

University of Colorado at Denver and Health Sciences Center
HIPAA Policy

Policy:	9.2 Security Incidents	Latest Revision: 04/17/2005 Page: 1 of 9
---------	---------------------------	---

I. Purpose, Reference, and Responsibility

A. Purpose

The purpose of this policy is to define a security incident and to provide the procedures for notification, investigation, and reporting both during and after a security incident.

B. Reference

45 C.F.R. § 164.308(a)(6).

C. Responsibility

It is the responsibility of all staff, faculty, students, trainees, and volunteers to report any real or suspected security incident to the proper authority immediately. It is the responsibility of the individual who receives a suspected security incident report to follow the procedures outlined in this policy.

II. Applicability and Definitions

A. Applicability

This policy applies to all electronic data contained on any personal or University owned computer used by any employee, student, trainee, or volunteer of the University of Colorado at Denver and Health Sciences Center. Any data used for academic, administrative, research, or health care purposes is subject to this policy.

B. Definitions

Application
Information Systems Department (IS)
Log Analyzers
Operating System

University of Colorado at Denver and Health Sciences Center
HIPAA Policy

Policy:	9.2 Security Incidents	Latest Revision: 04/17/2005 Page: 2 of 9
---------	---------------------------	---

Protected Health Information (PHI)
Security Incident
Security Officer

III. Policy

A. Security Incident

A security incident is an attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

B. Response and Reporting

UCDHSC is required to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of known incidents; and document incidents and their outcomes. This includes improper network activity and misuse of outside data.

Security Incident Reporting and Response Procedures are outlined in a flowchart in Appendix A and detailed below.

1. **SUSPECTED INCIDENT OCCURS** -- Access may occur through a misuse of Information System ("IS") resources that results in a widespread intentional or unintentional compromise of information security. Large scale intrusions into a computing network may lead to unauthorized access to sensitive information. A lost or stolen laptop may result in a security incident involving sensitive data.
2. **INCIDENT DETECTED** -- Incidents may be detected through many different means, with varying levels of detail. Automated detection capabilities include network-based and host-based intrusion detection systems, antivirus software, and log analyzers. Incidents may also be detected through manual means, such as problems reported by users. Some incidents have overt signs that can be easily detected, others are almost impossible to detect without automation.

University of Colorado at Denver and Health Sciences Center
HIPAA Policy

Policy:	9.2	Latest Revision: 04/17/2005
	Security Incidents	Page: 3 of 9

If the incident is a life threatening activity or an activity on a critical system, it must be reported immediately. If the activity includes access to non-critical systems or unauthorized activity, it must be reported within two (2) hours.

3. DO NOT DISTURB -- the data or computer. The incident may require further investigation. It is important that nothing be disturbed at this step of the procedure.
4. REPORT -- Telephone 303-724-HELP to report the incident. The individual who receives the report must use the Security Incident Log template, Appendix B, to document the report.
5. MITIGATE – if possible, any harmful effects of the incident that are known. This may mean removing the affected device(s) from the network.
6. CATEGORIZE INCIDENT -- The individual who receives the report must categorize the incident as:
 - a. *Denial of Service*—an attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and/or disk space.
 - b. *Malicious Code*— refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the security or integrity of the victim's data. Malicious code is usually designed to perform these inappropriate functions without the user's knowledge. Viruses, worms, and Trojan horses are considered forms of malicious code.
 - c. *Unauthorized Access*—occurs when a person gains logical or physical access without permission to a network, system, application, data, or other resource. Unauthorized access is typically gained through the exploitation of operating system

University of Colorado at Denver and Health Sciences Center
HIPAA Policy

Policy:	9.2	Latest Revision: 04/17/2005
	Security Incidents	Page: 4 of 9

or application vulnerabilities, by getting hold of usernames and passwords, or social engineering.

- d. *Inappropriate Usage*—occurs when a legitimate user violates acceptable computing use policies. Examples of inappropriate use include sending spam promoting a personal business, sending email perceived as harassing individuals, etc. Inappropriate use issues may not constitute a security incident, but must be assessed by the Security Officer to determine if the inappropriate usage has created a security incident.
- e. *Multiple Component*—a single incident that encompasses two or more incidents or falls into multiple incident categories. These incidents should be handled in line with the severest infraction involved.

7. INVESTIGATE AND RESPOND TO INCIDENT – The Security Officer will work with IS and the impacted campus unit to investigate and respond to the incident and mitigate any harmful effects of the incident, if possible.

Or, if appropriate, the SECURITY OFFICER CONVENES INCIDENT RESPONSE TEAM – If the incident cannot be handled by the Security Officer and/or IS, the Security Officer will call an ad hoc meeting of appropriate individuals to make up an incident response team to investigate and respond to the incident. The ad-hoc group may be composed of the following members or their representatives, as determined by the Security Officer to appropriately respond to the incident:

- Assistant Vice Chancellor of Information Systems;
- Registrar (if student data);
- Assistant Vice Chancellor, Human Resources;
- UCDHSC Legal Counsel;
- Vice Chancellor of affected unit;
- Dean, Director, Chair, or Head of affected unit;
- Public Relations;

University of Colorado at Denver and Health Sciences Center
HIPAA Policy

Policy:	9.2 Security Incidents	Latest Revision: 04/17/2005 Page: 5 of 9
---------	---------------------------	---

- Police (UCDHSC or CU System);
- Appropriate IS personnel;
- UCDHSC Privacy Officer;
- LAN Administrator of affected unit;
- Others, as determined by Security Officer.

If the incident is of significant magnitude, the following members should be considered by the Security Officer for inclusion in the group:

- Internal Audit;
- CU-System Legal Counsel;
- CU-System Public Relations;
- CU-System Privacy Officer;
- Other CU Campus Information Technology or IS Offices;
- Risk Management.

8. DOCUMENT – the incident, investigation, response, and outcome. The Security Officer, IS, and/or the Response Team must document the security incident, investigation of the incident, and response and remediation. The Security Officer is responsible for retaining documentation of incidents.
9. CONCLUSION -- The Security Officer, IS and/or the Response Team should determine if policies or procedures need to be implemented to prevent a re-occurrence of the incident or if additional campus education or purchase of network or computing security devices are needed to prevent similar future incidents.

C. Documentation

Security incident procedure documentation and changes shall be retained for six (6) years.

UCDHSC SECURITY INCIDENT RESPONSE PROCEDURE

1

Suspected Incident Occurs

2

Suspected Incident is Detected

- Unauthorized access to sensitive information (e.g. SS#, Cr Card #, PHI)
- Suspected misuse of IS resources resulting in compromise of information security
- Large scale intrusion

3

DO NOT DISTURB
Data or Computer

4

REPORT
303-724-HELP or HIPAA@UCHSC.EDU

5

If possible
Stop Escalation of Attack

6

CSIRT or Security Officer:
Categorize the Incident

- Denial of Service
- Malicious Code
- Unauthorized Access
- Inappropriate Usage
- Multiple Component

7

Investigate or CSIRT Group Convenes:

- Assistant Vice Chancellor, Information Systems
- Selected Information Systems Department Technical Personnel and as appropriate:
- Registrar (if student data involved)
- Assistant Vice Chancellor, Human Resources (if employee or employee data involved)
- UCDHSC Legal Counsel
- Vice Chancellor of affected area
- Dean or Director of affected area
- Public Relations
- Police (UCDHSC or CU-System)

Escalate to CU-System

- Internal Audit
- CU-System Legal Counsel
- CU-System Chief Privacy Officer
- Other CU campus IT Offices
- Risk Management

8

Check List:

- Document all steps as they are taken
- Who is identified as the lead for coordinating the investigation?
- What happened? What critical systems or data may be involved?
- Is the incident over?
- Is the incident likely to result in criminal or civil legal action?
- Preserve evidence and halt/isolate the incident as appropriate
- What is the risk? Who will be impacted? (Dept/Unit→Campus→University)

9

Investigation:

- Document all steps as they are taken
- Gather evidence (audit trails, logs, etc.)
- Analyze the evidence
- Determine the scope of the damage
- Restore system to operation, if appropriate

10

Conclusion:

- Document all steps as they are taken
- Communicate back to the CSIRT
- Notify individuals affected by the incident
- Determine ways to prevent a re-occurrence
- Evaluate incident Response Procedure and modify, if necessary

University of Colorado at Denver and Health Sciences Center
HIPAA Policy

Policy: 9.2
Security Incidents

Latest Revision: 04/17/2005
Page: 7 of 9

APPENDIX B

Security Incident Log

Date and Time Reported: _____

Reported to (name of person receiving report): _____

Date and Time of Incident: _____

Category of Incident: _____

Contact information for system owner—

Name: _____

Unit/Dept/College/School: _____

Location: _____

Phone Numbers: _____

Device serial number and model number: _____

Computer name: _____

MAC address: _____

IP address: _____

Witnesses/other parties of interest: _____

Who will take the lead in coordinating the investigation? _____

Members of investigating team: _____

University of Colorado at Denver and Health Sciences Center
HIPAA Policy

Policy: 9.2
Security Incidents

Latest Revision: 04/17/2005
Page: 8 of 9

Summary of Incident (attach sheet if necessary):

Is there sensitive data involved and explain: _____

Is the incident over? Yes No

If the incident is likely to result in criminal or civil legal action,

Preserve the evidence and halt/isolate the incident as appropriate.

What is the risk? Who will be impacted (dept/unit, campus, University)? _____

Outline the steps to be taken: _____

University of Colorado at Denver and Health Sciences Center
HIPAA Policy

Policy: 9.2
Security Incidents

Latest Revision: 04/17/2005
Page: 9 of 9

Security Incident Log—page 3

At conclusion of the investigation, were the individuals affected by the incident notified?
 Yes No (If yes, attach a copy of that correspondence.)

Has a final report of the incident, investigation, response, and remediation been written?
 Yes No (Attach a copy of the report.)