Do you know where your confidential paper documents are? The hackers and thieves sure do.

**What is Data Dumpster Diving?**

Data dumpster diving is a common tactic used by hackers and thieves in which they sift through the trash of others in hopes of discovering confidential personal and corporate information. This tactic is often the first used in a serious intrusion because going through the trash is a simple process compared to penetrating a firewall, deploying Trojans, stealing passwords, etc... to get the same information. Hackers know that people are the weakest link in the security chain and it only takes one person to improperly and illegally dump sensitive documents in the trash to hand over a gold mine of information.

**Examples of information that hackers and thieves look for:**

- Names, Addresses, Credit Card Numbers, Social Security Numbers
- Patient information
- Student record information
- Printouts of calendar information (tells them when everyone will be elsewhere, not logged into systems) to determine the best time to break in.
- Printouts of computer source code, e-mails, memos, notes containing passwords and account names.

**What are the proper procedures for paper document disposal?**

- Shred all sensitive data prior to disposal or place it in a Shred-it bin. If you take documents home with you, you must shred them in a cross cut shredder or bring them back to work to shred or place in a Shred-it bin.
- Protect printed sensitive data. Store sensitive data in a locked desk or cabinet and keep it only as long as required by regulation or company policy.
- Don’t leave unattended sensitive data on the copier, fax or printer.

Anything you do not want on the front page of the newspaper, or in the hands of strangers, should be shredded or placed in a Shred-it bin rather than placing it in the trash.

**What are the penalties for non-compliance?**
Violations may constitute grounds for corrective action up to and including termination of employment or student status, loss of UNC Health Care and UNC School of Medicine privileges or contractual or affiliation rights in accordance with applicable UNC Health Care procedures. Unauthorized use or release of confidential information may also subject the violator to personal, civil, and/or criminal liability and legal penalties.

Please review these UNC Health Care System policy documents for additional information:

**Confidentiality Statement:**
http://intranet.unchealthcare.org/intranet/hospitaldepartments/auditcomplianceprivacy/privacy/forms

**Information Security Policy:**
http://intranet.unchealthcare.org/intranet/hospitaldepartments/auditcomplianceprivacy/privacy/information-security