Advisory
HEALTH INFORMATION TECHNOLOGY
PRACTICE GROUP | OCTOBER 2008

WIGGIN AND DANA
Counsellors at Law

New Law Concerning the Protection of Personal Information Takes Effect on October 1, 2008

A new Connecticut law imposing protections against identify theft will take effect on October 1, 2008. The law, Public Act 08-167, applies to any person or entity that collects or possesses another person's personal information.

"Personal information" is defined in the Act as: "information capable of being associated with a particular individual through one or more identifiers . . . ." The Act includes examples such as:

- social security numbers,
- driver's license numbers,
- state identification card numbers,
- account numbers,
- credit card or debit card numbers,
- passport numbers,
- alien registration numbers, or
- health insurance identification numbers.

Publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media is specifically excluded.

Since the definition of "personal information" is broad, most health care providers will be covered by the new law. In fact, Public Act 08-167 specifically authorizes the Department of Public Health to enforce the law with respect to the individuals and institutions that it licenses.

Summary of the New Requirements:

1. *Prevention of Misuse By Third Parties*

The Act imposes a general obligation on any person or entity in possession of another person's personal information to safeguard that information from misuse by third parties. This duty to prevent misuse applies to personal information in any medium, including computer files or paper documents.

Although the Act does not describe the specific measures that must be taken to ensure personal information is safeguarded, it is adviseable to adopt safeguards that are consistent with industry standards. This would include, among other things, the implementation of technical safeguards, such as access controls, to

© 2008 Wiggin and Dana LLP
In certain jurisdictions this may constitute attorney advertising

protect personal information held in electronic form and the adoption of procedures to investigate, mitigate and remediate suspected and/or actual privacy breaches.

2. *Proper Disposal of Personal Information*

The Act further specifies that all personal information must be destroyed, erased, or made unreadable before disposal. Accordingly, you will need to adopt document destruction policies and practices that address this requirement or ensure your existing policies and procedures address the destruction or sanitation of documents and records containing personal information.

3. *Adoption and Publication of Privacy Protection Policy*

If you collect social security numbers in the course of business, you must adopt a privacy protection policy that specifically addresses the protection of social security numbers. The policy must prohibit unlawful disclosure of social security numbers and limit access to social security numbers. The policy must either be published or publicly displayed. This can be accomplished by posting the policy on an Internet web page, for example.

While many health care providers already have in place HIPAA privacy and security policies, the policies should be reviewed to ensure they address the protection of social security numbers. Alternatively, separate policies unique to the protection of social security numbers should be adopted.

Enforcement

The Act provides for a civil penalty of $500 for each intentional violation, with a $500,000 limit for any single event.

Starting October 1, 2008, Connecticut regulatory agencies will have the authority to enforce the Act with respect to the people or entities to whom they issue a license, registration, or certificate. You should therefore be prepared for the possibility that the Department of Public Health may ask to inspect your social security privacy protection policy as a part of a licensure survey or in response to a privacy complaint.

Note Regarding Connecticut's Security Breach Notification Law

In 2005, Connecticut passed a law requiring anyone conducting business in the State who owns, licenses, or maintains personal information held in electronic form to notify any Connecticut resident whose personal information may have been unlawfully accessed. The law, which went into effect on January 1, 2006 and is now codified at Connecticut General Statutes § 36a-701b, defines personal information as "an individual's first

name or first initial and last name in combination with any one, or more, of the following: (1) Social Security number; (2) driver's license number or state identification card; or (3) account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account." As in the new Public Act 08-167, public information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

The statute defines "breach of security" as "unauthorized access to or acquisition of electronic files, media, databases or computerized data containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable."

Under the statute, the disclosure must be made without unreasonable delay, unless a law enforcement agency determines that the notification will impede a criminal investigation, and the agency has requested that notification be delayed. Notification is not required if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, it is reasonably determined that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed. Failure to comply with this statute constitutes an unfair trade practice.

It is possible that notifications made to individuals of an actual or potential security breach under Connecticut's security breach notification law may come to the attention of the Attorney General's Office or a Connecticut regulatory agency, which may in turn scrutinize your policies and practices. Consequently, it is important that you implement the necessary policies and procedures required to comply with Public Act 08-167.

If you have any questions regarding this advisory, please contact:

Maureen Weaver
203.498.4384
mweaver@wiggin.com

Michelle Wilcox DeBarge
860.297.3702
mdebarge@wiggin.com

This publication is a summary of legal principles. Nothing in this article constitutes legal advice, which can only be obtained as a result of a personal consultation with an attorney. The information published here is believed accurate at the time of publication, but is subject to change and does not purport to be a complete statement of all relevant issues.