NEWSLETTER

Policing Your Own People

July 2013

The recent reports of terminations at Cedars-Sinai Medical Center following inappropriate review of celebrity medical records should serve as a reminder to every health care entity—and any company with sensitive information. You must police your own people. They need access to information to do their own job, but history has shown that they can't be trusted entirely. You need a plan to make sure that your own people aren't the cause of privacy and security breaches.

These breaches fall into three categories. There is the "celebrity" problem, which is particularly visible in the health care industry but could certainly apply in other areas—think back to one of the original privacy laws, the Video Privacy Protection Act, where video rental company employees disclosed records involving a U.S. Supreme Court nominee. Then there's the "I want to see how Aunt Sally is doing in the hospital" problem. These are more personal—and can be relatively innocuous—as with Aunt Sally, or more malicious, when it's not Aunt Sally but an ex-girlfriend or former boss—but are still illegal and inappropriate. Last is the most malicious category—where this internal access leads to identity theft, health care fraud, sale of information to tabloids, etc. Each of these categories has its own set of issues and potential solutions.

What Do You Need to Do About This?

Recognize That This Can (and Likely Will) Happen to You

This issue of internal access being misused can happen to any company in any setting. It's most visible in the health care industry, but the core problem arises when individuals need access to information about lots of people to do their job. Do you have customer service employees? Check-in personnel? Cashiers? That's pretty much everyone. Most companies have individuals who need access to lots of information to do their job—at relatively low levels of the company. These are always risk areas.

Make Sure Your People Are Trained

Some of these issues involve education and training. People may not recognize that they can't look up Aunt Sally's records, even if they are trying to be helpful. Teach your employees well.

Have Sanctions—and Use Them

Make sure your company has sanctions in place for this kind of inappropriate access to information. If people know they will get fired for snooping, most won't do it. While sanctions will not deter everyone, if people know that they will get caught and that they will be punished, it goes a long way.

Review Your Front-end Controls

One of the causes of this problem is the widespread availability of information within companies. All companies should review the access of employees to personal information. Access should be controlled by job responsibility in any place possible. If people have access to information that they do not need to do their job, then this access creates nothing but risk. Be aggressive and creative about how to control access.

Develop a "Back-end" Review Program

Access control is not a perfect solution. Many employees need access to lots of information to do their jobs. A customer service employee, for example, may need access to information about every customer, because you never know who will call. That's OK—although they don't really need access to everyone's social security number, right?

Once you have gone through your business activities and reduced and controlled access *wherever possible*, you still need a back-end program to review how access is actually being used. Can you tell what each employee looked at? Can you "spot-check" what employees are doing on a regular basis? Do you have a way of checking if you receive reports or complaints about inappropriate access?

This "back-end" program is clearly not one-size-fits-all. But every company needs to develop a program tailored to its business to keep tabs on what is actually going on. *You must recognize this risk and develop a program to proactively detect and deter problematic activity.*

Keep on Top of This Issue

This problem is not going away, but the means of tackling it change regularly. Your key: *Recognize that this is an issue and build a reasonable plan to address it.* Don't just rely on what you've done in the past. And make sure that you're keeping up with what's happening to others and with how your business is changing.