Legal Issues in Managing Computing and Electronic Resources

Nancy E. Tribbensee
Deputy General Counsel
Arizona State University
What do these claims have in common?

- Violation of federal and state privacy laws
- Negligence
- Gross negligence
- Breach of contract
- Violation of U.S. Constitution
To all TRICARE stakeholders:

I regret to announce that one of TriWest Healthcare Alliance's offices in Phoenix was broken into and computer equipment and data files containing personal information about our TRICARE beneficiaries were stolen. Since the motives for the crime are unknown at this time, it is important that you are aware that there is the possibility that the information may be misused, exposing beneficiaries to the potential of identity theft. I apologize to you for any inconvenience that this incident may cause you or your family members. Be assured that TriWest is working around the clock, in cooperation with the leadership of the DoD, to inform beneficiaries and help them take the proper precautions to safeguard against any potential fraudulent activity or misuse of their stolen information.

In addition to letters being sent to affected beneficiaries and providers, TriWest will be placing regular updates about this situation onto this section of the Central Region web site as developments occur. I encourage you to visit frequently in order to stay informed.

Rest assured that we are doing everything possible, in concert with Federal authorities, to prevent this type of break-in from occurring again at any of our facilities. As always, I would appreciate any suggestions you may have to help improve our processes as we strive to better serve the members of our nation's military and their families in the TRICARE Central Region.

Sincerely,

David J. McIntyre, Jr.
President and CEO
TriWest Healthcare Alliance
Stollenwerk v. TriWest Healthcare Alliance

- Class action lawsuit
- Approximately 562,000 plaintiffs
- Electronic records stolen from medical insurance provider for U.S. Military
Stolen records included:

- Name
- Address
- Duty station (for active military)
- Birth dates
- Social Security Numbers
- Medical claim information
- Consumer credit information
Lawsuit is seeking:

• General damages
• Special damages
• Punitive damages
• Injunctive relief
• Attorney’s fees
• Costs and interest
• Any other relief the court deems just and proper
Identity Theft

• Lost and stolen records

• Review what information is collected, how it is stored, how it is backed-up

• Adopt policy and procedures for lost and stolen records
Policy elements:

- Identify who should be contacted (e.g., police, registrar, personnel office, university attorney)

- Provide for notice to persons whose records were lost or stolen
Notice should include:

• FTC website on identity theft

www.consumer.gov/idtheft
Identity Theft Alert: TriWest HealthCare Alliance

Computer equipment and data files containing personal information about some TRICARE beneficiaries were stolen on Dec. 14, 2002, from TriWest Healthcare Alliance Corp. in Phoenix, Arizona. For more information on this incident, visit www.triwest.com/announcement.

If TriWest HealthCare Alliance has told you that you are among the group whose information was taken, contact each of the three major credit bureaus to place a fraud alert on your credit file and get your credit report. These reports are free to victims of fraud. The fraud alert will let creditors know to contact you before they open any new accounts in your name or make any changes to your existing accounts. Once you receive your reports, check them for errors and submit any necessary corrections.
Notice should also include:

- **Social Security Admin. fraud line:**
  - 1-800-269-0271

- **Credit Bureau Numbers**
  - Equifax 1-800-525-6285
  - Experian 1-888-397-3742
  - Trans Union 1-800-680-7289
General Security Issues

• Periodic campus security and liability audits should include electronic resources

• Others are constantly evaluating your security, you should be too.
Authorized access

• Who is authorized to use the system and for what purpose?

• How do you limit access of users upon separation from institution or misuse of system?

• How is the system protected against unauthorized access?
Identification of user (or station)

• Do campus systems allow for anonymous use (e.g., libraries)?

• For stations used by many users, are steps taken to remove information “left behind” by normal use?
Centralized or distributed systems?

For systems that are beyond central control:

- Who has access?
- Who is responsible?
- Who is monitoring?
- Who is coordinating with central administration?
- Do these folks even know about institutional policies?
Supervision of system administrators

• Student workers as systems administrators

• Who is supervising and at what level?
Which agency is in the best position to help?

- FBI
- State attorney general
- County attorney
- Campus police
- Student conduct office
Law enforcement: requests for information

- Consult counsel and institutional policies
- May preserve information while you consult
- Do not use e-mail to discuss possible electronic crimes
And finally,

- Security decisions, both electronic and non-electronic, need to be made in the context of the institutions primary missions.