A technical reference bulletin by the Risk Control Services Department of the Glatfelter Insurance Group

Glatfelter Healthcare Practice℠
A Division of Glatfelter Insurance Group

RISK COMMUNIQUÉ

Laptop Security

Laptop computer theft is an increasing risk exposure for healthcare organizations and represents more than just a property loss. Not only do you lose expensive technology, but you have a significant potential for lost data, including confidential patient information. The theft of a $1500 laptop can mean the loss of much more in terms of sensitive information.

Just ask Providence Health System located in Portland, OR. Computer back-up disks and tapes were stolen from an employee's car in late December 2005. These disks and tapes included the records of about 365,000 current and former patients. Due to the public outcry and the damage to their reputation, Providence Health System ended up paying for data protection services for all 365,000 patients.

According to the FBI, in the year 2000 there were 418,000 laptops and PCs lost or stolen in the USA. Insurance statistics show that if you own a laptop you have a 1 in 14 chance it will be stolen. This works out to about one computer theft every 53 seconds.

Laptops or tablet personal computers (PCs) are popular business tools and are used more and more in the hospice and home care industry. The technology makes information retrieval and data entry much easier, but their use also creates significant security concerns for personal and health-related information. Their use has become so common, in fact, that many people see a laptop as just another "device." As a result people have become careless. Almost every week there is another story of a stolen laptop that makes headlines. Our goal as healthcare providers should be to assure that our employees protect their assigned laptop—and the confidential information it contains—from theft.

Tips for preventing laptop theft

- Store shipments of new or unassigned laptops and computers in locked closets or rooms with controlled access. Make sure you have a complete inventory of all computer equipment from the time of delivery. Conduct regularly scheduled and random inventory checks.
- Engrave the company name/ID on all laptops. Record the laptop's identification number and keep it in a safe place. Check to see whether the laptop manufacturer or your local police department offers an asset identification or registry program.
- Provide employees with an inconspicuous storage case. Flashy laptop cases can attract thieves' attention. A simple weatherproof, padded carrying case will suffice as a protective container.
- Protect information stored on the laptops by utilizing document passwords. A strong password should appear to be a random string of characters. Passwords should be 8 or more characters in length and should combine letters, numbers and symbols.
- Advanced security measures are being provided with newer laptop systems. The use of data encryption is available along with biometric security chips.
- When leaving a laptop in the office, make sure it is hidden and secured.

- Remind employees not to place their laptops near an exterior window or so that it is visible on a car seat, which might encourage a "smash and grab" theft. If you must leave a laptop in the car, lock it in the trunk or safeguard it out of sight.
- Be sure that all important data contained on the laptop is backed up on a regular basis.
- When using a laptop for meetings or conferences, always keep it in sight. Do not leave the room without taking the laptop with you.
- Develop written policies and procedures regarding employee accountability for the safety and security of laptops assigned to them. Require a signed statement from all laptop users that they have reviewed this policy and understand it.
- Maintain a current list of all laptop users, assigned equipment, serial numbers and software. Audit the list annually.
- Investigate all incidents of theft or damage. Report all thefts to the police. Publicize incidents and information as required by law.

Summary

It is important that healthcare providers make a concerted effort to educate their employees about computer security in order to control the expenses and reputation damage associated with such a loss. In addition to including this information in new employee orientation, there should be annual updates and periodic reminders to maintain safety and security awareness.