Smart Phones, Tablets and Portable Memory Devices: Can You Afford the Liability of An Employee's Loss of a Device

BY Ron Stadler, Partner, Gonzalez Saggio & Harlan, S.C.

The biggest threat to your information technology is not an outside hacker -- it's an employee's forgetfulness. As technology becomes smaller and more portable, it becomes easier to lose, and lost devices have become a significant issue because most employers are not protecting the data on mobile devices. Accordingly, when the device is lost, the data on it can be accessed or it could be used to access your other systems. Just think of the implications:

- Counties and school districts often deal with medical information relating to employees, students, or service recipients. This can create HIPAA violations which are costly. The maximum civil penalty for a HIPAA-related data breach is $1.5 million.
- County employees also deal with programs for the well-being, treatment, and care of the mentally ill, developmentally disabled, alcoholic, and other drug dependent citizens. Under Wisconsin law disclosure of these records can result in liability for actual damages, exemplary damages of up to $1,000 for each violation and the awarding of reasonable attorney fees.
- Wisconsin recognizes the tort of the invasion of privacy the disclosure of private acts if the disclosure would be highly offensive to a reasonable person where the party disclosing the facts acted either unreasonably or recklessly. *Olson v. Red Cedar Clinic, 2004 WI App 102*. Courts outside of Wisconsin have recognized that data disclosure can be viewed as an invasion of privacy. *Rowe v. United Life and Health Ins. Co., 2010 WL 86391 (N.D. Ill.)*
- Information about employees or those you serve may constitute "consumer reports" within the meaning of the Fair Credit Reporting Act, and disclosure of that information could create liability for damages and attorney fees.

So how do you protect yourself from liability for accidental loss of a device containing sensitive data? The best way is to make sure that the device contains as little information as possible and that all devices have security that make it difficult to access by anyone who happens to find it.

A policy requiring password protection is important to preventing unwanted access. This should also be coupled with encryption. An encryption program allows one to not only encrypt email messages, but personal files and folders as well, even an entire volume or drive.

It is also highly recommended that a policy be implemented that requires software packages or applications that can be downloaded onto smartphones and tablets that allow users, in the event the device is lost or stolen, to automatically erase everything from the device or locate the device.

Best Practice Tips:
Seven Ways to Avoid Liability

1 Plan Ahead

Once a mobile device is lost or stolen it is too late. Don't wait for the lawsuit or confidential information loss to start managing your data.

2 Know What is Legally Required

For instance, what are the data retention obligations for particular information that you deal with? What safeguards, if any, exist for restricting access or retention?

3 Assign Responsibility to Manage the IT System

Appoint personnel responsible for maintaining and managing electronic data. This might be a collection of people from legal and IT, with input from HR or other departments. Get the people involved early who will need to make the system work when legal demands arise.

GONZALEZ SAGGIO HARLAN

About Gonzalez Saggio & Harlan

Gonzalez Saggio & Harlan, a national minority-owned law firm, was established in 1989. The firm's attorneys have extensive experience in a wide variety of areas and handle matters relating to governmental entities such as: education law; equal opportunities and employment law; government relations; public finance; energy, communications, and utilities.

The firm has fifteen nationwide offices and is based out of Milwaukee, Wisconsin.

County Mutual
Wisconsin County Mutual Insurance Corporation

About the County Mutual:

The Wisconsin County Mutual Insurance Corporation is dedicated to serving Wisconsin counties and local governments and the people they serve by providing long-term stability in insurance coverage, while controlling these costs.

What makes the County Mutual unique is our close working relationships with our member counties. Acting in collaboration, the County Mutual and county owners work as a team to aggressively control their claims costs by promoting quality risk management efforts that are second-to-none in the industry.

What started as a handful of counties joining forces in the midst of an insurance crisis in 1988 has grown to close to 75% of Wisconsin's counties being insured by the County Mutual today.

Working together, we truly are a **Mutual Effort**.

Smart Phones, Tablets and Portable Memory Devices: Can You Afford the Liability of An Employee's Loss of a Device, continued

BY Ron Stadler, Partner, Gonzalez Saggio & Harlan, S.C.

4 Locate the Various Forms and Keepers of Data

Remember that data can be stored within the physical memory of a laptop, tablet, or smartphone or may also be stored on external media such as a thumb drive. Before you can manage data for which the law may hold you accountable, you must first identify what and where the data is to ensure that the system you adopt will in fact capture the relevant data.

5 Select a Flexible Electronic Data Management System

Select a system that is flexible enough to address your particular retention, archiving, monitoring, filtering, and encryption needs. Pick a system that is "user friendly" so that employees do not take steps to circumvent it.

6 Adopt Policies

Adopt clear and simple policies consistent with applicable laws addressing such things as document retention. Adopt a well publicized employee electronic monitoring policy. Adopt encryption policies for confidential information to avoid inadvertent disclosures. Adopt disciplinary procedures to impress upon your workforce that you mean what you say.

7 Train and Audit and Then Training and Audit Some More

Policies and data management systems only work if employees know how to use them. It requires conscientious and consistent implementation and maintenance. Purchasing a data management system is only your first step to compliance. New data, new technology, new laws, new threats, and new employees all require diligent maintenance and ongoing training and audit.