PRIVACY LAW GUIDE

MAIER LAW GROUP
EMPLOYMENT AND PRIVACY LAW

MAIER LAW GROUP
EMPLOYMENT AND PRIVACY LAW

Table of Contents

What is privacy?

- Data privacy asks whether personal or confidential information is guarded in a way that protects the interest of the data subject. What about the monetary value of the information, in cases of proprietary information?
- These questions have always been asked, but they are much more urgent and relevant NOW.
- Privacy is what we do to ensure that information is being collected, shared, used, and disposed of in appropriate ways.

Why is data privacy such a hot topic?

- Data privacy is one of the fastest growing areas of law.
- As our production of information continues to grow, people are getting increasingly concerned with what happens to all this data, particularly as it relates to their private lives.

770 Tamalpais Drive, Suite 321, Corte Madera, CA 94925
maierlawgroup.com | tel. 415-515-1707 | fax. 415-524-4854

- Every two days now, we create as much information as we did from the dawn of civilization up until 2003, according to former Google CEO Eric Schmidt. That's something like five exabytes of data, he says.

What about data security?

- Even if we're careful about keeping private information private, there are hackers all around, and people's computers or devices can be lost or stolen. In the modern day, those devices carry tremendously sensitive information.
- How do we take technical, administrative, and physical steps we need to safeguard our important data? This is what we call data security.

What is personally identifiable information?

Personally identifiable information (PII) is any data that could potentially identify an individual, so it must be protected. PII includes:

- Name
- Social security number (SSN)
- Date of birth (DOB)
- Mother's maiden name
- Financial records
- Email address
- Driver's license number
- Passport number
- Health information

What are the types of privacy risks?

- Legal Compliance—Failure to comply with privacy laws and regulations can result in significant legal sanctions, liability, fines, etc. and even criminal penalties.
- Reputational—Having a privacy breach can severely damage the reputation of a company.

770 Tamalpais Drive, Suite 321, Corte Madera, CA 94925
maierlawgroup.com | tel. 415-515-1707 | fax. 415-524-4854

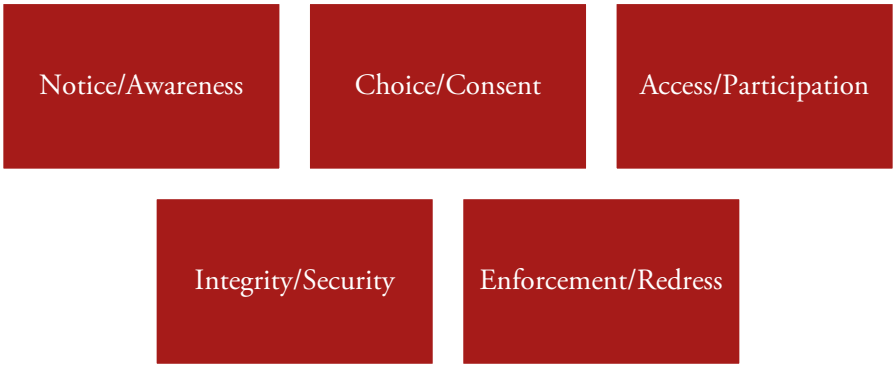
- Financial—Privacy violations can lead to costly litigation, large damage awards, and expensive and burdensome legal requirements (data security breach notification).
- Time and Resources—One of the largest often under-appreciated privacy risks involves the extensive amount of time and resources needed to respond to a privacy breach.
- Client Relationships—Privacy incidents or even poor privacy practices that have not involved an actual breach can sour relationships between a company and its clients or a company and its employees.
- Employee Disenfranchisement—Not taking care with PI of employees or clients sends a message that the company doesn't value its resources, is unsophisticated, and is not trustworthy.

What are the main causes of privacy incidents?

- Malware and hacking present the greatest threat, both in the number of breaches and the number of records breached.
- Physical breaches, resulting from theft or loss of unencrypted data on electronic devices, came in a distant second.
- Breaches caused by errors, predominantly misdelivery (of email, for example) and inadvertent exposure on the public internet, were a close third.

How do we practice good privacy?

- The Fair Information Privacy Principles are the five core components of privacy protection:



770 Tamalpais Drive, Suite 321, Corte Madera, CA 94925
maierlawgroup.com | tel. 415-515-1707 | fax. 415-524-4854

- Each industry has its own privacy laws. For example, non-bank financial institutions have Gramm-Leach-Bliley, and medical institutions have HIPAA.

Why do life science companies need to know about HIPAA?

- HIPAA is a federal law that governs protected health information ("PHI") in the United States. HIPAA protects individually identifiable health information.
- Most biotech and life sciences companies are not directly covered by HIPAA (i.e., they are not a covered entity or business associate).
- If your company collects and uses de-identified or individually identifiable patient health data from clinical studies and work closely with HIPAA-covered entities, it is still very important to understand HIPAA because clinical trial agreements may indirectly impose HIPAA standards on life sciences companies.

What are some HIPAA best practices?

- Determine whether your entity is a covered entity or business associate. This determination can be complex - consult with the experts in (or outside, if not available internally) your organization.
- If your organization is not a covered entity or business associate, determine whether it has contractual obligations to satisfy certain HIPAA requirements.
- If your organization does have to comply with HIPAA, there are many things you'll need to do. Again, consult with people with expertise in this area!
- If HIPAA does apply, life science companies should perform a risk assessment of HIPAA compliance. Next, they should review and update workforce training and policies to confirm HIPAA compliance. Finally, they should review and understand any business associate agreements.

What questions should you consider to evaluate your company's privacy?

- How does your business collect, use, share and store information of clients or employees? Do you have a lawful or legitimate basis for doing so?
- Where is the data stored/where is it going?

770 Tamalpais Drive, Suite 321, Corte Madera, CA 94925
maierlawgroup.com | tel. 415-515-1707 | fax. 415-524-4854

- How is information collected used and shared? What are the business purposes for each?
- Who has access to the information collected, and is there a less intrusive way to collect/process/store it?
- How are the Fair Information Practices met?
- What does your privacy policy say, where is it posted, and do you truly follow it?
- What are user expectations about your website/email system, etc.?
- Do you follow international data protection requirements and observe cross-border data transfer restrictions?

What are some privacy and security best practices?

- Secure paper and physical media.
- Control access to data sensibly.
- Use complex passwords.
- Practice laptop safety.
- Do not fall for phishing, malware, hoaxes, etc. in email or online.
- Use care when viewing or discussing sensitive information around people who do not need to know.
- Be careful with public internet.
- Exercise care when downloading software.

770 Tamalpais Drive, Suite 321, Corte Madera, CA 94925
maierlawgroup.com | tel. 415-515-1707 | fax. 415-524-4854