Data Privacy and Security
Ethical Obligations and the Protection of Client Data

Olmsted County Law Library
July 13, 2018
Stacy Harper, JD, MHSA, CPC
913-327-5120
sharper@spencerfane.com
*Licensed in Minnesota, Kansas, and Missouri
Disclaimer

This presentation is for education purposes only. The laws and regulations at issue in this lecture are open to interpretation. The proper course of action in any given situation related to data privacy and security is very fact specific. The information contained in these materials and presented during the lecture or in response to your questions is for the purpose of intelligent discussion and is not intended to be, and is not, legal advice.

Attendance at this presentation should not be construed as creating an attorney-client relationship with the speaker, nor should the information presented be construed as legal advice.
Why Law Firms?

• Cyber criminals are attracted to:
  – Clients’ intellectual property assets
  – Details of pending merger and acquisition activities
  – Information on litigation that could impact a stock price
  – Advance fee fraud
Impact on Law Firms

- ABA 2017 Technology Survey
  - At least one-third of companies with between 10 and 49 attorneys have been breached, and nearly one-fourth of companies with over 500 attorneys reported the same. 43% of companies overall reported malware infections.
  - Almost 10% of firms with over 500 attorneys reported a breach that affected client data – the worst possible form of breach for a legal firm.
  - Of the remaining breached firms, 38% reported loss of billable hours, 34% were required to pay a consultant to repair their data, and 23% were forced to pay to replace equipment.
  - Less than 5% of law firms report having a Chief Security Officer in charge of their data security.
Confidentiality
Rule 1.6 – Confidentiality

- A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.
- Comment 2 - A fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, the lawyer must not reveal information relating to the representation.
- Comment 17 - Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.
Rule 1.6 – Confidentiality

• Comment 17 (continued) - Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to:
  – the sensitivity of the information,
  – the likelihood of disclosure if additional safeguards are not employed,
  – the cost of employing additional safeguards,
  – the difficulty of implementing the safeguards, and
  – the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

• A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules.
Rule 1.6 – Confidentiality

• Comment 18 - When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.
Rule 1.1 - Competence

• A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation.

• Comment 8 - To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.
5.3 – Non-Lawyers

- a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer
Using Technology to Communicate Confidential Information to Clients

- E-mail without encryption may be used to transmit and receive confidential client information;
- Digital cordless and cellular telephones may be used by a lawyer to transmit and receive confidential client information when used within a digital service area;
- When the lawyer knows, or reasonably should know, that a client or other person is using an insecure means to communicate with the lawyer about confidential client information, the lawyer shall consult with the client about the confidentiality risks associated with inadvertent interception and obtain the client's consent.

Adopted January 22, 1999
Amended January 22, 2010
LPRB Opinion 22

- A lawyer has a duty under the Minnesota Rules of Professional Conduct (MRPC), not to knowingly reveal information relating to the representation of a client, except as otherwise provided by the Rules, and a duty to act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure. Rules 1.1, 1.6, MRPC. The lawyer’s duties with respect to such information extends to and includes metadata in electronic documents. Accordingly, a lawyer is ethically required to act competently to avoid improper disclosure of confidential and privileged information in metadata in electronic documents.

- Metadata can be “scrubbed” or removed from an electronic document by various means, including the use of special software programs or by scanning a printed copy of the document and sending it in a PDF format. Transmission of metadata can also be avoided by transmitting hard copies of the document rather than electronic copies or by faxing the document.
Receipt of Confidential Information
Rule 4.4 – Respect for Rights of Third Persons

- A lawyer who receives a document or electronically stored information relating to the representation of the lawyer’s client and knows or reasonably should know that the document or electronically stored information was inadvertently sent shall promptly notify the sender.

- Comment 2 - Paragraph (b) recognizes that lawyers sometimes receive a document or electronically stored information that was mistakenly sent or produced by opposing parties or their lawyers. A document or electronically stored information is inadvertently sent when it is accidentally transmitted, such as when an email or letter is misaddressed or a document or electronically stored information is accidentally included with information that was intentionally transmitted. If a lawyer knows or reasonably should know that such a document or electronically stored information was sent inadvertently, then this rule requires the lawyer to promptly notify the sender in order to permit that person to take protective measures.
Rule 4.4 – Respect for Rights of Third Persons

• Comment 2 (continued) - Whether the lawyer is required to take additional steps, such as returning or deleting the document or electronically stored information, is a matter of law beyond the scope of these rules, as is the question of whether the privileged status of a document or electronically stored information has been waived. Similarly, this rule does not address the legal duties of a lawyer who receives a document that the lawyer knows or reasonably should know may have been inappropriately obtained by the sending person. For purposes of this rule, “document or electronically stored information” includes, in addition to paper documents, email and other forms of electronically stored information, including embedded data (commonly referred to as “metadata”), that is subject to being read or put into readable form. Metadata in electronic documents creates an obligation under this Rule only if the receiving lawyer knows or reasonably should know that the metadata was inadvertently sent to the receiving lawyer.
If a lawyer receives a document which the lawyer knows or reasonably should know inadvertently contains confidential or privileged metadata, the lawyer shall promptly notify the document’s sender as required by Rule 4.4(b), MRPC.

A lawyer may be subject to a number of obligations other than those provided by the MRPC in connection with the transmission and receipt of metadata, including obligations under the Federal Rules of Civil Procedure and the Minnesota Rules of Civil Procedure. Removing metadata from evidentiary documents in the context of litigation or in certain other circumstances may be impermissible or illegal. Opinion No. 22 addresses only a lawyer’s ethical obligations regarding metadata under the Minnesota Rules of Professional Conduct.
Breach Notification
Rule 1.4 - Communication

- A lawyer shall promptly inform the client of any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(f), is required by these rules.

- Comment 7 - In some circumstances, a lawyer may be justified in delaying transmission of information when the client would be likely to react imprudently to an immediate communication. Thus, a lawyer might withhold a psychiatric diagnosis of a client when the examining psychiatrist indicates that disclosure would harm the client. A lawyer may not withhold information to serve the lawyer's own interest or convenience or the interests or convenience of another person. Rules or court orders governing litigation may provide that information supplied to a lawyer may not be disclosed to the client. Rule 3.4(c) directs compliance with such rules or orders.
Other Data Laws
GLBA – Who is Covered?

- Applies to “financial institutions” – companies that offer financial services or insurance.
- Applies to all businesses, regardless of size, that are “significantly engaged” in providing financial products or services.
- Examples include check-cashing businesses, payday lenders, mortgage brokers, nonbank lenders, personal property or real estate appraisers, professional tax preparers, and courier services. The Safeguards Rule also applies to companies like credit reporting agencies and ATM operators.
GLBA – What is Protected?

- names, addresses, and phone numbers;
- bank and credit card account numbers;
- income and credit histories; and
- Social Security numbers
• designate one or more employees to coordinate its information security program;
• identify and assess the risks to customer information in each relevant area of the company’s operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
• design and implement a safeguards program, and regularly monitor and test it;
• select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information; and
• evaluate and adjust the program in light of relevant circumstances, including changes in the firm’s business or operations, or the results of security testing and monitoring.
HIPAA – Who is Covered?

• Covered Entity
  – Health Plan
    • Includes an employer’s self-insured plan
  – Healthcare Clearinghouse
  – Health Care Providers Electronically Submitting “Covered Transactions” (e.g. claim, eligibility inquiry, remittance advice, etc.)
  – Transaction means the transmission of information between two parties to care out financial or administrative activities related to healthcare including claims or encounter information, healthcare payment or remittance advice, coordination of benefits, health care claims status, enrollment and disenrollment in a health plan, eligibility for a health plan, health plan premium payments, referral certification and authorization, first report of injury, health claim attachments, and other transactions prescribed by regulation.
HIPAA – Who is Covered?

• Business Associate
  – A person/entity who, with respect to a covered entity:
    • On behalf of such covered entity or an organized health care arrangement, but other than as a member of the workforce of the covered entity, creates, receives maintains or transmits PHI for an activity regulated by HIPAA, including claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; patient safety activities; benefit management; practice management and repricing; or
    • Provides, other than as a member of the workforce, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the covered entity or organized health care arrangement where the performance of service involves the disclosure of PHI.
  – BA includes a health information organization, e-prescribing gateway, or other person that provides data transmission services that requires access on a routine basis to such PHI; a person that offers a personal health record on behalf of a covered entity; and a subcontractor that receives, creates, maintains or transmits PHI on behalf of a BA.
  – Certain exceptions
HIPAA – What is Protected?

• Protected Health Information (PHI)
  – Individually identifiable health information that is transmitted in electronic media, maintained in electronic media, or transmitted or maintained in any other form, but not including education records covered by FERPA, certain higher education records, employment records held by a covered entity in its role as employer, and regarding a person who has been deceased more than 50 years.
  – Health information means any information, including genetic information, that is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse and relates to past, present, or future physical or mental health or condition of an individual, provision of health care, or past, present or future payment for the provision of health care.
  – Individually identifiable means information that identifies an individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
HIPAA – What is Required?

- Enter Into Business Associate Agreements before obtaining PHI
  - Use and disclose PHI as permitted by the BAA or as required by law;
  - Use appropriate administrative, technical, and physical safeguards to protect ePHI;
  - Report to the CE any unauthorized use/disclosure or security incident of the PHI;
  - Impose same restrictions on any subcontractors;
  - Make available PHI to respond to an individual’s request for access;
  - Make available PHI for amendment;
  - Make available the information required to provide an accounting of disclosures;
  - If carry out a CE's obligation under HIPAA, comply with HIPAA in the performance;
  - Make internal practices, books, and records available to HHS;
  - At termination, if feasible, return or destroy all PHI or extend protection; and
  - Authorize termination of the BAA by the CE, BA violates a term of the BAA.
GDPR – Who Is Covered

• Organizations Located in the EU
• Organizations located outside the EU if the offer goods or services to, or monitor the behavior of EU data subjects
• Organizations processing and holding personal data of data subjects residing in the EU, regardless of the company’s location
GDPR – What is Protected

• “personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
GDPR – What is Required

- Transparent processing of data, consistent with legal restrictions
- Limit the purpose of data use and retention
- Provide individuals certain rights related to data
- Obtain consent from the individual regarding data use
- Provide breach notification
- Assess data risks
- Impose obligations on subcontractors
- Provide training
State Breach Notification

- Breach notification laws are required in all 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands
- Notification time frames vary by state
- Notification requirements to other parties vary by state
- Definition of PII varies by state
- Rarely apply to data of entities
- States are continuing to amend
- Beginning to incorporate data security requirements
Other Confidentiality Laws

- Confidentiality obligations triggered by court rules
- Part 2 obligations for substance abuse treatment facilities
- Insurance
- Mental Health
- Worker’s Compensation
New California Law

• Goes into effect January 1, 2020
• Requires businesses to:
  – inform consumers of the categories of information collected;
  – provide consumers with copies of their personal information;
  – delete personal information upon consumer request;
  – disclose any third parties with whom information may be sold or shared for a business purpose and allowing the consumer to opt out of the sale of information;
  – avoid any discrimination against a consumer for exercising privacy rights; and
  – amend the business’s online privacy policy.
• Has limited exceptions
It’s a Continual Process

Training → Inventory

Policies → Risk Assessment

Safeguards and Risk Management
Stacy Harper, JD, MHSA, CPC
913-327-5120
sharper@spencerfane.com