Lawyers' Duties to Safeguard Clients' Sensitive Information

Edward C. Hopkins Jr., Esq.

FIP, CIPM, CIPT, CIPP/US, CIPP/G, CIPP/A, CIPP/C, CIPP/E

Key Terms

- Personal or Private Information (PI)
- Private Identifying Information (PII)
- Protected Health Information (PHI)
- Confidential Information (CI)
- Intellectual Property (IP)
- Sensitive Information (SI) = PI, PII, PHI, CI & IP

Examples of SI Requiring Security

- Attorney-client data
- Personal data
- Financial data
- Transaction records
- Tax records
- E-mails

A Lawyer's Duty in a Nutshell

Take reasonable measures to ensure only authorized people access, possess, and use clients' SI.

Sources of Legal Duties

- Other Nations' Laws (e.g. GDPR)
- Federal Laws (e.g. HIPAA, FTC Act)
- F.R.C.P. 5.2 *Privacy Protection For Filings Made With the Court*
- Other U.S. States' Consumer Protection/Deceptive Trade Practices Laws (e.g. Cal. Civ. Code § 1798.81.5(b), 201 Mass. Code Regs. 17.03(1))

Sources of Legal Duties (Cont.)

- Colo. RPC 1.1, 1.4, 1.6, 4.4, 5.1, and 5.3
- Colorado Consumer Protection Act
  - C.R.S. § 6-1-713.5. *Protection of personal identifying information*
  - C.R.S. § 6-1-715. *Confidentiality of social security numbers*
  - C.R.S. § 6-1-716 *Notification of security breach*
  - No private right of action (yet)

Sources of Legal Duties (Cont.)

- Promises in contracts (benefit of the bargain theory)
- Representations in marketing
- Fiduciary duties
- Negligence/Negligent Supervision

Sources of Legal Duties (Cont.)

- ABA Formal Opinion 477R "Securing Communication of Protected Client Information" (2017)
- ABA Formal Opinion 08-451 "Lawyer's Obligations When Outsourcing Legal and Nonlegal Support Services" (2008)
- ABA Formal Opinion 99-413 "Protecting the Confidentiality of Unencrypted E-Mail" (1999)

Sources of Legal Duties (Cont.)

- CBA Formal Ethics Op. 130 "Online Posting and Sharing of Materials Related to the Representation of a Client" (2017)
- CBA Formal Ethics Op. 119 "Disclosure, Review, and Use of Metadata" (2008)
- CBA Formal Ethics Op. 108 "Inadvertent Disclosure of Privileged or Confidential Documents" (2000)

477R's Guidelines

1. Understand the nature of the threat.
2. Understand how SI is transmitted or stored.
3. Use reasonable cybersecurity measures.
4. Determine how communications about SI should be protected.
5. Label SI.
6. Train lawyers and legal staff in technology and cybersecurity.
7. Conduct due diligence on vendors who provide related services.

Analyzing Reasonableness Under 477R

1) Information Sensitivity
2) Likelihood of Disclosure without Safeguards
3) Cost of Implementing Safeguards
4) Difficulty of Implementing Safeguards
5) How Safeguards Will Hinder Attorneys and Staff

Specific Threats

1) Theft and Loss of Devices
2) Employee Criminality (Insider Threat)
3) Social Engineering
4) Privilege Abuse
5) Bypassing of Security Controls
6) Network Port Probes

Specific Threats (Continued)

7) Unpatched Software Vulnerabilities
8) Denial of Service Attacks
9) Group Phishing
10) Spear Phishing
11) Website Exploits
12) Bots

Specific Threats (Continued)

13) Viruses and Worms

14) Trojan Horses

15) Zero-day Exploits

16) Spyware

Data Breach and Incident Response

- Your Obligations under C.R.S. § 6-1-716
  - Personal Information
  - Encrypted vs. Unencrypted Personal Information
  - Misuse of Information
  - Law Enforcement's Involvement in Criminal Breaches
- Develop a Detailed Plan (with an Expert's Help) before Breach Occurs
- Do Mock Data Breach ("Table Top") Exercises Annually

20 Recommended Measures

1) Get privacy program management and technical assistance from an expert information privacy professional.
2) Get information security management and technical assistance from an expert information security professional.
3) Encrypt all SI the firm and the firm's vendors store for clients.

20 Recommended Measures (Cont.)

4) Only use cloud-based data storage services that offer zero-knowledge, end-to-end encryption security and allow you to apply time-limited passwords to the files you share via the services.
5) Use virtual private networks when transmitting SI to encrypt it.

20 Recommended Measures (Cont.)

6) Use strong passwords that limit access to data storage devices containing clients' SI and have 12 to 16 characters, at least one upper case letter, at least one lower case letter, at least one number, and at least one symbol.
7) Keep all firm electronic equipment and software up to date.

20 Recommended Measures (Cont.)

8) Monitor developments in hacker software and tactics that have been used or will likely be used against law firms by reading leading information security blogs.

9) Design and implement access control measures that limit access to SI to only people who need to access it to effectively represent the firm's clients.

20 Recommended Measures (Cont.)

10) Design and implement a plan that will enable the firm to immediately remove someone's access to all client SI stored in data storage devices the firm controls.

11) Log, monitor, and audit individuals' use of firm computer systems and clients' SI.

20 Recommended Measures (Cont.)

12) Analyze individuals' use of firm computer systems and SI to identify and investigate suspicious activity or activity that indicates the user could be an insider threat who has accessed or has attempted to access SI without authorization.

20 Recommended Measures (Cont.)

13) Design and implement data archiving measures that ensure SI the firm attorneys and staff no longer need to access frequently is encrypted and stored in data storage devices that are not connected to the internet.

14) Design and implement data backup measures that ensure the firm will maintain immediate access to clients' SI even after a ransomware attack.

20 Recommended Measures (Cont.)

15) Create and enforce privacy and information security program policies, including but not limited to bring your own device (BYOD) polices, email communications policies, and internet use policies.

16) Conduct regular privacy and information security education and training for firm attorneys and staff, and, if necessary, for clients, vendors, or business partners.

20 Recommended Measures (Cont.)

17) Conduct biannual audits of firm privacy program management and information security management programs to ensure the programs are still reasonable, and ensure attorneys and staff understand and comply with them.

18) Conduct annual audits of vendors and business partners who store or transmit clients' SI to ensure their privacy program management and information security management measures meet or exceed the standards your firm set.

20 Recommended Measures (Cont.)

19) Create a data breach response plan, which will include a ransomware response plan.

20) Conduct annual data breach response training and exercises.

Questions