FACULTY SENSITIVE DATA CLEANUP

Last year, the University of Arizona notified nearly 10,500 students and former students that they may be a target of identity theft. The notifications were in response to a likely exposure of student social security numbers, which were used as student IDs. One of our primary risk factors has been historical class rosters on faculty computer systems that are stolen or compromised. An additional 9,800 research records containing personally identifiable data on research study participants were exposed.

This checklist is designed to assist faculty members in proactively locating files that contain personal student data and to ameliorate the risk associated with these files. Aside from identity theft, security breaches often bring negative press to the department and institution. In a time of growing compliance standards for research activities, we risk questions from granting agencies and serious consequences to the perception of UA's ability to safeguard data. The University of Hawaii is an example of breach impact: http://www.khon2.com/news/local/story/UH-Security-Breach-Impacts-More-Than-40-000/DGdfJhopHkmPRHP9h6sKQA.cspx

PLEASE TAKE A FEW MINUTES TO CHECK ON YOUR RISK:

- ☐ Did you teach classes in 2008 or prior years AND did you keep an electronic class roster on your computer with student names and grades? If so, it is very likely that the rosters are in Excel files, contain student names and IDs and that the IDs contain social security numbers. UA was in the process of remediating SSNs, but had not completed all students.
    - ☐ Look in directories/folders of classes that you teach for semesters/years in 2008 or earlier and for Excel or other files storing class roster data
- ☐ Do you conduct research that involves details about individuals AND does the data include demographic data including SSN, Driver's license, family names, addresses, phone numbers, etc.? You may need to check your data repositories to be sure about some of these elements. Often research involves a specific situation that may cause embarrassment to study participants.
    - ☐ Look for research data containing personal information about student participants or research under compliance regulations from national agencies (these data should be encrypted).

REMEDIATION OPTIONS:

1. Deleting the file is the best course of action if enough time has passed that the final grade on record is all you would need for any inquiry.
2. Alternatively, delete all student IDs and resave the file.
3. Encrypt the data if you feel you must keep it. Sophos Safeguard Encryption has been purchased for the university. Please contact your IT support, your Information Security Liaison or the Information Security Office at 621-8476 for more information.

Follow these procedures for an office desktop, backup drives, office laptop, USB drives and home computers. The data has often traveled between these devices and each has been the source of a security incident this past year.