

# Privacy & Security Law Update

## How confident are you? Privacy Program Assessments

Privacy professionals are often asked to determine what statements can be made to customers, employees and regulators about privacy practices.

In order to make statements with confidence, it is critical to know what your practices really are. You can collect data about your practices in many different ways, but self-assessments deliver more value per dollar spent than just about any other tool.

### Goals

The privacy self-assessment should be designed to accomplish a defined educational



goal or to determine if a specific control is working or an identified risk is being properly managed.

For example, you might want to know if all sensitive information is being handled appropriately. Or you might want to test the ability of your customer service team to respond accurately to questions.

To establish the right goals, spend a few minutes thinking about the risks that keep you awake – employee misconduct, vendor errors, data transmission failures – and then consider what controls you have in place to address these risks.

These are the controls you should assess first.



### Methodology

The next task is to develop an assessment methodology. We recommend defining a list of questions that, when answered, will provide you with the information you need. If possible, establish metrics that rate the effectiveness of the control based on the answer given.

*continued on page 2*

## IN THE SPOTLIGHT... Secure Destruction

Privacy and security laws require secure disposal of personal information.

PIMS recommends that companies adopt a formal secure destruction policy, with implementing procedures, then train workers and periodically assess compliance.

The policy should prohibit discarding paper or electronic media containing sensitive personal information, unless the information is ren-

dered inaccessible. It should address all media, including memory sticks and other portable devices.

Paper records should be shredded or burned. Electronic media should be destroyed or erased in such a way that personal information cannot be recovered from the object.

This policy will help companies comply with the GLBA Safeguards Rule,

the FTC's Disposal Rule for consumer reports, the HIPAA Security Rule for protected health information, and state laws like Georgia Code 10-15-2, which provides that businesses may not discard records containing personal information unless they have taken reasonable steps to ensure that no unauthorized person will have access to the information.

### *PIMS Named a Top Privacy Law Firm*

PIMS was named one of the "Best Privacy Consultancies" in a March 7, 2005 survey of privacy professionals in ComputerWorld Magazine.



## Privacy Assessments

In large organizations, formal survey tools are usually required to enable sufficient data collection. The survey tool may contain check-box questions or require detailed answers. You may supplement the survey by examining samples of documents or “mystery shopping” your processes.


It is important to balance your desire to collect data with the possible business disruption caused by the process. If the assessment is too simple, you won't be able to draw appropriate conclusions. But if the process is too onerous, you may face resistance from the participants.

### Privacy Studio's March Madness

March was “Moving Month” at PIMS! Tanya and Peggy have officially moved into spacious Suite 202 at 2931 Paces Ferry Road in Atlanta.



Peggy and Tanya in the new conference room

Conveniently located in the beautiful Vinings neighborhood, our global corporate headquarters is near shopping, restaurants and Starbucks. We welcome visitors and can provide our out-of-town colleagues with an office or conference room at any time. 

### Implementation

Once the survey tool is finished, you need to identify appropriate participants and ask them to complete the questionnaire by a set date. To ensure cooperation, the process must be supported by senior business leaders and positioned as a positive knowledge-enhancing event.

Ideally, the assessment program will also raise awareness of your privacy compliance goals with the target audience. To do this, include a statement of your goals in the survey introduction. Additionally, for each survey, be sure to ask the respondents what concerns they have about your controls. These answers can be most illuminating.

When the surveys are in, you need to determine what steps, if any, can be taken to improve your risk profile. Learning that your controls work is good, but finding ways to minimize

risk is better. You should also share the results and recommendations appropriately.

### A Word of Caution

There's always the chance that your assessment will reveal serious non-compliance issues. You should talk with your legal department before you start to see if you can protect the assessment results under the attorney-client privilege.

You must also be prepared to address any material gaps. Ignorance of gaps is not a defense in an enforcement action, but the penalties for ongoing non-compliance may be much worse if you have actual knowledge of the problems.

If you have any questions about assessments or would like help developing a self-assessment program, please call Peggy Eisenhauer at 404-914-1163.

## Chambliss Golf Classic Benefits Children

PIMS is proud to announce its sponsorship of a hole at the upcoming **Robert C. Chambliss Foundation Golf Classic** benefiting Children's Healthcare.



This event raises money for the

Rainbow Response Transport Team, a pediatric ambulance service that enables critically-ill children to be brought to the Children's Healthcare hospitals for treatment. This service has helped thousands of our sickest children be moved safely via specialized ground and air transportation.

The Golf Classic takes place on Monday, May 15, at the St. Ives Country Club in Duluth, GA. A reception for golfers and sponsors is scheduled for May 14. For information on this wonderful program, including golfer registration and sponsorship, please visit the Chambliss Foundation website at [http://www.chamblissfoundation.org/golf\\_classic.htm](http://www.chamblissfoundation.org/golf_classic.htm).

This newsletter is intended for clients and friends of Privacy & Information Management Services—Margaret P. Eisenhauer, P.C. PIMS is a Georgia Law Firm specializing in privacy, security and information management. If you do not wish to receive communications from PIMS, please email [tanya@privacystudio.com](mailto:tanya@privacystudio.com)—we will gladly remove you from our mailing list.

The information contained in this newsletter has been prepared for informational purposes only and is not legal advice. This communication is not intended to create an attorney-client relationship. Whether you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials. If you are not a current client of PIMS, please do not send any confidential information.

Privacy & Information Management Services—Margaret P. Eisenhauer, P.C.  
4355 Cobb Parkway—Suite J-280, Atlanta GA 30339  
Phone: 404-914-1163  
[www.privacystudio.com](http://www.privacystudio.com)