by John Wunderlich

How SERIOUSLY Do You Take PRIVACY?

On January 12, 2011, a number of news outlets reported the firing of three employees and one contracted nurse from the University Medical Center (UMC) in Tucson, Arizona; UMC was where the surviving victims from a well-publicized shooting were being treated.

"The hospital has terminated three clinical support staff members this week for inappropriately accessing confidential electronic medical records, in accordance with UMC's zero-tolerance policy on patient privacy violations," read the statement issued by UMC officials. This demonstrated a high level of commitment to the protection of privacy by UMC. Is this the same standard to which payroll professionals should hold themselves?

Most surveys of Canadians indicate that there are two types of data about themselves that are critical and must be protected: medical and financial (including payroll) data. So based on UMC's actions in Arizona, we should ask ourselves:

- Are there similar types of privacy violations in the payroll world?
- Is your organization *prepared* to terminate for cause for deliberate privacy violations?
- Is your organization *able* to terminate for cause for deliberate privacy violations?
- Is your organization *willing* to implement the policy if there was a privacy breach?

Are there similar types of privacy violations in the payroll world?

This is readily answered in the affirmative, and I am not necessarily referring only to criminal activities, such as selling payroll data to identity thieves. It may be as simple as a payroll administrator looking up a manager's or co-worker's pay or benefits to share with a friend or colleague. This is a deliberate accessing of personal information for a purpose other than the one for which it was collected. (Bonus points to readers who can identify which privacy principles this violates!)

Is your organization *prepared* to terminate for cause for deliberate privacy violations?

Most privacy policies include a phrase such as "Violations of this policy may lead to discipline, up to and including termination." However, most organizations neglect to actually determine the kinds of violations that should lead to termination. Is a single egregious violation enough or does it require a pattern of behaviour and progressive discipline? Does the violation have to be deliberate? Does the number of records involved have any effect? Does it matter whether the person whose information is violated knows about the violation?

In my opinion, a single egregious, deliberate violation of someone's privacy should be sufficient to trigger an immediate termination for cause. No matter how much training and awareness it provides, your organization's commitment to the protection of personal information will likely only be taken as serious by a regulator or auditor if it is prepared to terminate offenders. You should consider clarifying where your organization stands.

Is your organization *able* to terminate for cause for deliberate privacy violations?

Even if your organization is prepared to terminate for cause, is it able to do so? Is your organization's policy clear on the circumstances where violators will be terminated so that employees are informed? Are you in a unionized environment, where a collective agreement might come into play? Do you have HR best practices that require progressive discipline and demonstration of cause before termination?

Think of a privacy policy violation in the same way as a workplace health and safety violation. If someone is blatantly ignoring the rules, he or she is a danger to everyone. Can you work through these issues effectively with the employee and/or the union? Examining these

questions will tell you whether you have the capability to terminate for cause for privacy violations.

You should validate the provisions of your privacy and HR policies to ensure they match your policy wishes (expressed in your responses to the questions above). If you identify any significant gaps, then you have a project to work on.

Is your organization *willing* to implement the policy if there was a privacy breach?

So you have determined that your organization's policy is to take privacy violations seriously. You have also ensured your policies give you the discretion to terminate, as well as the guidelines on which violations qualify for termination. At this point, you are probably hoping this is a policy that you'll never have to implement. However, it's better to be clear going in. If your organization is not willing to enforce the policy, it should seriously consider modifying it.

Play this scenario out. Your organization has a database administrator who is indispensable because she understands all your systems, even the legacy ones. You discover that she has been using current data to test new systems and that other employees could therefore access the data if they wanted to. The administrator demonstrated a casual disregard for your security and privacy policies. If it were anyone else, you would initiate termination—but would you for this person? What if it were the president of the organization we were talking about? Until you have had discussions and have a clear answer to that question, your organization is not ready to face a serious privacy incident. ■

John Wunderlich is an information privacy and security consultant, based in Toronto. For more information, check out his intermittently updated website at http://compliance.wunderlich.ca.

Notice: This column reflects solely the opinions of the author. Individuals are encouraged to seek qualified legal advice on points of law or matters of interpretation.

PUBLICATIONS
FROM THE CPA

Your Payroll
Privacy
Questions Answered,
second edition

Payroll, by its very nature, has always operated with the realities of confidentiality and privacy protection. This updated publication looks at how privacy laws apply to payroll management and discusses what should be done and what would be beneficial to do.

Your Payroll
Vacation
Questions Answered

One of the biggest anxieties for payroll professionals is dealing with annual vacations. This is particularly true if your organization operates in more than one jurisdiction. This publication provides detailed information and resources on payroll-related issues surrounding vacation time and pay in Canada.

THE CANADIAN PAYROLL ASSOCIATION CPA ACP L'ASSOCIATION CANADIENNE DE LA PAIE

To order your copy ($44.95 each plus tax & shipping), visit **www.payroll.ca**.