



## Digital Storage Search And Seizure

<b>Title: Digital Storage Search And Seizure</b>		<b>Applicable Policy: HSC-200 Security and Mgmt of HSC IT Resources</b>
<b>Doc Type: Procedure</b>	<b>Procedure #: HSC-200 SOP.1</b>	<b>Effective Date:</b>
<b>Process Owner (Name and Title): HSC CIO</b>	<b>Revision Date:</b>	<b>Applies To: HSC Workforce</b>

### PURPOSE/DESCRIPTION/OVERVIEW

A search and seizure of computers, hard drives, and other digital storage devices may only be executed by the Executive Vice Chancellor or his/her designee if, in assessing the circumstances presented and exercising practical judgment and common sense, he/she decides that there is a fair probability that evidence might be destroyed or is being used in an unauthorized manner.

An Emergency Situation Exception may be applied to searches that must be conducted immediately, and may be used in situations where any delay would result in the destruction or removal of evidence.

### PROCEDURE

Each search and seizure action is to be carried out in alignment with the principle and standards defined below. A written report will be produced by the lead investigator detailing how the actions taken align to these principles and standards. Any conclusions in the final report must be based on evidence gathered in alignment with the principles and standards outline below.

### Notification of Seizure

Except where the owner or consignee is personally notified or seizure is made pursuant to a search warrant, the HSC shall, as soon as practicable following the seizure or other receipt of seized property, provide notification of seizure through a verifiable process, to the owner or consignee, if known or easily ascertainable. Such notification shall describe the seized property, and shall state the time, place, and reason for the seizure.

### Seizure Principles:

1. When dealing with digital evidence, all general forensic and procedural principles must be applied.
2. Upon seizing digital evidence, actions taken should not change or modify the evidence.
3. When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.
4. All activities relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.
5. An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.
6. Any individual or agency which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

### General Evidence Dos & Don'ts

1. Minimize Handling/Corruption of Original Data
2. Account for Any Changes and Keep Detailed Logs of Actions
3. Comply with the Five Rules of Evidence (Admissible, Authentic, Complete, Reliable, Believable)



4. Do Not Exceed Your Knowledge
5. Follow Local Security Policy and Obtain Written Permission
6. Capture as Accurate an Image of the System as Possible
7. Be Prepared to Testify
8. Ensure Your Actions are Repeatable
9. Work Quickly
10. Proceed from Volatile to Persistent Evidence
11. Do Not Run Any Programs on the Affected System
12. Ensure that Complete and Accurate Documentation is of the Highest Priority

#### **Electronic Evidence May Include the Following:**

- System (computers and peripherals functioning together)
- Stand-alone computers
- Laptops
- Cell phones
- Media
- Hard drives
- Diskettes
- USB Storage devices
- Memory cards
- Other similar devices

#### **Step 1: Preparing for the Search & Seizure**

- Ensure that all written authorizations are in order
- Responders should determine:
  - The type of case (e.g., misconduct, ePHI safety, child porn, IP theft, etc.)
  - The type of computer(s) involved;
  - The operating system(s) used; and
  - The level of technical savvy of the end user.
- A Primary Evidence (PE) person should be appointed. The PE is responsible for preparing a detailed plan for documenting, preserving, and maintaining the integrity of all seized evidence (digital and paper).

#### **Step 2: Securing and Evaluating the Scene**

- Control the scene
  - Limit access to only authorized persons
  - Record the names of all individuals present during the search
  - Obtain signatures from department and/or police representative
- Confirm when the system was last accessed
- Establish a chronology of access to the media
- Photograph or video tape the entire scene including the contents on the monitor

#### **Step 3: Securing the System**

- If the system is "On" do not perform a controlled shut down. Pull the power cable! (Unless a memory dump is required, i.e., encryption keys need to be retrieved.)
- If the computer is "Off" do not turn it on.



- Disconnect all remote access to the system (e.g., Network cables, USB cables, etc.). Tag and label all cables and connectors.
- Physically examine the system (i.e., remove covers and photograph).
- Document models and serial numbers of the system and its components.
- Inventory all peripherals (e.g., USB devices, printers, scanners, WAPs, fax machines, etc.).
- Search scene for secondary storage media (USB drives, devices, diskettes, tapes, etc.)
- Make detailed notes and complete the attached Chain of Custody form.

#### Step 4: Processing

In compliance with the principle and standards above the HSC will use forensic equipment to document the steps above and the details of the analysis used in the course of gathering evidence. To aid in these efforts the HSC maintains forensic equipment that is capable of the following:

Generate forensic results that are court-cited for a digital investigations platform. Quick, stable and with ease of use features. Performs comprehensive processing and indexing of all data (in allocated and slack space) stored on the target media. Built-in methods to review data and identify relevant evidence (visualization and explicit image detection technology may be included) to quickly discern and report the most relevant material to the investigation. Correlation of data sets from different sources, such as, computer hard-drives, mobile devices, network data, internet storage, etc. is possible if needed. (As of Jan. 2015 the AccessData FTK Ver. 5.6 is in use)

\*Note: Other technical and non-technical methods may be used to gather evidence if authorized by the lead investigator.

Search and seizure actions are to be carried out by authorized UNMHSC/UNMH staff acting on written authorization and working in accordance with the forensic principles defined above. The determination of what data is relevant, what devices will be searched and what will be reported rests with the authorized investigator assigned to the case.

Forensic equipment maintained by the HSC Information Security Office (or other professionally contracted equipment) may be used to manage and process search and seizure actions. These actions may include, but are not limited to, forensic copies, advanced searching, secure storage of devices, and management of any advanced or third party analysis. The HSC procedures for use of the HSC ISO forensic equipment are to be carried out and overseen by the HSC ISO, unless an otherwise authorized and approved authority intervenes.

#### DEFINITIONS

**Emergency Situation Exception:** A person who possesses common authority or has frequent access over the premises; e.g., co-worker, janitor, etc. can authorize a consent to search within limits (NOT the whole office or any computers). Many departments require signing a consent form. Silence, simple nodding of the head, or waving through an open door is NOT consent. Agents should be especially careful about relying on consent as the basis for a search of a computer when they obtain consent for one reason but then wish to conduct a search for another reason.

**SEIZURE:** By definition is the deprivation of enjoyment to exercise dominion or control over a thing. Management may temporarily seize university property and hold it indefinitely if it is material to an ongoing investigation.



**REFERENCES**

HHS, IRB, HRR, HIPAA

**AREAS OF RESPONSIBILITY**

Executive Vice Chancellor: Authorization  
 HSC Chief Information Officer: Procedures  
 HSC Information Security Officer: Security Oversight

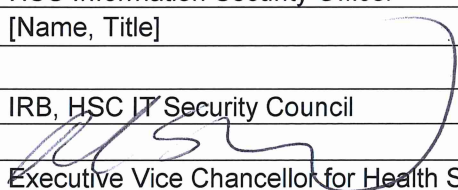
**RESOURCES AND TRAINING**

Resource/Department	Contact Information
HSC Information Security Office	<a href="mailto:HSC-ISO@salud.unm.edu">HSC-ISO@salud.unm.edu</a> 272-1696

**SUMMARY OF CHANGES**

New Procedure

**DOCUMENT APPROVAL & TRACKING**

Item	Contact	Date	Approval
<b>Owner</b>	HSC Chief Information Security Officer HSC Information Security Officer		
<b>Consultant(s)</b>	[Name, Title]		
<b>Recommender(s)</b>			[Y or N/A]
<b>Committee(s)</b>	IRB, HSC IT Security Council		[Y or N/A]
<b>HSC Legal Office</b>			[Y or N/A]
<b>Official Approver</b>	Executive Vice Chancellor for Health Sciences Center		Yes
<b>Official Approver Signature</b>		Date: 3/2/2015	
<b>2nd Approver</b>			
<b>2nd Approver Signature (Optional)</b>		Date:	
<b>Policy Origination Date:</b>			

**ATTACHMENTS**

Appendix A: Chain of Custody Form Attached Below

**Item Number(s):** \_\_\_\_\_  
**Case:** \_\_\_\_\_

**To be completed by initial collector:**

Evidence collected by (name): \_\_\_\_\_  
 Date/Time collected: \_\_\_\_\_  
 Evidence description:  
 \_\_\_\_\_  
 \_\_\_\_\_

Describe Collection method (include operating system, utility, commands, arguments, etc):  
 \_\_\_\_\_  
 \_\_\_\_\_

What application software/utility is required to view the file?:  
 \_\_\_\_\_  
 \_\_\_\_\_

Where is evidence initially stored?: \_\_\_\_\_  
 How is evidence initially secured?: \_\_\_\_\_  
 Collector signature: \_\_\_\_\_ Date: \_\_\_\_\_

**Copy History:**

Date	Copied By	Copy Method	Disposition of original and all copies

**Transfer History:**

Transferred from (print name, sign & date): \_\_\_\_\_  
 Transferred to (print name, sign & date): \_\_\_\_\_  
 Where is evidence now stored?: \_\_\_\_\_  
 How is evidence now secured?: \_\_\_\_\_

Transferred from (print name, sign & date): \_\_\_\_\_  
 Transferred to (print name, sign & date): \_\_\_\_\_  
 Where is evidence now stored?: \_\_\_\_\_  
 How is evidence now secured?: \_\_\_\_\_

Transferred from (print name, sign & date): \_\_\_\_\_  
 Transferred to (print name, sign & date): \_\_\_\_\_  
 Where is evidence now stored?: \_\_\_\_\_  
 How is evidence now secured?: \_\_\_\_\_

Transferred from (print name, sign & date): \_\_\_\_\_  
 Transferred to (print name, sign & date): \_\_\_\_\_  
 Where is evidence now stored?: \_\_\_\_\_  
 How is evidence now secured?: \_\_\_\_\_

Transferred from (print name, sign & date): \_\_\_\_\_  
 Transferred to (print name, sign & date): \_\_\_\_\_  
 Where is evidence now stored?: \_\_\_\_\_  
 How is evidence now secured?: \_\_\_\_\_