Policy Summary: Information System Resource and Data Owners must document the receipt, transfer and removal of electronic media which contain Sensitive Data.

Purpose: This policy reflects our commitment to identify and implement security controls which will keep risks to information system resources at reasonable and appropriate levels.

Policy: Sensitive Data located on information system resources or electronic media must be protected against theft and unauthorized access. Sensitive Data must be consistently protected and managed through its life cycle, from origination to destruction.

Information system resources and electronic media for which this policy applies include, but are not limited to, computers (servers, desktops and portable computing devices (PCD)), floppy disks, backup tapes, CDROMs, zip drives, portable hard drives and USB storage devices with stored sensitive data.

All electronic media that contains Sensitive Data must be clearly marked during transport and must have a tracking number associated with it.

There must be a formal, documented process that ensures consistent control of all electronic media and information system resources containing Sensitive Data while it is in transport. At a minimum this process must ensure the following:

1. Sensitive Data in transport is encrypted when warranted/feasible
2. An exact copy of Sensitive Data is maintained in case of loss or damage
3. A complete Record of Transport including:
   A. What was transported
   B. When it was transported and where was its final destination
   C. Why it was transported
   D. Who handled it during transport
   E. When it arrived at its final destination
   F. Condition upon arrival
   G. Frequency of transport (For PCDs only)

For PCDs in which the transportation of Sensitive Data will be a regular or cyclical (more than twice per year) occurrence, a single transport record will meet the above requirement for “record of transport” for each occurrence. Each time one of the parameters within the “record of transport” changes, a new record is required.

At least annually, a University-wide inventory to identify all electronic media that contain Sensitive Data must be performed. Inventory results must be documented and stored in a secure manner.

Documentation: All data collected and/or used as part of the Risk Management Process and related procedures will be formally documented and securely maintained.

Scope/Applicability: This policy is applicable to all OUHSC workforce members.
| **Regulatory Reference:** | HIPAA 45 CFR 164.308(a)(1)(ii)(B)  
16 CFR Part 314 Standards for Safeguarding Customer Information  
[section 501(b) of the Gramm-Leach-Bliley Act ("G–L–B Act")  
Payment Card Industry Data Security Standard (PCI DSS) |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definitions:</strong></td>
<td>See the Information Security Policy Definitions document for definitions</td>
</tr>
<tr>
<td><strong>Responsible Department:</strong></td>
<td>This policy is applicable to all faculty, staff, students, volunteers, and business associates of OUHSC and OU Health Care Components.</td>
</tr>
<tr>
<td><strong>Enforcement/Audit:</strong></td>
<td>The university’s Internal Auditing department is responsible for monitoring and enforcement of this policy.</td>
</tr>
<tr>
<td><strong>Renewal/Review:</strong></td>
<td>This policy is to be reviewed and updated as needed by IT Information Security Services.</td>
</tr>
</tbody>
</table>