

Privacy & Security Law Update

from Qualification to Termination

Working with Vendors

U.S. companies are increasingly subject to fiduciary-like duties with regard to sensitive personal information. These duties include protecting the information with reasonable security measures, preventing misuse of the information (such as uses outside of a privacy notice), and notifying individuals of security breaches. The duties mandate both internal controls and oversight of data processors.

Federal Regulations

Federal laws impose information security requirements on companies in certain industries. Companies “significantly engaged in activities that are financial in nature” are subject to the Gramm-Leach-Bliley Act



(GLBA) Safeguards Rule; health-care companies are sub-

ject to the HIPAA Security Rule. These laws also require controls on data processors.

The GLBA Safeguards Rule requires financial institutions to maintain an information security program containing administrative, technical and physical safeguards to protect the security, confidentiality and integrity of customer information. Financial institutions must oversee service providers by selecting service providers that can maintain appropriate safeguards, and requiring security controls in a contract.

The HIPAA Security Rule contains requirements for data processors (or business associates, BAs). Each BA must (1) implement administrative, physical, and technical safeguards to protect the confidentiality, integrity, and



availability of the information; (2) ensure that its agents implement appropriate safeguards; (3) report security incidents; and (4) authorize termination if the BA violates a material term of the contract.

State Laws

In 2004, California became the first state to impose a general security standard on businesses that maintain personal information. CA Civil Code 1798.81.5 targets entities that

continued on page 2

PIMS Sample Standard Vendor Security Terms are included on pages 3 & 4.

IN THE SPOTLIGHT... Social Security Numbers

In 2002, California became the first state to protect Social Security numbers (SSNs). CA Civil Code 1798.85 prohibits any person or entity from:

- Publicly posting or displaying a SSN in any manner.
- Printing a SSN on any card required for the individual to access products or services.
- Requiring an individual to transmit a SSN over the Internet unless the connection is secure or the SSN encrypted.
- Requiring an individual to use a SSN to access a website, unless a password or other authentication device is also required to access the website.

- Printing an individual’s SSN on any document mailed to the individual, unless state or federal law requires the SSN to be on the document or it consists of a “form or application.”

Many states have copied this law, in some cases adding provisions. For example, some states prohibit the recording of SSNs on payment instruments or using SSNs as identification numbers or account numbers. Michigan requires companies to have a written policy for SSNs.

Companies are also expected to secure SSNs because this data element is so closely associated with identity theft.

Companies should classify SSNs as a “sensitive data element” so that it receives appropriate protection. Companies should ensure that data processors agree to protect SSNs and comply with these laws.

Companies should also ensure that all transmissions of SSNs are secure and that SSNs are not being sent or received by unencrypted email or inappropriately included on paper documents sent via the mail.

Privacy Studio.com

The Art of Information Management

Managing Vendors

are *not* covered by GLBA, HIPAA or other Federal laws.

This law requires businesses that handle sensitive personal information (such as Social Security numbers, California ID numbers, financial information or medical records) about Californians to maintain reasonable security procedures and pro-

tect the information from unauthorized access, destruction, use, modification or disclosure. This law also compels businesses to impose security requirements on entities that process data for them.

Over 35 states have enacted security laws. While many of these laws focus on security breach notification, several parallel the California law and require companies to protect personal information. As dis-

cussed in the Spotlight column, many states also regulate the processing of Social Security numbers.

Unfair Trade Practices Liability

Even absent a specific law, companies must protect sensitive personal information. Failure to protect information is considered an unfair trade practice because it can cause substantial injury that is not offset by any countervailing benefits and that cannot reasonably be avoided by the individual.

In the absence of explicit requirements, regulators look to the GLBA Safeguards Rule as a model. Since GLBA requires “reasonable security,” the FTC and others believe that it sets a good standard for all companies.

Companies must also prohibit data processors from using personal information in a manner that is inconsistent with the companies’ published privacy notices. As the FTC opined in the Cart-Manager case, data processors cannot exceed the scope of companies’ privacy notices, and companies must manage the actions of the data recipients.

Companies should use their data processing contracts to inform their data processors of the appropriate scope of their use of the company’s personal information as well as their obligation to reasonably safeguard the data from loss or unauthorized access.

Conducting Due Diligence on Data Processors

It is critical that companies ask prospective vendors the following types of questions about their privacy and security programs as part of their pre-contract due diligence.

1. Do you have a written policy regarding the confidentiality and security of information you process for customers? [If so, please provide a copy.] Is this policy implemented with specific, written security procedures? Please provide contact information for your chief security officer and chief privacy officer.
2. Have you implemented a formal security program containing administrative, physical and technological controls to protect your computer systems, operating systems, networks, applications and databases?
3. Will the information we provide you be segregated? Do you have procedures to limit access to only those workers who need access to perform services for us?
4. Would our information be encrypted or otherwise protected during transmission to/from us and among your workers and processors? What secure transmission technology do you employ?
5. Do you have procedures to limit the ability of workers to download information from your systems and network onto desktops, laptops, PDAs or other portable devices? Are all laptops and portable devices encrypted?
6. Have you established physical and logical security domains with highly-restricted access? Would our information be maintained in the highest level domain? Would paper copies of our information be kept in locked file cabinets?
7. Do you have procedures to redact or limit the display of sensitive data elements (such as Social Security numbers) in your computer systems?
8. Do you conduct background checks on all workers? Do workers sign confidentiality agreements? Are workers trained on privacy, security and confidentiality? Are workers monitored for compliance with your policies and procedures?
9. Has your security program been audited or assessed by a third party? If so, when was it conducted and by whom? [Please provide a copy of the report.]
10. Do you have established procedures to detect and respond to a security incident?
11. Would your professional liability insurance be sufficient to cover all costs associated with an incident involving our information? [Please provide coverages.]

Kudos to Very Caring Clients

Please join us in congratulating two individuals who have literally gone the extra mile to help others. Last month, **John Gevertz** (ADP) completed the Bresnan Bike Tour, a 200-mile ride to benefit the Special Olympics, while **Connie LaMotta** (LaMotta Strategic Communications) participated in the “Walk-to-de-Feet ALS.” PIMS is proud to support their efforts with contributions to these very worthy causes.

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—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 us 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

PIMS Sample Standard Vendor Terms

Vendor agrees that it shall comply with the following provisions with respect to all “Personal Information” collected, used, transmitted or maintained for Company **and its affiliates**. This Addendum stipulates privacy, confidentiality, and security requirements and demonstrates compliance with applicable privacy, security and data protection laws.

1. **Definitions.**

- (a) “Personal Information” means any and all data (regardless of format) that (i) identifies or can be used to identify, contact or locate a natural person, or (ii) pertains in any way to an identified natural person. **Personal Information includes: [list specific elements.]**
- (b) “Processing” means any operation or set of operations which is performed upon Personal Information, whether or not by automatic means, such as collection, compilation, use, disclosure, duplication, organization, storage, alteration, transmission, combination, redaction, erasure, or destruction.
- (c) “Sensitive Personal Information” is a subset of Personal Information, which due to its nature has been classified by law or by Company policy as deserving additional privacy and security protections. Sensitive Personal Information consists of: (i) all government-issued identification numbers, (ii) all financial account numbers (including payment card information), (iii) individual medical records and biometric information, (iv) all other data obtained from a U.S. consumer reporting agency, (v) data elements revealing race, ethnicity, national origin, religion, trade union membership, sex life or sexual orientation, and criminal records or allegations of crimes of EU residents, **and (vi) any other Personal Information designated by Company as Sensitive Personal Information.**
- (d) “Services” means any and all services that Company requests the Vendor to perform under any contract or agreement that involves Processing of Personal Information. **[If possible, tie with services contemplated in the contract.]**

2. **General Obligations.**

- (a) Vendor will Process Personal Information only as authorized and as necessary to perform the Services.
- (b) Vendor shall immediately inform Company in writing: (i) if it cannot comply with any material term of its agreement with Company regarding the Services. If this occurs, Vendor shall use reasonable efforts to remedy the non-compliance. Company shall be entitled to suspend the communication of Personal Information and to terminate any of Vendor’s further Processing of Personal Information; (ii) of any request for access to any Personal Information received from an individual who is (or claims to be) the subject of the data; (iii) of any request for access to any Personal Information received by Vendor from any government official (including any data protection agency or law enforcement agency); (iv) of any other requests with respect to Personal Information received from Company’s employees or other third parties, other than those set forth in the agreement. Vendor understands that it is not authorized to respond to these requests, unless explicitly authorized by Company or the response is legally required under a subpoena or similar legal document issued by a government agency that compels disclosure by Vendor.
- (c) **If the Services involve the collection of Personal Information directly from individuals, Vendor will provide the individuals with a clear and conspicuous privacy notice, which notice shall be approved by Company.**
- (d) **Vendor shall not transfer the Personal Information across any national borders or permit remote access to the Personal Information from any employee, affiliate, contractor, or other third party outside of the country unless Vendor has the prior written consent of Company for such transfer or access.**
- (e) Vendor shall cooperate with Company and with its affiliates and representatives in responding to inquiries, claims and complaints regarding the Processing of the Personal Information.

3. **Confidentiality; Data Access and Disclosure.**

- (a) **Consistent with the confidentiality provisions of the agreement with Company,** Personal Information is considered Confidential Information of Company and Vendor must maintain all Personal Information in strict confidence.
- (b) Vendor may disclose Personal Information to its employees and workers, but only to the extent such individuals: (i) require access to the Personal Information to perform the Services; (ii) have been subject to an appropriate background investigation whose results were acceptable; (iii) have been trained on the privacy, confidentiality and security

requirements related to the Personal Information; and (iv) are subject to an appropriate confidentiality agreement in a form approved by Company.

(c) Vendor shall not disclose, transmit, or otherwise make the Personal Information available to other third parties (including subcontractors) unless such Processing is required to perform the Services or has been explicitly authorized by Company in writing.

4. Information Security Requirements

(a) Vendor shall have implemented and documented appropriate operational, technical and organizational measures to protect Personal Information against accidental or unlawful destruction, alteration, unauthorized disclosure or access. Vendor's security program shall contain the minimum standards set out on Company Security Requirements Document, a copy of which is attached hereto. Vendor will regularly test and monitor the effectiveness of its safeguards, controls, systems and procedures. Vendor will periodically identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of the Personal Information, and ensure that these risks are addressed. Vendor will also monitor its workers [and subcontractors] for compliance with the security program requirements.

(b) If the Processing involves the transmission of Personal Information over a network, Vendor shall have implemented appropriate supplementary measures to protect the Personal Information against the specific risks presented by the Processing. Sensitive Personal Information may only be transmitted in an encrypted format.

(c) Sensitive Personal Information may not be stored on any portable computer devices or media (including, without limitation, laptop computers, removable hard disks or flash drives, personal digital assistants (PDAs) or computer tapes) unless the Sensitive Personal Information is encrypted.

(d) Upon request, Vendor shall provide Company with information about the Vendor's information security program. Vendor shall also submit its data processing facilities for audit, which shall be carried out by Company (or by an independent inspection company designated by Company). Vendor shall fully co-operate with any such audit. In the event that any such audit reveals material gaps or weaknesses in Vendor's security program, Company shall be entitled to suspend transmission of Personal Information to Vendor and terminate Vendor's Processing of Personal Information until such issues are resolved.

(e) Vendor will promptly and thoroughly investigate all allegations of unauthorized access to, use or disclosure of the Personal Information. Vendor will notify Company immediately upon discovery of any such unauthorized access to, use or disclosure. Vendor shall bear all costs associated with resolving a security breach, including (without limitation), conducting an investigation, notifying consumers and others as required by law or the Payment Card Industry Data Security Standard, providing consumers with one year of credit monitoring, and responding to consumer, customer, regulator and media inquiries.

(f) When the Vendor ceases to perform Services for Company, Vendor will either (i) return the Personal Information (and all media containing copies of the Personal Information) to Company, or (ii) purge, delete and destroy the Personal Information. Electronic media containing Personal Information will be disposed of in a manner that renders the Personal Information unrecoverable. Upon request, Vendor will provide Company with an Officer's Certificate to certify its compliance with this provision. If any Personal Information is retained by Vendor, Vendor warrants that it shall ensure the continued confidentiality and security of the Personal Information and shall not actively Process the Personal Information.

(g) Vendor shall carry appropriate insurance to address the risks from its Processing of the Personal Information. Company shall be named a third party beneficiary of these policies.

5. Compliance with Laws

Vendor must stay informed of the legal and regulatory requirements for its Processing of Personal Information. Vendor's Processing shall comply with all applicable privacy or security laws and regulations, as well as Vendor's own privacy notices.

DISCLAIMER

These sample vendor terms are general provisions, provided for information and reference purposes only. These provisions are designed to illustrate the types of terms that should be included in vendor contracts; they are not designed to meet legal requirements that apply to the processing of regulated information (such as financial records or healthcare data). They also do not provide an adequate substitute for contract-specific due diligence and negotiation. For more information about these sample terms, please call Peggy Eisenhauer at 404-914-1163.

If you have questions about a specific vendor contract, please seek appropriate legal advice.