17th Annual Family Law Institute

Ensuring Data Privacy and Security in Your Practice

November 15, 2018
2:00 PM
Suburban Collection Showplace, Novi, MI

PAI

Agenda

- Ethical obligations
  - Confidentiality
  - Competence
  - Supervision of lawyers and non-lawyers
- Torts
  - Intrusion on Seclusion
  - Publicity Given to Private Life
  - False Light
- Federal and State Law
- Contracts
- Steps to take to Protect Information
- Breach

Discussion Hypo

Recent law school grad - passed the bar

Burning desire to help people

Decides to “hang out a shingle”

Is confident she knows Family Law subject matter

Uncertain of obligations regarding treatment of client data

What does she need to know?

Ethical Obligations - Confidentiality

Confidentiality

- ABA Model Rule 1.6(a):

"… [a] lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent."

- ABA Model Rule 1.6(c):

"[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"

PAI

Confidentiality

Comment 17 to Rule 1.6(a) gives advice on the determination of reasonableness:

- *Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the:*
  - *sensitivity of the information,*
  - *likelihood of disclosure if additional safeguards are not employed,*
  - *cost of employing additional safeguards,*
  - *difficulty of implementing the safeguards, and*
  - *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.

PAI

Confidentiality

MRPC Rule: 1.6 Confidentiality of Information

(a) "Confidence" refers to information protected by the client-lawyer privilege under applicable law, and "secret" refers to other information gained in the professional relationship that the client has requested be held inviolate or the disclosure of which would be embarrassing or would be likely to be detrimental to the client.

(b) Except when permitted under paragraph (c), a lawyer shall not knowingly:

(1) reveal a confidence or secret of a client;

(2) use a confidence or secret of a client to the disadvantage of the client; or

(3) use a confidence or secret of a client for the advantage of the lawyer or of a third person, unless the client consents ter full disclosure.

PAI

Confidentiality

- **MRPC Rule: 1.6 Confidentiality of Information-cont.**

(c) A lawyer may reveal:

(1) confidences or secrets with the consent of the client or clients affected, but only after full disclosure to them;

(2) confidences or secrets when permitted or required by these rules, or when required by law or by court order;

(3) confidences and secrets to the extent reasonably necessary to rectify the consequences of a client's illegal or fraudulent act in the furtherance of which the lawyer's services have been used;

(4) the intention of a client to commit a crime and the information necessary to prevent the crime; and

(5) confidences or secrets necessary to establish or collect a fee, or to defend the lawyer or the lawyer's employees or associates against an accusation of wrongful conduct.

PAI

Confidentiality

- Arizona Bar Opinion No. 09-04 (Dec 2009) provides some examples of what a lawyer should do to take reasonable security precautions to secure client information. The case involved an online file storage and retrieval system for client access of documents. The client file system:
  - Used Secure Sockets Layer server
  - Encrypted files
  - Several layers of password protection
  - Unique and randomly generated folder names and passwords
  - Conversion of each document to PDF format and
  - Another unique alpha-numeric password to retrieve contents

Confidentiality

- In addition to the protections on the client file system the Opinion provides some examples of what a lawyer should do to take reasonable security precautions to secure client information such as consideration of firewalls, password protection schemes, encryption, and anti-virus measures.
- The opinion does require exercise of sound professional judgment on steps necessary protect against foreseeable attempts at unauthorized access
- The opinion does not require a guarantee of invulnerability to unauthorized access

PAI

Discussion Hypo

She determines to use off the shelf “stuff”

Not technically savvy

Devices added and connected at will

What does she need to know?

Ethical Obligations - Competence

Competence

- **ABA Model 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 Rule 1**.1

" [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.

MRPC Rule: 1.1 Competence provides similar requirements.

PAI

Competence

- Arizona Bar Opinion No. 09-04 (Dec 2009) provides:
- "It is also important that lawyers recognize their own competence limitations regarding computer security measures and take the necessary time and energy to become competent or alternatively consult available experts in the field."
- "As technology advances occur, lawyers should periodically review security measures in place to ensure that they still reasonably protect the security and confidentiality of the clients' documents and information".

Discussion Hypo

Things are going reasonably well

Has enough work - bills are being paid on time

Determines she could be more efficient with some help

Seeks to hire legal assistant and administrative support

Added staff requires additional equipment

What does she need to know?

Ethical Obligations
Supervision of Lawyers and Non-Lawyers

Confidentiality

MRPC Rule: 1.6 Confidentiality of Information

- (d) A lawyer shall exercise reasonable care to prevent employees, associates, and others whose services are utilized by the lawyer from disclosing or using confidences or secrets of a client …

Supervision of Lawyers and Non-Lawyers

- ABA Model Rule 5.1:

"[a] partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct.“

- ABA Model Rule 5.3:

“a partner, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer.”

Supervision of Non-Lawyers

MRPC Rule 5.3: Responsibilities Regarding Nonlawyer Assistants

With to a nonlawyer employed by, retained by, or associated with a lawyer:

- (a) a partner in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer;
- (b) 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; and

Supervision of Non-Lawyers

MRPC Rule 5.3: Responsibilities Regarding Nonlawyer Assistants – cont'd

(c) a lawyer shall be responsible for conduct of such a person that would be a violation of the rules of professional conduct if engaged in by a lawyer if:

- (1) the lawyer orders or, with knowledge of the relevant facts and the specific conduct, ratifies the conduct involved; or
- (2) the lawyer is a partner in the law firm in which the person is employed or has direct supervisory authority over the person and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

In addition to ethical obligations

- Common law torts
- Federal Law and Regulations
- State law
- Contractual requirements
- Client demands

Intrusion Upon Seclusion

Restatement (Second) of Torts

Section 652B **Intrusion Upon Seclusion**

One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Publicity Given to Private Life

Restatement (Second) of Torts

Section 652D **Publicity Given to Private Life**

One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that

(a) would be highly offensive to a reasonable person, and

(b) is not of legitimate concern to the public

False Light: Restatement

False Light: Restatement

One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if

(a) the false light in which the other was placed would be highly offensive to a reasonable person, and

(b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.

State and Federal Legal Requirements

US Federal & State Statutory Law

- Federal statutes
  - Tend to be narrowly focused
- State law
  - State constitutions may recognize explicit right to privacy (Hawaii, California)
  - State statutes and common (tort) law
  - Local laws and regulations (for example: ordinances on soliciting anonymously)
- This, together with international, is where most practitioners spend their time

PAI

Examples of Federal Laws

- **Cable Communications Policy Act**
- **CAN-SPAM Act**
- **Children's Online Privacy Protection Act**
- **Computer Matching and Privacy Protection Act**
- **Consumer Credit Reporting Reform Act**
- **Driver's Privacy Protection Act**
- **Electronic Communications Privacy Act (ECPA)**
- **Electronic Funds Transfer Act**
- **Electronic Signatures in Global and National Commerce Act**
- **Employee Polygraph Protection Act**
- **Fair and Accurate Credit Transaction Act (FACTA)**
- **Fair Credit Reporting Act (FCRA)**
- **Family Educational Rights and Privacy Act**
- **Financial Services Modernization Act (aka Gramm-Leach-Bliley)**
- **Foreign Intelligence Surveillance Act**
- **Freedom of Information Act**
- **Health Insurance Portability and Accountability Act (HIPAA)**
- **Identity Theft and Assumption Deterrence Act**
- **Privacy Act of 1974**
- **Privacy Protection Act of 1980**
- **Right to Financial Privacy Act**
- **Telecommunications Act**
- **Telemarketing and Consumer Fraud Act**
- **Video Privacy Protection Act**
- **Video Voyeurism Prevention Act**

Selected Areas of State Legislation

- Identity theft protection
- Data security
- Security breach notification
- Social security number protection
- Marketing
- Spyware and adware
- Radio frequency identification devices
- Insurance
- Vehicle data event recorders
- Background checks
- Privacy statements

Federal Legal Requirements

Federal privacy/security requirements imposed under law, few examples:

- Gramm, Leach Bliley (GLBA) – financial privacy
- Health Insurance Portability and Accountability Act (HIPAA) – health information
- Family Educational Rights and Privacy Act (FERPA) – education records
- Children's Online Privacy Protection Act – (COPPA) – online information about children under the age of 13
- Fair Credit Reporting Act (FCRA)
- Drivers Privacy Protection Act (DPPA)

State Legal Requirements

Michigan examples:

- Identity Theft Protection Act 452 of 2004 (http://www.legislature.mi.gov/(S(rbn0j5eyd5wdtjjh0rwzfsyq))/mileg.aspx?page=getObject&objectName=mcl-Act-452-of-2004&highlight=identity%20AND%20theft
- Breach notification Excerpt: http://www.legislature.mi.gov/(S(reea1zi3i4nayj1emkoo2bf0))/mileg.aspx?page=GetObject&objectnam**e=mcl-445-72**
- Social Security Number Privacy Act https://www.michigan.gov/documents/Social_Security_Number_Privacy_Act_118553_7.pdf
- Internet Privacy Protection Act https://www.legislature.mi.gov/documents/2011-2012/publicact/htm/2012-PA-0478.htm
- Surveillance of or distribution, dissemination, or transmission of recording, photograph, or visual image of certain bodily parts of an individual having reasonable expectation of privacy http://www.legislature.mi.gov/(S(u5klkyak4svsdij5p20k4zrr))/mileg.aspx?page=GetObject&objectname=mcl-750-539j

Contracts

- Client specific requirements
- Payment Card Industry –Data Security Standards
- Business Associate Agreements
- Client security assessments
- EU Standard Contractual Clauses for cross border data transfers

Discussion Hypo

Business keep improving

There is more work then can be handled with existing staff

The firm has expanded to 10 lawyers with added support staff

Added staff requires additional equipment

What does she need to do now?

Steps to Take to Protect Information

With new personnel it is essential to maintain a training program:

- New employees should receive training before being granted access to information
- Existing employees should receive training to stay current with firm practices

Steps to Take to Protect Information

If you do not have deep technical expertise, engage a consultant. In many cases you may want to engage one even if you have the expertise to:

- Do things you can't or shouldn't (efficient use of time)
- Help establish a security program
- Have them test your security program

Steps to Take to Protect Information

Conduct an inventory of:

- All hardware that may be connected to your office network or the internet
- Software applications
- Online services
- Assess security implications of each

Steps to Take to Protect Information

Consider data types and flows:

- Who creates it
- Where is it stored
- Sharing data outside the firm
- Client imposed security standards
- Federal contractor compliance

Steps to Take to Protect Information

Investigate security of remote services:

- For Cloud providers understand how they operate
  - own servers
  - out sourced to whom what security, backup capabilities
- Physical service providers
  - Cleaning
  - Equipment servicing

Steps to Take to Protect Information

- Establish a cybersecurity policy and follow it
- Inform employees of what to do and what not to do
- Provide training
- Specify and limit access to on site servers
- Create password standards and consider password protection software
- Use two factor authentication
- In the office use a wired connection rather than Wi-Fi
- Use encryption

Steps to Take to Protect Information

- Create and enforce employee access restrictions – Need to know basis and least privileged access
- Use antivirus protection
- Prohibit installation of programs without prior authorization
- Provide and malware training to not open email attachments or click link if email unusual out of the ordinary from unrecognized sources
- Test your policy

Steps to Take to Protect Information

- Use secure methods to handle sensitive information
- No email transfers to home computers
- Do not store sensitive information on portable devises
- Use lock out tools to lock down access after specified number of logon attempts)
- Install remote data wipe capabilities

Steps to Take to Protect Information

- Require encryption on all devices with sensitive data
- If sensitive documents are transferred by email at a minimum password protect them
- Establish and honor client desires on use of encryption
- Careful with use of mobile devices - free Wi-Fi may be costly in terms of security
- Use VPN

Steps to Take to Protect Information

- Establish a back-up system
- Check on cloud providers back up and recovery capabilities
- If storing information on local devices only consider also storing on cloud
- Conduct periodic diagnosis of hardware to check for warnings of failure
- Keep duplicate infomration on an online back-up site
- Have an Incident Response Plan and periodically test it

Steps to Take to Protect Information

- Establish a records management policy
- Provide new hire and ongoing employee training
- Limit access to information on a need to know basis
- Consider insurance cover for disasters
  - Understand to coverage and limitation
  - Determine if and the amount of restoration services provided

Steps to Take to Protect Information

Website

- Use appropriate and adequate security
- Where hosted, verify service provider's security protocols
- Use a firewall
- If website site provides for two way communication, use robust security and obtain outside confirmation where needed

Incident Response and Breach Notification Requirements

Breach Notification Laws

- Designed to help enforce security obligations
  - In theory helps consumers protect themselves
  - Provides government authorities enforcement opportunities
  - Bad PR and breach-associated costs encourage compliance
- Breaches generally triggered by the unauthorized access to, or acquisition of, personal data covered by the law
- Other variables affect whether a breach notification law applies such as:
  - Storage medium involved
  - Use of data encryption

PAI

Federal Breach Notification: (GLBA)

Regulations adopted by financial regulators and the FTC pursuant to GLBA include breach notification provisions for unauthorized access to sensitive customer information held by banks and other financial institutions.

Federal Breach Notification: HIPAA (HITECH)

- Written notices must be provided within 60 days after *discovery* of the breach
  - Law enforcement delay if notification would impede a criminal investigation or damage national security
  - Content requirements
- A covered entity must notify:
  - HHS of any breach involving more than 500 individuals when it provides consumer notice
  - HHS annually of breaches involving fewer than 500 individuals
  - Prominent media in a state of breaches involving more than 500 residents of the state

PAI

Federal Breach Notification: HIPAA (HITECH)

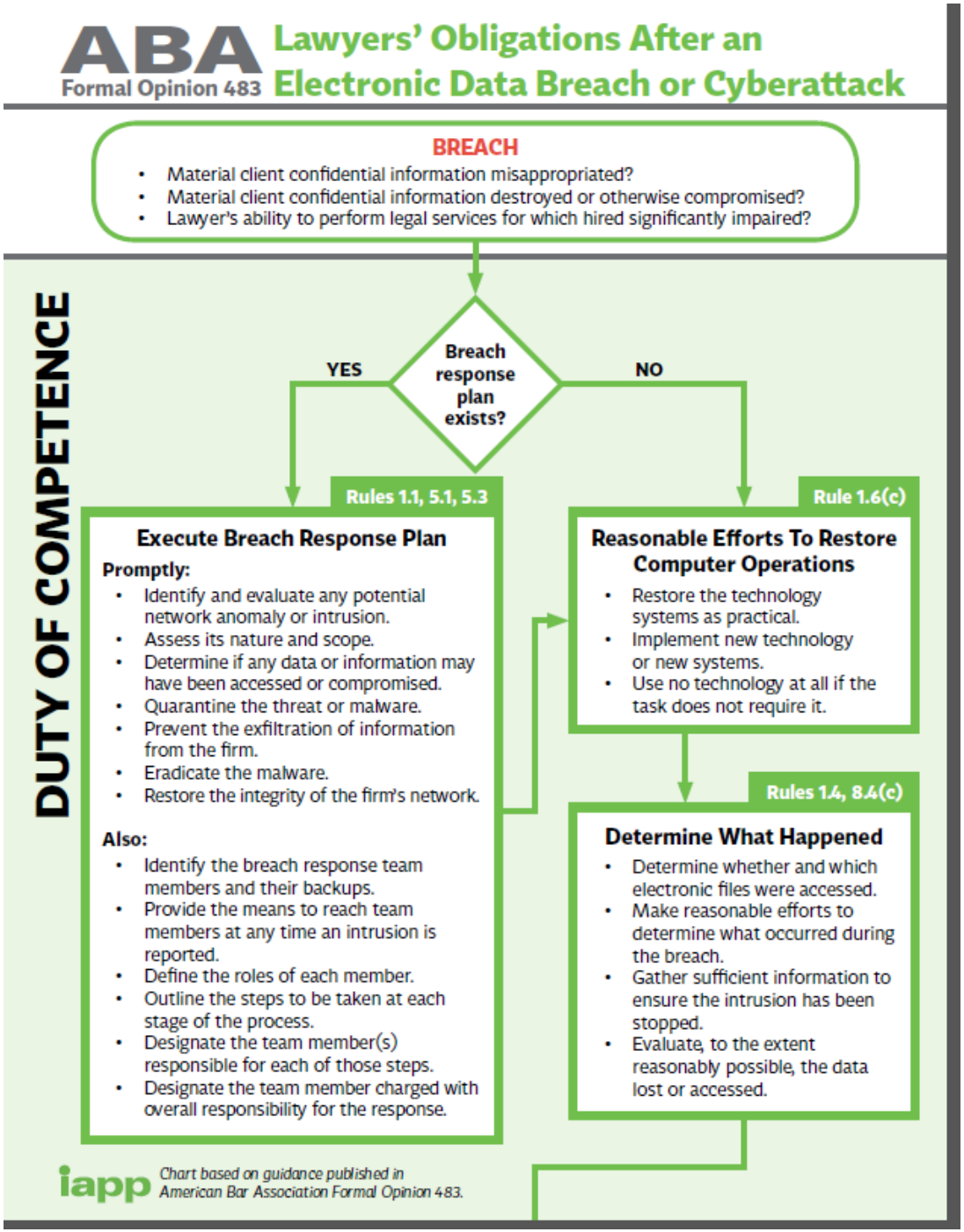
- A Business Associate that discovers a breach must notify the covered entity
- Similar FTC rule for Vendors of personal health records and entities offering products or services through Web site of a vendor of personal health records

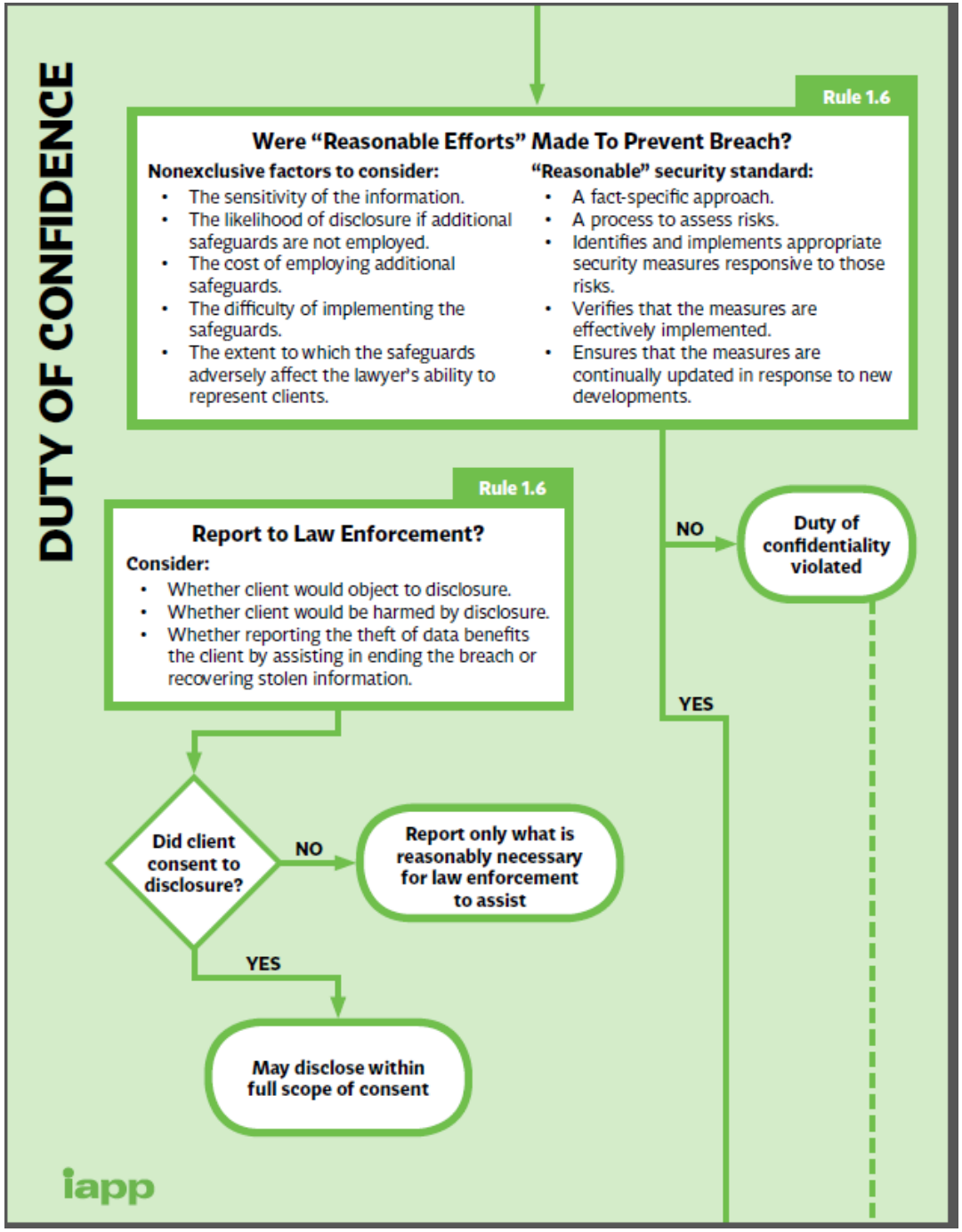
U.S. State Breach Notification Laws

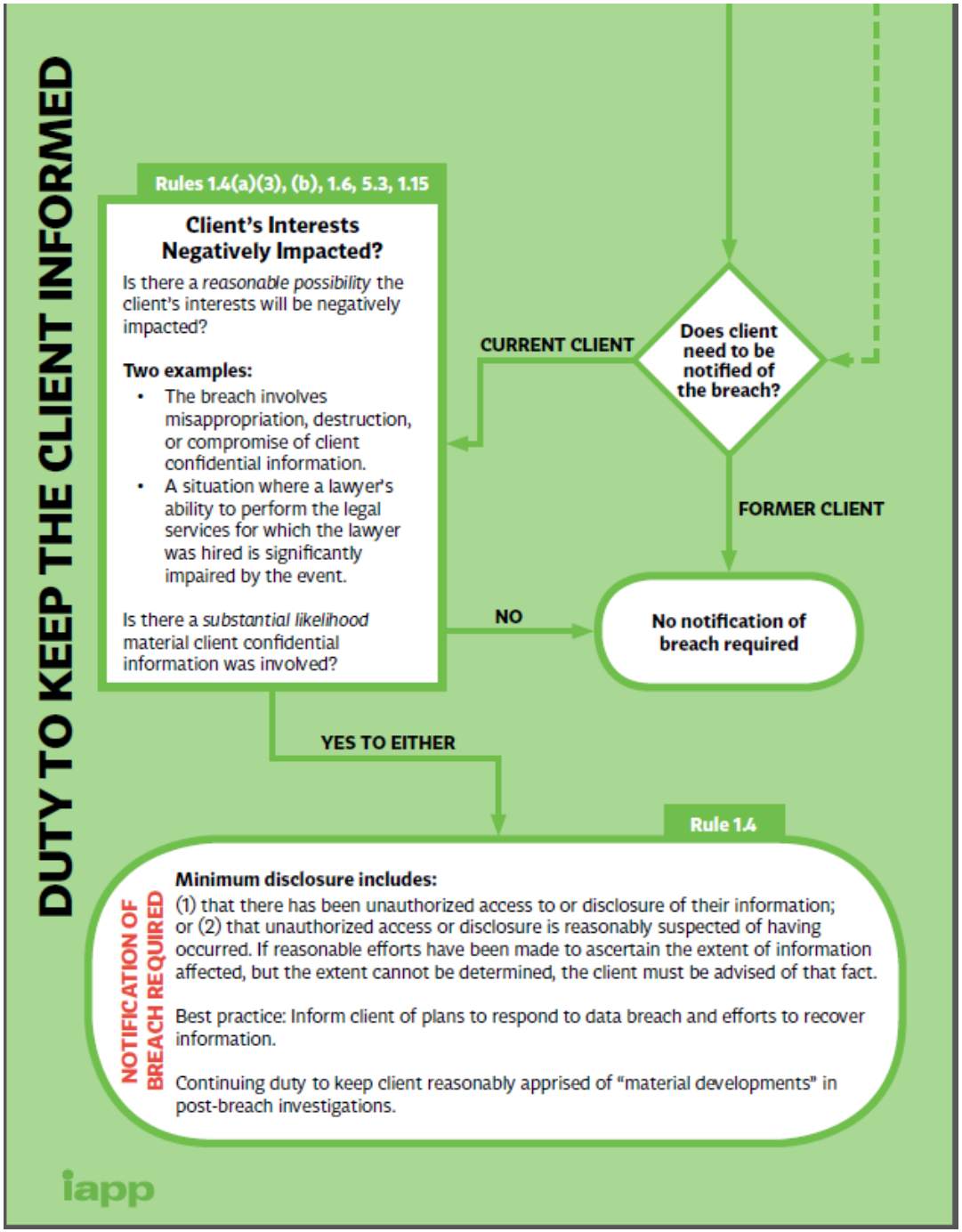
All 50 states, District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands with laws:

- PI usually covered: name plus SSN, driver's license number, bank account information with PIN, or health information (often with an exception when encrypted), and there are significant state variations of covered PI
- Notice to individuals required in the event of a breach and, in some instances, notice to credit-reporting agencies and/or regulators *(e.g.*, New York Attorney General, New Jersey State Police) also specified
- A significant number of states impose requirements with respect to the content of the consumer notice
- State Insurance regulators also impose notification requirements on insurance companies

Breach Incident ABA Guidance


ABA
Formal Opinion 483
Lawyers' Obligations After an Electronic Data Breach or Cyberattack
BREACH
Material client confidential information misappropriated?
Material client confidential information destroyed or otherwise compromised?
Lawyer's ability to perform legal services for which hired significantly impaired?
DUTY OF COMPETENCE
Breach response plan exists?
YES
NO
Rules 1.1, 5.1, 5.3
Execute Breach Response Plan
Promptly:
Identify and evaluate any potential network anomaly or intrusion.
Assess its nature and scope.
Determine if any data or information may have been accessed or compromised.
Quarantine the threat or malware.
Prevent the exfiltration of information from the firm.
Eradicate the malware.
Restore the integrity of the firm's network.
Also:
Identify the breach response team members and their backups.
Provide the means to reach team members at any time an intrusion is reported.
Define the roles of each member.
Outline the steps to be taken at each stage of the process.
Designate the team member(s) responsible for each of those steps.
Designate the team member charged with overall responsibility for the response.
Rule 1.6(c)
Reasonable Efforts To Restore Computer Operations
Restore the technology systems as practical.
Implement new technology or new systems.
Use no technology at all if the task does not require it.
Rules 1.4, 8.4(c)
Determine What Happened
Determine whether and which electronic files were accessed.
Make reasonable efforts to determine what occurred during the breach.
Gather sufficient information to ensure the intrusion has been stopped.
Evaluate, to the extent reasonably possible, the data lost or accessed.
iapp
Chart based on guidance published in American Bar Association Formal Opinion 483.


DUTY OF CONFIDENCE
Rule 1.6
Were "Reasonable Efforts" Made To Prevent Breach?
Nonexclusive factors to consider:
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.
The extent to which the safeguards adversely affect the lawyer's ability to represent clients.
"Reasonable" security standard:
A fact-specific approach.
A process to assess risks.
Identifies and implements appropriate security measures responsive to those risks.
Verifies that the measures are effectively implemented.
Ensures that the measures are continually updated in response to new developments.
NO
Duty of confidentiality violated
YES
Rule 1.6
Report to Law Enforcement?
Consider:
Whether client would object to disclosure.
Whether client would be harmed by disclosure.
Whether reporting the theft of data benefits the client by assisting in ending the breach or recovering stolen information.
Did client consent to disclosure?
NO
Report only what is reasonably necessary for law enforcement to assist
YES
May disclose within full scope of consent
iapp


DUTY TO KEEP THE CLIENT INFORMED
Rules 1.4(a)(3), (b), 1.6, 5.3, 1.15
Client's Interests Negatively Impacted?
Is there a *reasonable possibility* the client's interests will be negatively impacted?
Two examples:
• The breach involves misappropriation, destruction, or compromise of client confidential information.
• A situation where a lawyer's ability to perform the legal services for which the lawyer was hired is significantly impaired by the event.
Is there a *substantial likelihood* material client confidential information was involved?
Does client need to be notified of the breach?
CURRENT CLIENT
FORMER CLIENT
NO
No notification of breach required
YES TO EITHER
Rule 1.4
NOTIFICATION OF BREACH REQUIRED
Minimum disclosure includes:
(1) that there has been unauthorized access to or disclosure of their information; or (2) that unauthorized access or disclosure is reasonably suspected of having occurred. If reasonable efforts have been made to ascertain the extent of information affected, but the extent cannot be determined, the client must be advised of that fact.
Best practice: Inform client of plans to respond to data breach and efforts to recover information.
Continuing duty to keep client reasonably apprised of "material developments" in post-breach investigations.
iapp

Resources

- ***ABA* Model Rules of Professional Conduct *Client-Lawyer Relationship* Rule 1.1 Competence**
  http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence.html
- ***ABA* Model Rules of Professional Conduct *Client-Lawyer Relationship* Rule 1.1 Competence – Comment [8]**
  http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/comment_on_rule_1_1.html
- ***ABA* Model Rules of Professional Conduct - *Client-Lawyer Relationship* Rule 1.6: Confidentiality of Information**
  http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information.html
- ***ABA* Model Rules of Professional Conduct *Law Firms And Associations* Rule 5.1: Responsibilities of a Partner or Supervisory Lawyer**
  http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_5_1_responsibilities_of_a_partner_or_supervisory_lawyer.html

PAI

Resources

- ***ABA* Model Rules of Professional Conduct *Law Firms And Associations* Rule 5.3 Responsibilities Regarding Non-lawyer Assistance**
  http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_5_3_responsibilities_regarding_nonlawyer_assistant.html
- **State Bar of Arizona Ethics Opinions 09-04: Confidentiality; Maintaining Client Files; Electronic Storage; Internet** 12/2009
  http://www.azbar.org/Ethics/EthicsOpinions/ViewEthicsOpinion?id=704
- **Michigan Rules of Professional Conduct**
  https://courts.michigan.gov/Courts/MichiganSupremeCourt/rules/Documents/Michigan%20Rules%20of%20Professional%20Conduct.pdf

- **See also**
- ABA Formal Opinion 99-413 Protecting Confidentiality of unencrypted email
- ABA Formal Opinion 08-451 Lawyer's obligations when Outsourcing Legal and Non-legal Support Services
- ABA Formal Opinion 10-457 Lawyer Websites
- ABA Formal Opinion 11-459 Duty to Protect the Confidentiality of Email Communications With One's Clients

PAI

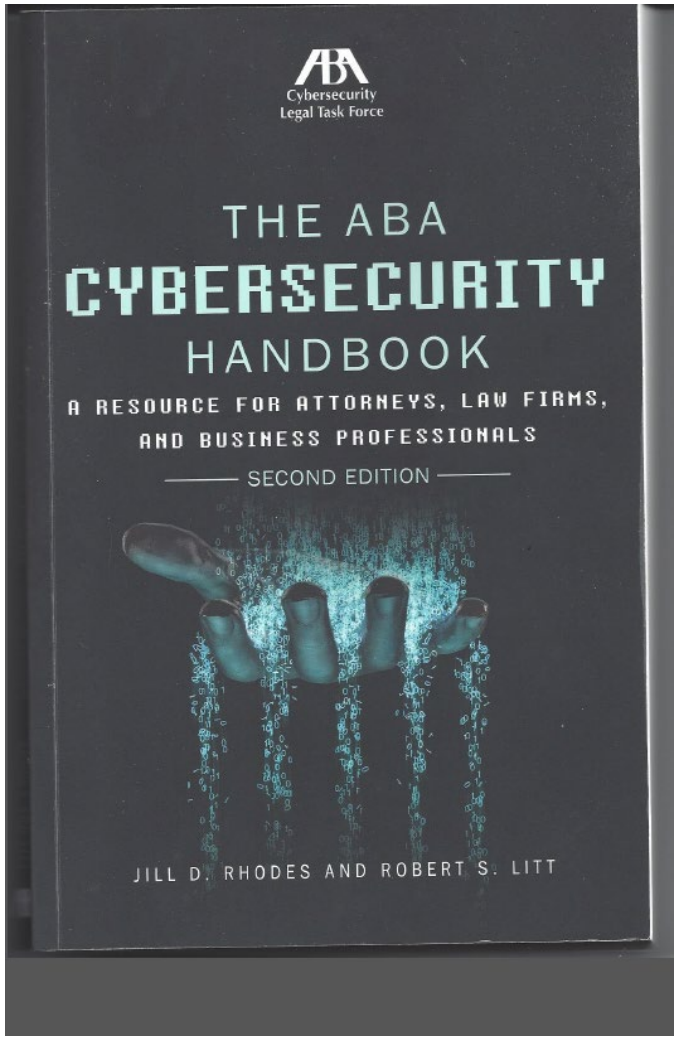
Resources

- **See also**
- ABA Formal Opinion 99-413 Protecting Confidentiality of unencrypted email
- ABA Formal Opinion 08-451 Lawyer's obligations when Outsourcing Legal and Non-legal Support Services
- ABA Formal Opinion 10-457 Lawyer Websites
- ABA Formal Opinion 11-459 Duty to Protect the Confidentiality of Email Communications With One's Clients
- ABA Formal Opinion 17-477 Securing Communication of Protected Client Information
- ABA Formal Opinion 18-480 Confidentiality Obligations for Lawyer Blogging and other public Commentary
- ABA Formal Opinion 18- 482 Ethical Obligations Related to Disasters
- ABA Formal Opinion 18-483 Lawyers' Obligations After an Electronic Data Breach or Cyber Attack

- **IAPP**
  https://iapp.org/media/pdf/resource_center/ABA_Data_Breach_Response_Flowchart.pdf

PAI

Resources


ABA
Cybersecurity
Legal Task Force
THE ABA
CYBERSECURITY
HANDBOOK
A RESOURCE FOR ATTORNEYS, LAW FIRMS,
AND BUSINESS PROFESSIONALS
SECOND EDITION
JILL D. RHODES AND ROBERT S. LITT

Contact Information

Robert L. Rothman

Privacy Associates International LLC

rrothman@privassoc.com

www.privassoc.com

(248) 880-3942

Keith A. Cheresko

Privacy Associates International LLC

kcheresko@privassoc.com

www.privassoc.com

(248) 535-2819