by John Wunderlich

This is the first of six articles that will deal with the different aspects of managing personally identifiable information through its life cycle. This article focuses on the policy and procedure framework necessary to be able to talk about, manage, and measure personally identifiable information, beginning with when your organization first acquires it to when your organization can safely dispose of it.

An Information Life Cycle Approach: It's Not Always about You

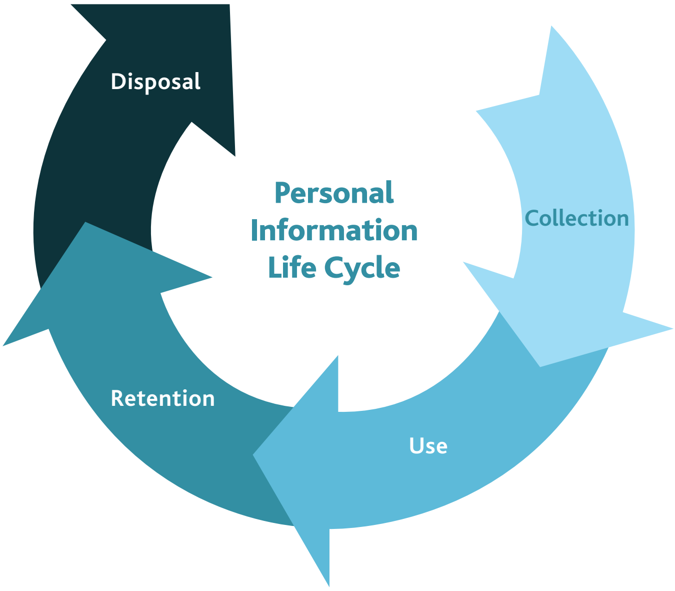
Sometimes it is worthwhile to step back and look at what you are doing and why. This is especially true when there are risks involved— as is the case with the collection, use, disclosure, retention, and disposal of personally identifiable information. Just because last year's approach sufficiently minimized risks does not mean it continues to do so.

The New Year is a good time to start thinking about this. After the yearly tax filing deadlines are past, it is a good time to map out where you are going with your information policies and procedures.

Information life cycle management (ILM) is a comprehensive approach to managing the flow of an information system's data and associated metadata from start to finish. This approach is not just about hardware or storage procedures; it tries to capture, and sometimes automate, the process of moving information through an organization's information systems.

Information, or data, management is becoming increasingly important as compliance-related issues proliferate. Privacy is just one area of this issue. If your organization does not already have an ILM project in place, now would be a good time to start. What does that mean for payroll professionals?

The life cycle of payroll/HR data from a privacy perspective can be simplified in the following chart: information coming into the organization (collection), sharing of the information within and outside of the organization (use), storing of the information while at the organization (retention), and destroying the information once no longer needed (disposal).



To get ready to manage the information through its life cycle, you need to ensure you have the policies and procedures in place to implement what you need to do. The following is a list of some of the most essential tools.

Policies

- **Employee Privacy Policy:** This policy should state clearly what data is collected from employees and for what purposes. This ensures that "collection" and "use" are documented properly. From an ILM perspective, the policy should also provide guidance on when and to whom data may be disclosed, and set out the general rules for retention.
- **Data Security Policy:** The security policy is the complement to the privacy policy. It should set out the requirements for ensuring that data disposal is documented, and how retention limits may be implemented.
- **Data Retention Schedules:** Each organization should establish what requirements for data retention apply to it. At minimum, this should define what data is required to be kept to meet Canada Revenue Agency requirements, and there may be additional industry or professional standards. From a privacy

point of view, the actual length of retention is the minimum time necessary to exhaust all reasonable business uses and applicable regulatory requirements for retention.

- **Third Party Requirements Policy:** There should be a policy, or at least standard language, for organizations to which data is disclosed to follow. This does not apply to government agencies that obtain data under statutory authority.
- **Data Disposal Policy:** At the end of the retention period for personally identifiable information, it must be disposed of. This policy provides guidance to ensure that all copies of data are identified and disposed of in a timely manner.

Request for Questions & Feedback

Over the course of 2012, I will devote one column to each of the following topics:

- **Collection:** What information can you gather and why?
- **Use:** What can you do with the information you have and why?
- **Disclosure:** With whom can you share information and why?
- **Disposal:** How can you safely dispose of information?
- **Metrics:** What kind of information do you want to use to measure your successes?

I would like to include practical advice that relates to how you do business. To that end, please send me questions about privacy and information life cycle or examples of when you did one aspect of the life cycle particularly well. I am also interested in hearing about challenges that you have faced.

Send you questions and feedback to **john@wunderlich.ca**. Include "**CPA Life Cycle**" in the subject line.

With your input, I think we can make some interesting, relevant case studies to help all of us improve the way we meet our privacy requirements. ■

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.