix B	CIIS Backup Methodology	Page 34
Appendix C	CIIS SSL Session Diagram	Page 35
Appendix D	CIIS SSH2 Session Diagram	Page 35
Appendix E	CIIS SSL Transmission	Page 36

Colorado Immunization Information System (CIIS)
Security Policies and Procedures

The Colorado Immunization Information System contains data used for the purpose of maintaining a central immunization record for the State of Colorado¹. To this degree, the Colorado Immunization Information System contains data that is sensitive in nature. Therefore, the offices of the Colorado Immunization Information System have created a security policy containing standards of conduct and controls used to ensure accurate and confidential data retrieval while maintaining a secure environment. Throughout this policy the term Colorado Immunization Information System (CIIS) will be considered both a reference to the offices and staff managing the system, as well as to the system itself. Due to ongoing changes within the health care and technology fields, the CIIS security policy will be reviewed, at minimum, on an annual basis to ensure compliance with current standards, laws, and legislation. Any security certification required by the Center for Disease Control, or any other governing body, will be performed by the CIIS staff, as well as a third-party contracted agency if applicable, to ensure compliance with the current security policy. This policy complies with the standards defined by the following agencies:

- Department of Health and Human Services
45 CFR Parts 160, 162, and 164
Health Insurance Reform: Security Standards; Final Rule
- Standards for Privacy of Individually Identifiable Health Information; Final Rule
- International Organization for Standardization (ISO 17799)
- American National Standards Institute (ANSI)
- National Institute of Standards and Technology (NIST)
- National Infrastructure Protection Center (NIPC)
- Crisis Emergency Response Team (CERT)
- Peter Gutman, University of Auckland

¹ A diagram of the CIIS session may be found in Appendix A

- 1 The definitions of terms used within the body of this policy are as follows:**
 - 1.1 Definitions of CIIS staff and participants:**
 - 1.1.1 Project Administrator (PA)**

Oversees the adherence to this security policy, on a program level basis. Provides fiscal approval, and oversight, of all IT projects, actions, and equipment. The Project Administrator must approve all IT standards and procedures.
 - 1.1.2 Systems/Application Security Analyst (SASA)**

Responsible for the daily IT operations in regard to acquisition, transmission, storage, and reliability of data. Maintains hardware and software services necessary for the transmission and storage of data. Responsible for the creation of a security policy and, upon approval from the Project Administrator, implementation and enforcement of the policy. Oversees data security as it relates to hardware, software, media, physical vulnerabilities, and user education. Will maintain logs to aid in investigations of anomalies or corruption of the CIIS infrastructure.
 - 1.1.3 Data Manager/Analyst (DMA)**

Responsible for daily maintenance and analysis of data; including data quality issues. The DMA will notify the Project Administrator of any data anomalies or corruption; and will maintain logs to aid in investigations of anomalies or corruption of the CIIS database.
 - 1.1.4 Immunization Coordinator (IC)**

Acts as a liaison between the users and the PA, SASA, and DMA. Responsible, along with the SASA and Help Desk Technician, for training of users in the security policies and procedures. Will report any security policy noncompliance to the PA or SASA. Will transport data received in the field to the CIIS office.
 - 1.1.5 Help Desk**

Acts as an intermediary between users and the SASA by being the first point of contact for any technical issues and questions. Will report any security violations to the PA or SASA. Responsible, along with the IC, for the training of users in the security policies and procedures.
 - 1.1.6 User**

Responsible to use all data and resources in a manner consistent with the policies regarding confidentiality and security as set forth by this policy. In addition, they will report any anomalies or breaches of security on their machines, or within their network, to any employee of CIIS, who must report it immediately to the SASA.

1.1.7 Site CIIS Administrator

Responsible for monitoring users at a participating site and insuring their compliance with the standards set forth in this security policy. Will contact CIIS in regard to account creation, modification, and disablement.

Information security is defined as:

“...the preservation of:

- a) confidentiality: ensuring that information is accessible only to those authorized to have access;**
- b) integrity: safeguarding the accuracy and completeness of information and processing methods;**
- c) availability: ensuring that authorized users have access to information and associated assets when required.”²**

1.3 A control is a set of policies, practices, procedures, organizational structures and software functions that “need to be established to ensure that the specific security objectives of the organization are met.”³

1.4 The CIIS is a database of immunization information that has been collected from all participating sites and is offered to those sites as a centralized resource of immunization data.

1.5 The term “participating sites” refers to any health care organization, including their employees, which is actively entering, retrieving, or accessing information contained within the CIIS Database.

**2 The Confidentiality statement for CIIS, including penalties for violation of the policy, can be found at: <https://crisp.uchsc.edu/crisp>
Sanctions for violations of confidentiality may be imposed as stated in Colorado Revised Statute 25-4-1705, Section 5, Sub-section III, Parts A and B:**

“(A) Any officer, employee, agent of the department, or any other person who violates this section by releasing or making public confidential immunization records or epidemiological information in the immunization tracking system or by otherwise breaching the confidentiality requirements of subparagraph (II) of this paragraph (e) or releasing such information without authorization commits a class 1 misdemeanor and, upon conviction thereof, shall be punished as provided in section 18-1.3-501 (1), C.R.S. The unauthorized release of each record shall constitute a separate offense pursuant to this subparagraph (III).

² Section 1.2 quoted from the International Organization for Standardization 17799 PG viii.

³ Section 1.3 quoted from the International Organization for Standardization 17799 PG viii.

(B) Any natural person who in exchange for money or any other thing of value violates this section by wrongfully releasing or making public confidential immunization records or epidemiological information in the immunization tracking system or by otherwise breaching the confidentiality requirements of subparagraph (II) of this paragraph (e) or releasing such information without authorization commits a class 1 misdemeanor and, upon conviction thereof, shall be punished as provided in section 18-1.3-501 (1), C.R.S.”

- 3 The Colorado Immunization Information System holds the right to modify this security policy any time they see fit, and will make every attempt to contact all users to notify them of the changes that will affect them. All modifications to this policy must be approved by the SASA, with final approval being made by the PA.**

- 4 Physical and environmental controls for the locations of servers, workstations, and any other machine that will convey information contained within the CIIS are crucial to the confidentiality of data. Therefore all persons employed by CIIS will adhere to all standards stated within this section. Although CIIS does not mandate the compliance of these standards to participating agencies, unless stated otherwise, CIIS considers the standards to be best practice and recommends the implementation of the standards unless found to be inapplicable to the agency’s situation.**
 - 4.1 Any server that maintains CIIS information will comply with the following controls:**
 - 4.1.1 The use of RAID 5, at a minimum, on all drives hosting the database and RAID 1 on the system drives.**
 - 4.1.2 BIOS Passwords at the setup and boot level when feasible.**
 - 4.1.3 Server Locks – Both on the case of the machine and on their enclosure, when applicable.**
 - 4.1.4 UPS Backup – Commensurate with the size of the server, with a battery life capable of shutting down the server safely and server shut down capability.**
 - 4.1.5 Server traffic is filtered at the Transport and Application layers.**
 - 4.1.6 Disabling any removable media drives or communication ports when feasible.**

 - 4.2 The following physical safeguards must incorporated for any facility housing a server containing information obtained from the CIIS Database, as well as any area within that facility housing the server:**
 - 4.2.1 The CIIS central server will be located within a facility that is secured at all points of entry with either tumbler lock and/or keypad devices.**
 - 4.2.2 The area will be locked at all times and any persons wanting to gain admittance must contact an employee within the secured area and explain their reason for being there. Any suspicious activity will be reported to the SASA immediately.**

- 4.2.3 Any person requesting entry must be physically let into the area by the employee; the employee must then escort the person and ensure that the person's actions are visible at all times.**
- 4.2.4 Both the main entry door and the door to the server room will be secured via a keypad entry system. Only those UCHSC employees that have cause to work with the servers in that room will be granted a keypad code.**
- 4.2.5 UCHSC will maintain a list of approved CIIS employees that may be allowed into the server area, and who may work on the CIIS server locally. Any person not on the list will not be allowed entry.**
- 4.2.6 All CIIS employees who have been granted access to the UCHSC server room will be given a list of contact names and numbers and will be briefed on server center procedures and proper protocol.**
- 4.2.7 Any facility that houses data taken from, or sent to, the CIIS must keep all points of entry locked when the facility is not staffed, or when the area of data storage cannot be directly observed.**
- 4.2.8 Any server configured for the purpose of redundancy to the CIIS will be stored in the CIIS offices and the area will be secured via locking mechanism from unauthorized action.**
- 4.2.9 Any server configured for the purpose of redundancy to the CIIS will be stored in an enclosure and the enclosure will be secured via locking mechanism from unauthorized action.**
- 4.2.10 Only staff approved by CIIS will be given keys to the redundant server area and the enclosure, all other parties will not be allowed access in the server area without direct supervision of a CIIS staff member.**
- 4.2.11 CIIS reserves the right to deny any party access, or revoke access, to both the primary server room and the secondary server room for any reason and at any time.**
- 4.2.12 All facility maintenance records of any work performed can be obtained at:
Central Services and Administration
4200 East Ninth Avenue
Denver, CO 80262**
- 4.2.13 Inspection of all facilities housing CIIS data, to include the monitoring of basic physical controls and reporting of problems/issues found, will occur through a third party agency approved by the CIIS. Any concerns will be reported immediately to the PA or SASA.**

- 4.2.14** A redundant power supply, such as an external diesel generator, will be used to maintain consistent power to the facility housing the CIIS. When is it not feasible to incorporate this control, a comparable alternative should be applied.
 - 4.2.15** A gas-based fire protection system will be active in any facility housing the CIIS. When is it not feasible to incorporate this control, a comparable alternative should be applied.
 - 4.2.16** Continuity of facility security will be reviewed routinely to assure compliance with the policies set forth in this section by all parties.
- 4.3** Any workstation or peripheral that accesses the CIIS Database, or disseminates CIIS Database data to a user, will:
- 4.3.1** Be enclosed in an area that can be secured, when not in use, from any person not authorized to access the CIIS.
 - 4.3.2** Be placed in such a way as to ensure the CIIS session cannot be observed by other users or non-users.
 - 4.3.3** Utilize a password lockout scheme to ensure the machine will prohibit unauthorized access when not in use.
 - 4.3.4** Be turned off at the end of the business day.
 - 4.3.5** Have a case lock system that will ensure tampering or removal of parts cannot occur to the computer should it be out of the direct control of the user or site. The key to which, will be secured by the person in charge of IT resources at the facility
 - 4.3.6** Be secured within an office, or other pre-defined space, which utilizes a tumbler-locking device and can be locked from the public when not in use.
 - 4.3.7** Be turned off when not in use.
 - 4.3.8** Utilize a surge protection device.
 - 4.3.9** Have any communication device installed registered with the SASA.
 - 4.3.10** The user will not allow others onto the computer while they are logged into the CIIS, or network domain, and must log off the CIIS and domain upon completion of tasks.
 - 4.3.11** The installation of hardware on any machine accessing the CIIS should be limited to only essential components, and only when absolutely necessary. Approval must be obtained from the PA or SASA prior to installation.
 - 4.3.12** The installation of third-party software should be limited to only that which is necessary for the performance of the user's job. The PA or SASA must approve additional software prior to its installation.

- 4.4 All machines and users that access the UCHSC network must comply with the UCHSC policies regarding confidentiality. The policies can be found at the UCHSC web site:**
<http://www.uchsc.edu/is/policies/aup.htm>
It is the responsibility of the user to consult this policy, the UCHSC help desk, or the SASA should there be any questions about the campus protocol.
- 4.4.1 Due to the UCHSC network being protected through the use of firewalls, only HTTP, FTP, SSL, SSH and email traffic are allowed on campus; no other services are allowed without approval by UCHSC.**
- 4.4.2 The creation process of UCHSC accounts differs from that of CIIS accounts, therefore UCHSC should not be contacted about issues surrounding CIIS accounts.**
- 4.5 Facilities accessing the CIIS will ensure employee understanding of physical security standards by issuing a statement detailing all precautions involved in the physical securement of their facility. Anyone participating in the CIIS program should establish a policy in regard to hardware/software receipt and removal that is reasonably sufficient to protect the confidentiality of CIIS data, given the size and resources of the facility⁴. Failure to maintain a secure environment can result in the facility losing their ability to implement and use the CIIS.**
- 5 As UCHSC user accounts and CIIS user accounts are managed by two separate entities, they should therefore be consulted independently for security problems associated with that account. UCHSC problems should be directed to the UCHSC help desk⁵, while CIIS Database security problems should be directed to the SASA.**
- 5.1 The following standards pertain to the process of CIIS account confirmation, establishment, and modification; violation of these standards may result in access to the CIIS being rescinded or denied.**
- 5.1.1 Access authorization is the process of confirming a user's identity, validating their level of need, and documentation of the process.**
- 5.1.1a Any party requesting access to the CIIS must be actively employed by a site that has a completed Letter of Agreement (LOA) on file with CIIS. If there is no LOA on file for the site, the account request will be denied.**

⁴ Refer to section 6 for further standards on the receipt and removal of hardware and software components from a facility.

⁵ The UCHSC help desk can be contacted Monday through Friday from 8 am to 4 pm (MST) at (303) 724-4357 or in person on the fourth floor of building 500 on the UCHSC Fitzsimmons campus.

- 5.1.1b All parties requiring access to the CIIS must complete an account request form⁶. Any request not made with this form will not be approved.
- 5.1.1c Each site participating in CIIS will have a designated Site Administrator; each Site Administrator will be selected and approved by the CIIS Information Technology staff.
- 5.1.1d The Site Administrator must approve each account request and access request of every user associated with their site, and must state their approval in writing to the CIIS staff before any account will be created.
- 5.1.1e Access must be approved by the CIIS staff before an account to the CIIS will be created.
- 5.1.1f Only after the Site CIIS Administrator validates an account and access controls are defined for the user, will an account be approved and created.
- 5.1.1g An account request form must be signed by both user, and Site CIIS Administrator or it will not be approved.
- 5.1.2 Access Establishment is the process of creating an account for the purpose of access to the CIIS. Authentication to the CIIS is user-based, in that each account is created unique to the user based on information supplied by the user and confirmed by a Site CIIS Administrator. Once the user has authenticated to the system, their account privileges are role based and are dependant upon user's access need and job requirements.
 - 5.1.2a Level of access for an account will be determined based upon:
 - a) User's responsibilities in regard to data entry
 - b) User's need to access information contained in the CIIS
 - c) User's need to access administrative components of the CIIS.
 - d) Account permanence
 - 5.1.2b Once an account is created, the user will be contacted directly by a CIIS employee who will inform them of their account ID and password via telephone.
 - 5.1.2c Account information will only be given directly to the user after confirmation of the user's identity. Account information will not be left on voicemail, or given to another person.

⁶ The form can be obtained on the CIIS website https://crisp.uchsc.edu/crisp/help/login_request.htm or by contacting the CIIS offices at (303) 724-1043.

- 5.1.2d** Upon receipt of their account, the user will be required to access the CIIS at that time and change their password. The password must comply with the following criteria:
 - a)** Eight to twelve characters in length.
 - b)** Password must be alphanumeric, containing both number and letter characters.
 - c)** Password cannot begin or end in a number
 - d)** Password cannot contain patterns of the same three characters or more
 - e)** Password cannot contain repeating patterns of three characters or more
 - f)** Password cannot contain spaces
- 5.1.2e** The user can then access the CIIS via password authentication with their account only. The use of another account not approved by CIIS for the user will result in access being revoked.
- 5.1.2f** The user cannot allow another person to use their account information. Allowing another person to use their account to access the CIIS will result in both users' access to the CIIS being revoked. Further sanctions may result from any violations of the laws and policies set forth in section 2 of this policy that were incurred by violation of this section.
- 5.1.2g** All users are required to log off of the CIIS upon completion of their session.
- 5.1.2h** All account requests will be kept on file at the CIIS offices.
- 5.1.3** Access modification is the standard by which a user's account will be modified after the account has been created and is made active.
 - 5.1.3a** Minor account modification (e.g. demographic information) may be performed via the CIIS user info interface, or by contacting the CIIS offices.
 - 5.1.3b** Any major account modification (e.g. account id, disablement, security modification, etc.) will be performed by an employee of CIIS. All major modifications must be requested, in writing, by the user and approved by their Site Administrator.
 - 5.1.3c** Site CIIS Administrators must inform CIIS immediately if a user will no longer participate in the CIIS program so that the account can be disabled.

- 6.3** The CIIS has a mechanism for the inventory and tracking of software and hardware components that is received at the facility. The inventory is to be centrally managed by the SASA and all users will be informed of the management contact for the tracking system.
- 6.4** Once a component is received by the CIIS, the component will be entered into the inventory. If a component is removed after its initial installation, a narrative of the action will be created to aid in any subsequent security investigation in the event of a breach. All employees must give notice to the SASA prior to installation of hardware. Should the hardware be determined to create more risk than the benefits provided by its installation, its installation will be denied.
- 6.5** Any component that will be utilized in a mobile capacity must be registered as such with the SASA so that mitigation of potential vulnerabilities can be performed, thereby reducing the impact of a breach, should one occur.
- 6.6** Any component that stores protected, or sensitive, data and can be easily removed from the CIIS facilities is required to have encryption software installed and all data defined in this section will be encrypted by the software.
- 6.7** At the end of the component's life cycle it will be disposed of in the following manner to ensure there is no disclosure of information obtained through communication with the CIIS.
- 6.7.1** All fixed media will be securely erased using a third party application to ensure that all data on the media is unrecoverable⁹. If it cannot be erased, the media will be destroyed in such a way that data cannot be recovered.
- 6.7.2** All removable media will be securely erased using a third party application to ensure all data on the media is unrecoverable⁹. If it cannot be erased, the media will be destroyed in such a way that data cannot be recovered.
- 6.7.3** All paper documents containing data obtained from the CIIS will be shredded or destroyed to the point that visual recognition cannot occur.
- 6.7.4** Any media may be re-used, either removable or fixed, so long as it has been securely erased.

⁹ The CIIS considers data to be “unrecoverable” after erasure under the Gutman standard, which can be found at http://www.usenix.org/publications/library/proceedings/sec96/full_papers/gutmann/

6.7.5 If the possibility exists that there will be a future need to access the data contained on the component, the data may be saved to a secure storage facility that must comply with the standards set forth in section 8.2 of this policy.

7 CIIS recognizes that software applications applied to the CIIS servers, as well as those accessing the CIIS, are potential attack vectors and therefore must be secure in accordance with best practice. CIIS has therefore created software standards aimed at decreasing the potential for exploit of these vectors. These standards will not only cover the area of software, but are to include any type of audit log associated with the application as well. The standard will designate fields and log types necessary for the effective auditing of the CIIS.

7.1 Data encryption will be accomplished through the use of a 128-bit SSL Certificate.

7.1.1 The certificate will be acquired through a top level Certificate Authority.

7.1.2 The certificate validation and renewal will be performed by the SASA.

7.1.3 Information on certificate validity can be obtained while connected to the CIIS, or by contacting the CIIS offices.

7.2 CIIS will utilize, at minimum, Microsoft SQL Server 2000 to run its database. Any upgrades of this system will only occur after it has been determined by the CIIS staff to be prudent and secure.

7.2.2 The service pack, patch maintenance, and hardening of this server will be the responsibility of the SASA.

7.2.3 Maintenance of the database is the responsibility of the SASA.

7.2.4 Management of tables within the database will be the responsibility of the DMA and SASA.

7.2.5 The CIIS database tables will be configured to allow users to view site-specific information based on the user's account.

7.2.5 Account authentication occurs through domain authentication and through the CIIS application.

- 7.3 CIIS servers will run, at minimum, on a Microsoft 2000 platform. Any upgrades of this system will only occur after it has been determined by the CIIS staff to be prudent and secure.**
 - 7.3.1 The maintenance of the operating system will be the responsibility of the SASA, and will include all service pack and patch updates, as well as any hardening required to bring the server into compliance with this policy and current best practice.**
 - 7.3.2 NTFS partitioning will be used on all CIIS servers; access to the partitions will be managed by the SASA.**
 - 7.3.3 All servers will run only the minimum services and programs necessary to maintain the CIIS.**
 - 7.3.4 All servers will be assessed regularly for possible vulnerabilities that could create an exposure of the system. Any vulnerability found will be evaluated and mitigated to their lowest feasible risk level.**

- 7.4 Any CIIS server maintaining any web application will use, at minimum, Microsoft Internet Information Server 5.0. Any upgrades of this system will only occur after it has been determined by the CIIS staff to be prudent and secure.**
 - 7.4.1 The SASA will maintain the web server software through the provision of service packs and patches, as well as modifying the server to secure against known vulnerabilities, as determine by current best practice.**
 - 7.4.2 The SASA will configure and maintain all key sets necessary for the operation of the CIIS and its employees.**
 - 7.4.3 Any modifications to the CIIS web site will be performed within a development environment and tested thoroughly prior to deployment in the production environment.**
 - 7.4.4 Testing of modifications will be performed by the SASA, DMA, IC, and Help Desk, depending upon the nature of the modification. Modifications must be approved by the PA prior to being moved to production.**

- 7.5 Local authentication to any CIIS server will be achieved via the use of a domain account.**
 - 7.5.1 In the event an employee or application cannot authenticate via a domain account, a local account will be created by the SASA for the individual.**
 - 7.5.2 In the event it is necessary for an employee or application to access a service running on any CIIS server that cannot be accessed via either of these authentication methods, an account will be generated for the user based on the program or service's authentication policy.**

- 7.6 Virus protection for all UCHSC servers will be provided by the UCHSC Information Services Department through use of McAfee virus software and virus consoles. Management of this software is performed centrally through UCHSC, but it will be the responsibility of the SASA to inform UCHSC of any problems and to maintain the software locally.**
- 7.7 Activity on the CIIS will be monitored at a number of levels and through the use of multiple applications. The three main areas of observation for the CIIS will be the web server, database server, and the hardware.**
- 7.7.1 The web server will generate daily W3SVC logs that collect data on date, time, client IP address, User name, Server IP address, Server port, Method, URI stem, URI query, protocol status, and user agents.**
- 7.7.1a The logs will then be collected and manually scanned for anomalies and entries of attempted breaches.**
- 7.7.1b Once the logs have been manually scanned, they will be added to an analysis database that will produce html representations of web site activity for analysis of usage trends by the CIIS staff.**
- 7.7.2 The database of the CIIS has been designed with an audit table that tracks a user's session activity. The table will log user accounts, logins, logoffs, queries, posts, and duration.**
- 7.7.2a Table data will be collected and reports generated via SQL queries as to:**
- a) Data access**
 - b) Data manipulation**
 - c) Table access**
 - d) User habits**
 - e) Site access**
 - f) Access trends**
 - g) Anomalies**
- 7.7.2b In addition to the use of the audit table and SQL queries, the database server itself will be monitored via third-party application, or SQL query, and will observe:**
- a) Average Latch Wait Time (ms)**
 - b) Buffer Cache Hit Ratio**
 - c) User Connections**
 - d) Average Lock Wait Time (ms)**
 - e) Lock Timeouts/sec**
 - f) Database Allocation Percentage**
 - g) Transactions/sec**
 - h) Memory Pages/sec**
 - i) Percentage of Processor Time Used**

- j) **Disk Transfers/sec**
- k) **Network Kb Total/sec**

7.7.2c Although hardware output will be partially monitored through SQL tools, the server will be monitored through a system performance log as well. The log will create a baseline and monitor changes in hardware performance. The monitor will record:

- a) **Pool Nonpaged Failure**
- b) **Memory Available Bytes**
- c) **Memory Pages/sec**
- d) **Percentage disk Time**
- e) **Percentage Disk Idle Time**
- f) **Disk Reads/sec**
- g) **Disk Writes/sec**
- h) **Average Disk Queue Length**
- i) **Processor Interrupts/sec**
- j) **Percentage of Process Time On Processor**
- k) **Processor Queue Length**
- l) **Network Interface Bytes Total/sec**
- m) **Network Interface Bytes Received/sec**
- n) **Network Interface Bytes Sent/sec**

7.7.2d Operating system events will be collected via system, security, and application logs.

- a) **The logs will be monitored for anomalies that might show a security breach, system failure, or component malfunction. Server logs will be backed up, and archived at the CIIS offices.**
- b) **Audit logs will monitor unsuccessful login attempts as well as information changes to files other than the database.**

7.7.3 The logs may be written directly to the server, but must be moved to another machine as soon as possible and must be routinely backed-up up to a network storage device.

7.7.4 Audit logs will be reviewed at routine intervals, as well as after any possible unauthorized intrusion into the server.

7.7.5 Alerts and notifications of anomalies and violations of audit policies will be forwarded to the SASA.

- 8 The CIIS recognizes that events may arise that could cause a disruption of service to the CIIS. Therefore standards and procedures have been created to minimize the impact of the event on the availability and integrity of the data contained within the CIIS. The following procedures will cover facility and server access, as well as contingency plans in the event of catastrophic failure.**
- 8.1 In the event the server maintaining the CIIS must be accessed during an emergency, both physical and virtual controls have been built into the security plan.**
- 8.1.1 Should, during an emergency situation, the server need to be physically accessed, the server support group for UCHSC will be given emergency authority to perform whatever action is necessary until such time as a CIIS staff member responds to the server facility.**
- 8.1.2 Two CIIS personnel, the SASA and DMA, will be responsible for emergency response should there be a need. Both staff members will have access keys to the server's case and will be authorized to perform whatever task may be necessary until the emergency situation subsides and the CIIS is again able to function in a safe and secure manner.**
- 8.1.3 Both CIIS representatives will have the contact numbers for the server support personnel and will need to have the ability to contact them after hours should the need arise.**
- 8.1.4 The UCHSC server support staff will be made aware of the two contact points for the CIIS program in the event of emergency and will only contact them, as well as respond to their calls, should an emergency situation occur. Any action must be approved with the SASA prior to its execution.**
- 8.1.5 In the event that an emergency occurs that would facilitate the need for remote access to the server, the UCHSC server support department will be granted limited administrative privilege on the server. They can therefore stop and start services, applications, and the server when necessary.**
- 8.1.6 Remote access to any server will be performed via the use of a software package, or hardware device, that will utilize an accepted standard of security for encrypting its session.**
- 8.1.7 Remote access will only be allowed to those individuals granted the authority to do so by CIIS. CIIS limits this authority to only those individuals who are at an administrative and technical level to appropriately and effectively manage any emergency situation that may occur.**
- 8.2 All removable media will be stored off site at a facility overseen by the SASA. The facility will be locked and provides the ability to move, or otherwise protect, the media should a natural disaster or human interference attempt to destroy the media.**

- 8.3 The CIIS acknowledges that it is best practice to create and maintain a definitive back up policy so as to minimize the impact of a catastrophic event. The following contingency plan was developed to address the availability and integrity of data housed in the CIIS during such an event.**
- 8.3.1 The contingency plan will be reviewed every 90 days for accuracy and consistency with present status of data and program**
 - 8.3.2 Applications and data determined to be necessary for the proper maintenance and operation of the CIIS will be backed up nightly, and all applications will be kept on a separate set of CD media. Applications to be included in this category are:**
 - 8.3.2a Encryption software**
 - 8.3.2b Algorithms for SQL queries**
 - 8.3.2c SSL Certificates**
 - 8.3.2d Third party applications**
 - 8.3.2e Web Server Software**
 - 8.3.2f Server Operating System Software**
 - 8.3.2g SQL Server Software**
 - 8.3.2h Server hardware Drivers and Management software**
 - 8.3.3 Data that will be stored on removable tape media on a nightly basis will include, but not be limited to:**
 - 8.3.3a Primary CIIS Database**
 - 8.3.3b Primary CIIS Log Database**
 - 8.3.3c MSDB Database**
 - 8.3.3d Master Database**
 - 8.3.3e CIIS Backups to include:**
 - a) Full weekly backups**
 - b) Differential daily backups**
 - c) Transactional hourly backups**
 - 8.3.3f Web server logs**
 - 8.3.3g Server Security logs**
 - 8.3.3h Server Application logs**
 - 8.3.3i Server Security logs**
 - 8.3.3j Third party applications and their logs**
 - 8.3.4 Data backups and storage are classified into two categories; CD media and tape media. Media backups will occur as follows¹⁰:**
 - 8.3.4a Any data stored upon CD media will be backed up immediately upon receipt of application or data. The media will then be stored off site in a separate geographical location.**
 - 8.3.4b Any data that will be stored upon tape media will be backed up to two separate storage devices:**

¹⁰ Appendix B contains a diagram of the CIIS back up methodology.

- a) The first will reside in building 500 of the UCHSC Fitzsimmons Campus, and will be maintained by the Information Technology department of UCHSC.
 - b) The second will reside in building 406 of the UCHSC Fitzsimmons Campus and will be maintained by the Information Technology Department of CIIS.
- 8.3.4c** The UCHSC backups will occur daily with an initial full backup of the data, including system state, then will maintain daily differential backups from that point forward.
- 8.3.4d** The CIIS backups will occur daily and will perform a full backup of the data weekly, with differential backups on a daily basis during the week.
- 8.3.4e** The CIIS database itself will be backed up in full weekly, with differential backups occurring daily and transactional backups occurring every hour. Transactional backups will be increased as demand on the CIIS increases.
- 8.3.4f** Once the tape media has been created, it will be stored in a location that is geographically separate from the back up site. The storage facility will maintain security of the media while in its possession through the use of keyed locks, keypads, or a combination of both.
- 8.3.4g** All application and data backups will be tested at regular intervals to ensure data integrity and stability within the media.
- a) The restore process will be tested on a quarterly basis so as to maintain the smallest window of server down time as possible.
- 8.3.4h** Integrity of the backup media will be monitored daily to insure that all data is valid and can be restored from the media.
- 8.3.4i** Backup logs will be maintained, and read, daily.
- 8.3.4j** All software and hardware restoration exercises will be documented and used for future contingency plan modification and review.
- 8.3.4g** All tape and CD media will be released only to an employee of CIIS or their designated representative.
- 8.3.5** In the event of a disaster to the primary CIIS site, Fitzsimmons Campus - Building 500, that would prevent the normal operation of the CIIS, operations would be moved to the secondary CIIS site, the CIIS' main office, until such time as it is determined to be safe for the CIIS to begin operation in Building 500 again.

- 9.2.1 CIIS defines risk analysis as the study and investigation of a system's components, from hardware to software, to ensure all vulnerabilities have been mitigated to the highest level of security given budgetary and realistic operating parameter constraints.**
- 9.2.1a All components, whether software or hardware in nature, will be given an initial assessment for risk to the CIIS' existing architecture should they be introduced.**
 - 9.2.1b Components will be assessed as to their reliability in performing tasks consistent with the CIIS' daily activities.**
 - 9.2.1c Components will be assessed as to their validity to perform the tasks they are designed to control.**
 - 9.2.1d Components will be researched as to any history in regard to stability of the product overall and vulnerability to malicious attack. Potential component vulnerabilities will be weighed against ability to control and mitigate the stated vulnerability, impact of vulnerability on the CIIS, severity of the vulnerability, and long-term cost of labor investment.**
 - 9.2.1e Risk will be analyzed according to threat level of software or hardware vulnerability; threat level being defined as the practicality of the exploit, difficulty of exploit, whether an exploit presently exists, could exist, or is merely theoretical, and time/labor investment needed to maintain an acceptable level of risk.**
 - 9.2.1f Analysis will continue to occur after implementation of component to insure component continues to maintain an acceptable level of risk within the CIIS structure.**
 - 9.2.1g Internal risk analysis will be performed by the CIIS staff to test the present level of risk at the physical, network, and operating system vectors on all computers under CIIS management. Analysis will include, but will not be limited to:
 - a) Port scans**
 - b) Vulnerability scans**
 - c) Configuration scans**
 - d) Virus, worm, Trojan, spyware and malware scans**
 - e) Report generation of potential attack vectors and vulnerabilities****
 - 9.2.1h External evaluation of the CIIS will be contracted to a third party agency. The external evaluation of the CIIS will include, but will not be limited to:
 - a) Port scans**
 - b) Vulnerability scans**
 - c) Configuration scans****

- d) **Spyware and malware scans**
- e) **Stress testing**
- f) **Network mapping**
- g) **Report generation of potential attack vectors**
- 9.2.1i **Continued risk analysis will include, but will not be limited to:**
 - a) **Monitoring security information sites and periodicals**
 - b) **Obtaining notification from OEMs as to product updates**
 - c) **Monitoring system logs**
 - d) **Monitoring server logs**
 - e) **Monitoring audit tables**
 - f) **Monitoring access history**
 - g) **System alerts, to include server outages, file modification, intrusion detection, and firewall logs**
- 9.2.2 **The CIIS defines risk management as any action taken to ensure the best acceptable level of risk during the life cycle of the CIIS from all potential vectors of attack.**
- 9.2.2a **The task of risk management will include, but is not limited to:**
 - a) **Removing or disabling unnecessary services and applications**
 - b) **Maintaining the minimal amount of connections necessary for optimal operation and management of the CIIS.**
 - c) **Monitoring changes in security policy within the network.**
 - d) **Maintaining upgrades and updates to existing components.**
 - e) **Replacing, or repairing worn or obsolete components whose failure could result in CIIS compromise.**
 - f) **Developing and implementing secure code that ensures limited risk potential.**
 - g) **Maintain proper access control to the server through privilege accounts, limited account permissions, running services in accounts of least privilege, and physical restraints in both the facility and on the server.**
- 9.2.2b **Any breach, whether successful or unsuccessful, will be logged. The log will include the aggressor's time, date, IP address, exploit used, vulnerability associated with exploit, and the details of the breach.**

- 9.2.2c Included in the log will be the resolution to the breach, which will include resolution of the IP address, Registrar information about contacts, any correspondence that occurred with the contact, and any modifications made to the software or server.
- 9.2.2d The aggressor's IP address will be added to the CIIS' IP filters, and the UCHSC Network Support Team, as well as the aggressor's ISP, will be notified of the incident.
- 9.2.2e It is the sole discretion of the UCHSC Network Support Team as to any further action that will be taken in regard to firewall modification or access points.
- 9.2.2f In the event data is modified or deleted, a report will be issued to the governing law agency.
- 9.2.2b Risk management will also occur at the CIIS user level by limiting user accounts to least amount of privilege necessary to complete their tasks.
- 9.2.2c Users will be trained in the proper use of the CIIS and will be required to sign a statement acknowledging their training and understanding of proper use, as well as sanctions should they violate the CIIS security policy¹¹.
- 9.2.2d The CIIS Security Policy may be obtained by contacting:
 Elaine Lowery, CIIS Program Manager
 12477 East 19th Avenue
 Aurora, Colorado 80439
 (303) 724-1072

10 To comply with legislative mandates regarding the transmission of sensitive data between agencies, in addition to following current accepted best practices, the CIIS has created procedures and standards for the secure transmission of data to its facilities as well as to participants in the CIIS.

10.1 All immunization data required to update or maintain the CIIS will require encryption of the data during transmission to or from the offices of CIIS or through the Internet application. Due to environmental and procedural differences, each area of data transmission will be defined separately.

10.1.1 Direct transmission to the CIIS facility or employees of CIIS:

10.1.1a CIIS operates a secure FTP server that utilizes the SSL and SSHv2 protocols for session encryption¹². Use of CIIS FTP services will require that a formal request be made of the CIIS and an account approved. The user agrees not to disclose information about the FTP server, or their FTP account. All

¹¹ Sanctions are defined in sections 2 and 5.1 of this policy.

¹² Diagrams of the FTPS and SFTP sessions can be referenced in Appendix C and D respectively.

transmission schedules should be discussed with the CIIS staff prior to transmission of data. **Secure FTP is the only supported standard for the transmission of data to the CIIS offices.**

10.1.1b In the event identifiable information is sent via electronic mail, the data must be encrypted prior to transmission utilizing an algorithm accepted as secure. Any data sent to the CIIS offices via email must be approved by CIIS before transmission.

10.1.2 Transmission of data via the CIIS web application:

10.1.2a All data exchanged between the user's Internet browser and the CIIS immunization registration server will be encrypted using an algorithm accepted as secure.

10.1.2b CIIS utilizes the SSL standard for encrypting data during an Internet exchange¹³. CIIS uses 128-bit cipher strength for all SSL connections; any user attempting to access the CIIS site without using 128-bit cipher strength will be denied access.

10.2 As defined in section 10.1.2, the CIIS utilizes a Secure Socket Layer certificate for transmission of data to its web application. The certificate is created under the follow standards:

10.2.1 The CIIS certificate uses an RC4 128 bit encryption scheme, with an RSA 1024 key. The encryption schema utilizes SHA1 hashing to ensure session integrity.

10.2.2 The Internet Engineering Task Force (IETF) standard for SSL 3.0 and the Internet Draft of the IETF standard may be found at: <http://wp.netscape.com/eng/ssl3/draft302.txt>

10.2.3 The Standard for RC4 stream cipher may be found at: <http://www.rsasecurity.com/rsalabs/faq/3-6-3.html>

10.2.4 International Organization for Standardization (ISO) standard for RSA can be found at their web store under ISO 9796.

10.2.5 RSA standards can be obtained through RSA Laboratories' web site <http://www.rsasecurity.com/rsalabs/faq/3-1.html>.

11 The CIIS understands that a substantial part of maintaining a secure database is the continuing education of its users in all facets of security. The CIIS instructs users in multiple areas of security, including raising awareness of potential security concerns. Training is divided into two parts for the purposes of discussion, initial training and ongoing awareness education. Employees of CIIS are also required to follow, and comply with, the HSC computer use policy:

<http://www.uchsc.edu/policies/#Information%20Systems>

¹³ A diagram of the SSL session can be referenced in Appendix E

- 11.1 Initial user education occurs when a site comes online, when a user requests an account for the CIIS, and during new hire orientation. The initial training process encompasses the following areas of security education.**
- 11.1.1 Discussion of the CIIS security policy regarding user access, acts that violate policy standards, and the sanctions that will occur for policy violation¹⁴.**
 - 11.1.2 Discussion of proper use of the CIIS data and sanctions for misuse of data¹⁵.**
 - 11.1.3 Discussion of the proper use of the CIIS application, including login and log off policy.**
 - 11.1.4 All machines directly accessing the CIIS will be checked for vulnerabilities and for compliance of minimal connectivity requirements.**
 - 11.1.5 A cursory explanation of the Secure Socket Layer protocol and how it secures data.**
 - 11.1.6 Discussion of virus protection software, both strengths and weaknesses.**
 - 11.1.7 Users will be informed of safe Internet use activities and will be educated on unsafe practices that could result in a potential security breach.**
 - 11.1.8 Discussion of social engineering practices and ways to prevent security breaches through proper action.**
 - 11.1.9 Users will be informed of the password generation policy and any standards they must comply with in order to create a password on the CIIS system. They will also be informed of the ninety-day expiration standard and the method for password regeneration.**
 - 11.1.10 All users will receive this information through verbal instruction and documentation provided at the time of their training.**
- 11.2 Ongoing awareness education will occur after the user and site have begun using the CIIS, as well as during the employment of any CIIS staff member. Awareness education will build upon the base of knowledge given to the user during their initial security training through preventative and proactive measures to ensure compliance with established security standards, as well as to minimize any potential for a breach of security. Awareness education will include, but is not limited to:**

¹⁴ As defined in sections 2 and 5.1

¹⁵ As defined in section 2 and 5.1

- 11.2.1 The notification of Site CIIS Administrator, or a site's information technology department, of any security posts or announcements that could create security breaches or otherwise place the CIIS in jeopardy.**
- 11.2.2 Notifying the Site contact about any changes to the CIIS that would affect the site's ability to interact.**
- 11.2.3 Contacting CIIS Site Administrators to collect information on users that have been discharged from their site, or to inform them of accounts that have prolonged inactivity and confirm the user's status.**
- 11.2.4 Password expiration after ninety days of usage, thereby assuring all users will maintain a unique and secure password methodology.**
- 11.2.5 Site visits to make CIIS staff accessible for questions in regard to policy and to perform site checks to assure compliance with CIIS security standards.**
- 11.2.6 Providing web site links to agencies that supply further security compliance information, as well as proper data entry information.**
- 11.2.7 Users will be trained in the proper response to malfunctions and incidents of various situations.**
 - 11.2.7a Anomalies in software or hardware that adversely affect, or have the potential to impede, the normal function of the CIIS will be reported to the CIIS offices.**
 - a) An anomaly is any problem or situation, either malicious or overt in nature that the user has no technical ability to resolve.**
 - b) An application is any program, script, or file created by a user or a third party.**
 - c) Hardware is any physical piece of equipment that is used to obtain, store, or disseminate information in an electronic manner.**
 - 11.2.7b In the event a user suspects their password has been used or stolen they must contact their supervisor immediately; if the supervisor is not there, they should contact the CIIS offices via email or telephone.**
 - 11.2.7c When a supervisor receives notice of a lost, stolen, or misused account, they must also contact the CIIS offices immediately and re-register the user.**

11.5.6 Chain email and unsolicited virus warnings should not be forwarded. Any notification received about potential viruses should be sent to the site administrator or IS department, and it will be up to that person to notify users should the email be confirmed as legitimate.

11.5.7 Users should educate themselves to social engineering attacks via email, such as Phishing and hoaxes. In the event the user is unsure on how to handle a suspect email, they should contact their IT department, or the Help Desk.

12 The CIIS acknowledges that in the course of daily support of the CIIS, that it may be necessary to contract the services of a third-party company or contractor. Policies were created to define procedures to be taken when employing an outside contractor, and the contractor's responsibilities in regard to compliance with the policies and standards created by the CIIS.

12.1 Third party employees are defined as any person who is not a salaried employee of CIIS, but works in a capacity to support or further the development of the CIIS. Persons in this category may receive compensation through CIIS or another agency, but are not in the direct employment of CIIS as a salaried employee.

12.2 All third party employees will comply with the rules of conduct set forth in this policy, and will be held to the same legislation, laws and rules of confidentiality as employees of CIIS and its users.

12.3 All third party employees will be held to the same sanctions as employees of CIIS and its users should they violate the security policy¹⁷.

12.4 A third party employee's level of access to the CIIS will be determined by the same criteria defined in section 5.

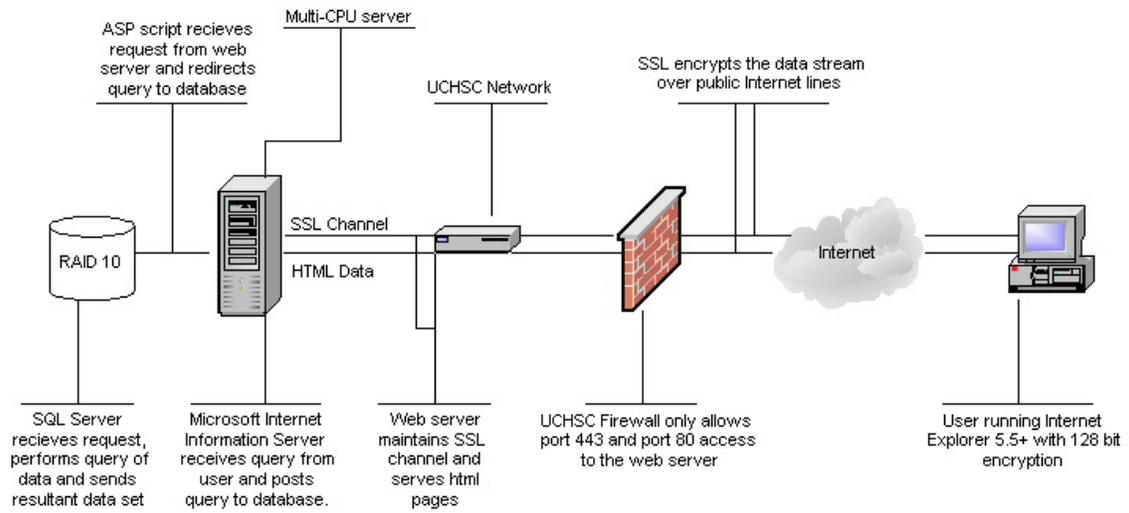
12.5 A third party employee's physical access to CIIS offices, computers (including peripherals), and data is determined based upon the employee's job description, need for information and CIIS and UCHSC access policies. The PA will use these criteria to determine the level of physical access to be granted.

12.6 All third party employees are required to use safe and secure methods that are in compliance with this security policy and the HIPAA security standard when using, transporting, or housing any data classified as PHI under the HIPAA security standard.

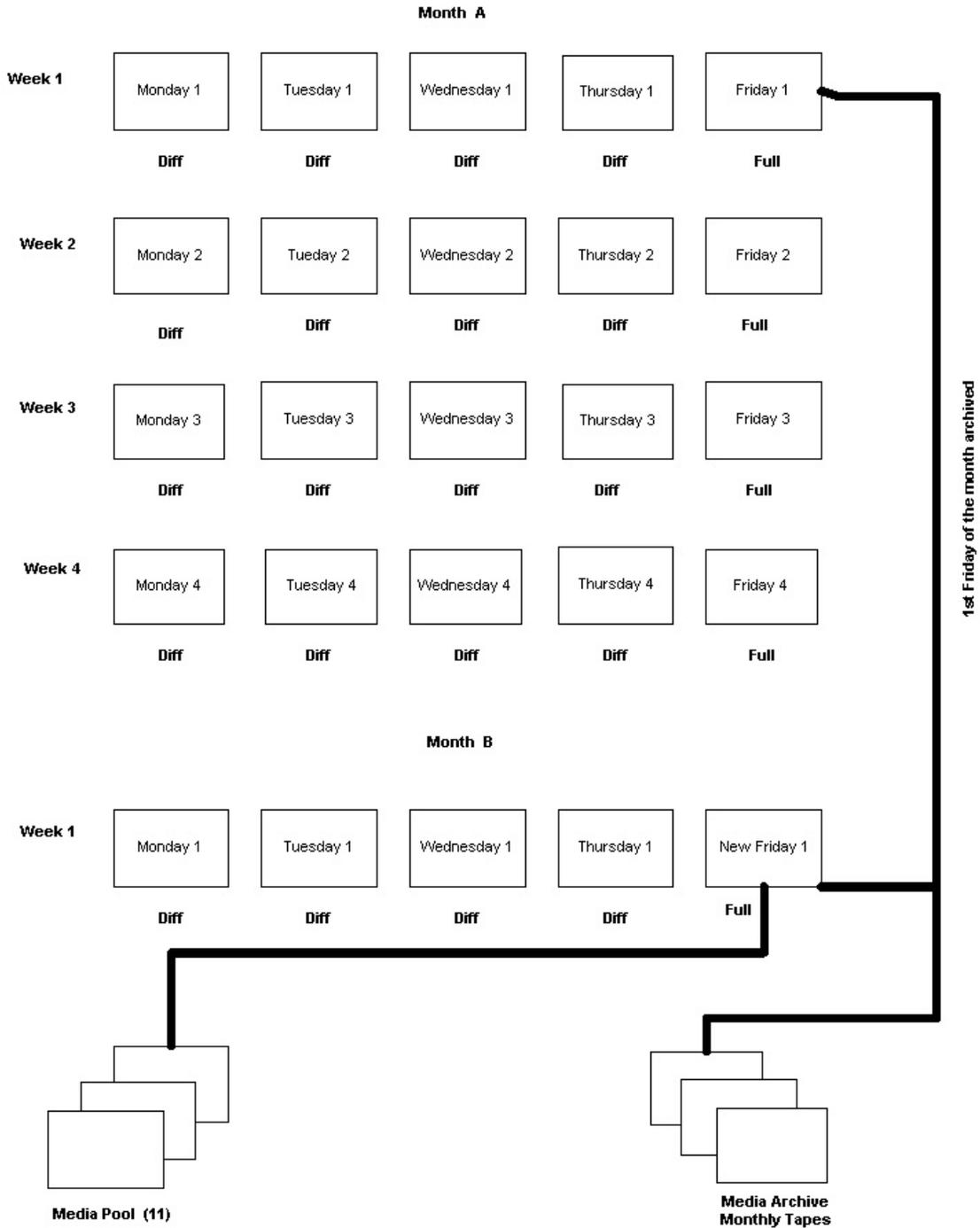
¹⁷ Refer to sections 2 and 5.1 for sanctions

- 13 Although every standard contained with this policy is accepted as best practice and therefore considered an acceptable level of securement, CIIS policy will be monitored and modified to include future standards, legislation, or laws, as they are deemed applicable. In assessing the need to modified the existing policy, due care will be given to the following areas:**
- 13.1 Communication protocol compliance**
 - 13.2 Hardware advances**
 - 13.3 Software releases**
 - 13.4 Current security best practice**
 - 13.5 Present legislation and law**
 - 13.6 Compliance with governing and regulatory agencies**
 - 13.7 Environmental changes**
 - 13.8 Employee and staffing issues**
 - 13.9 User input and reports**
 - 13.10 Log and event data**
 - 13.11 Demands on bandwidth**
 - 13.12 Performance issues**
 - 13.13 Administrative issues**
 - 13.14 Encryption advancement**

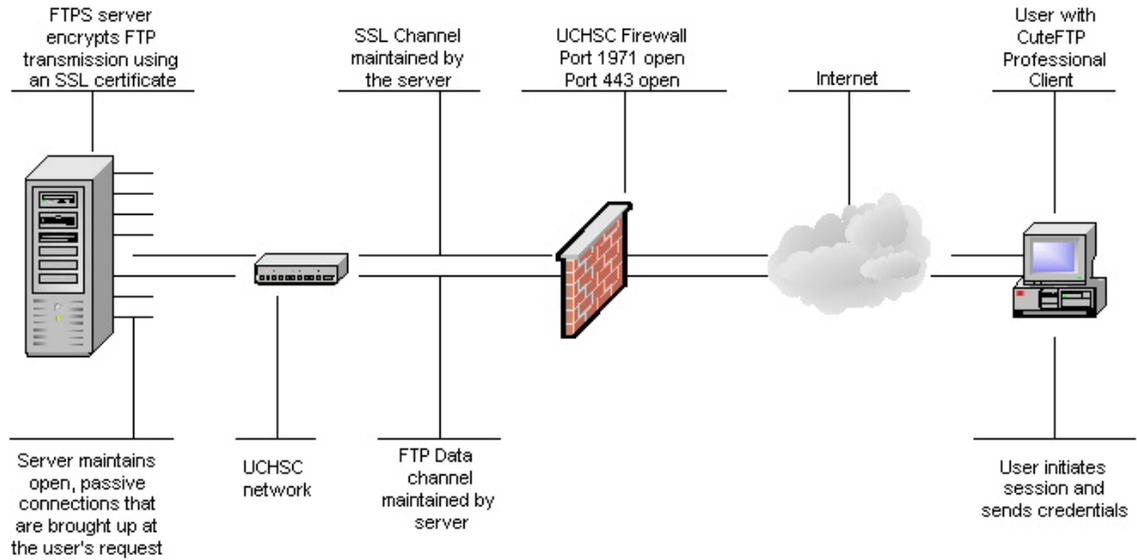
Appendix A – The Colorado Immunization Information System Session Diagram



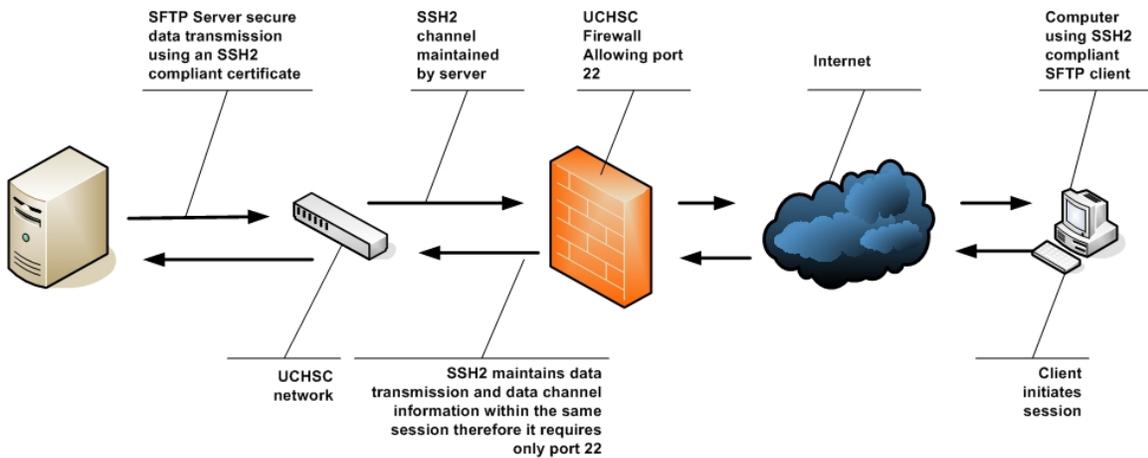
Appendix B – Colorado Immunization Information System Backup Methodology



Appendix C – The Colorado Immunization Information System SSL Session



Appendix D – The Colorado Immunization Information System SSH2 Session



Appendix E – The CIIS Secure Sockets Layer Session

