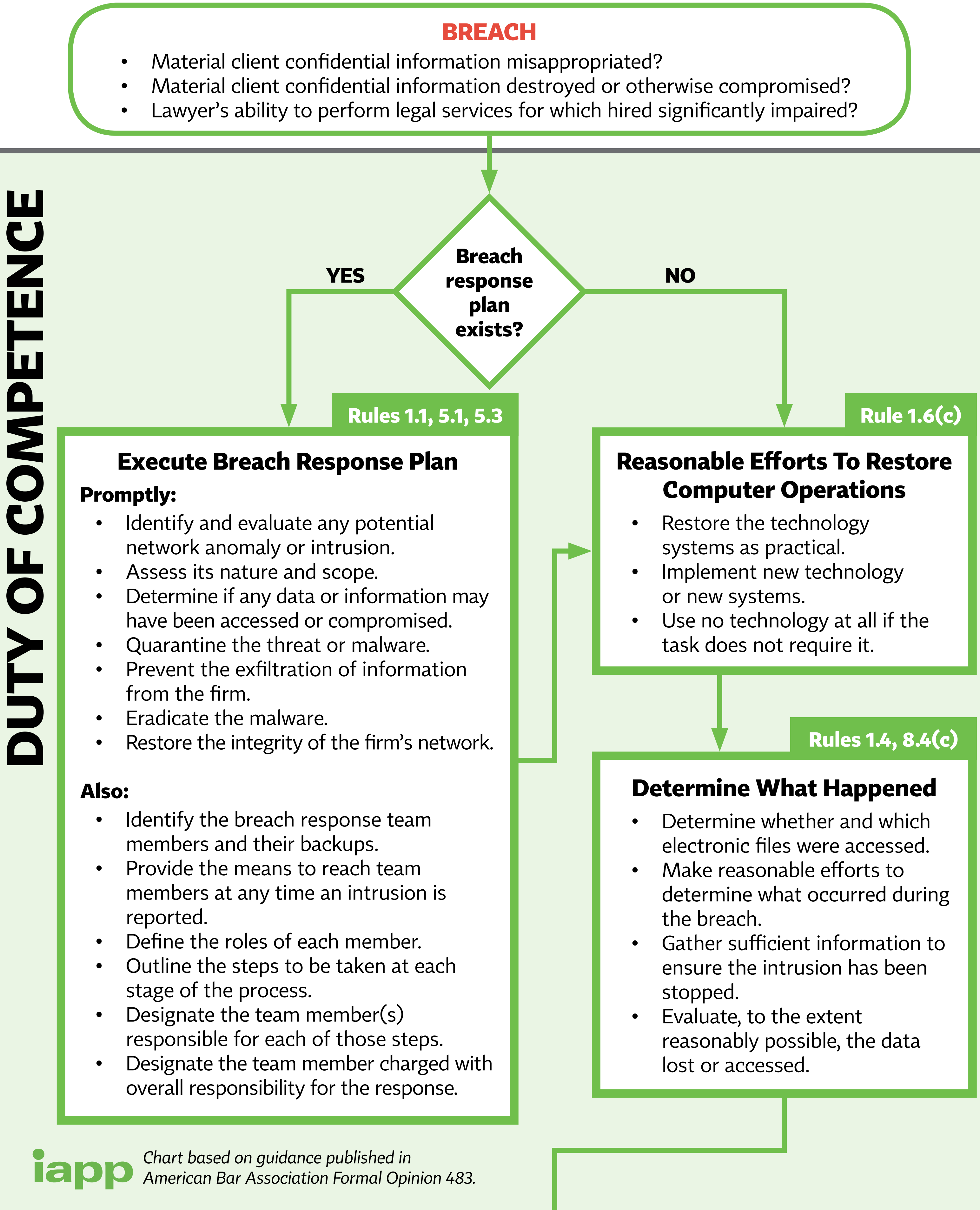
ABA Formal Opinion 483

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.

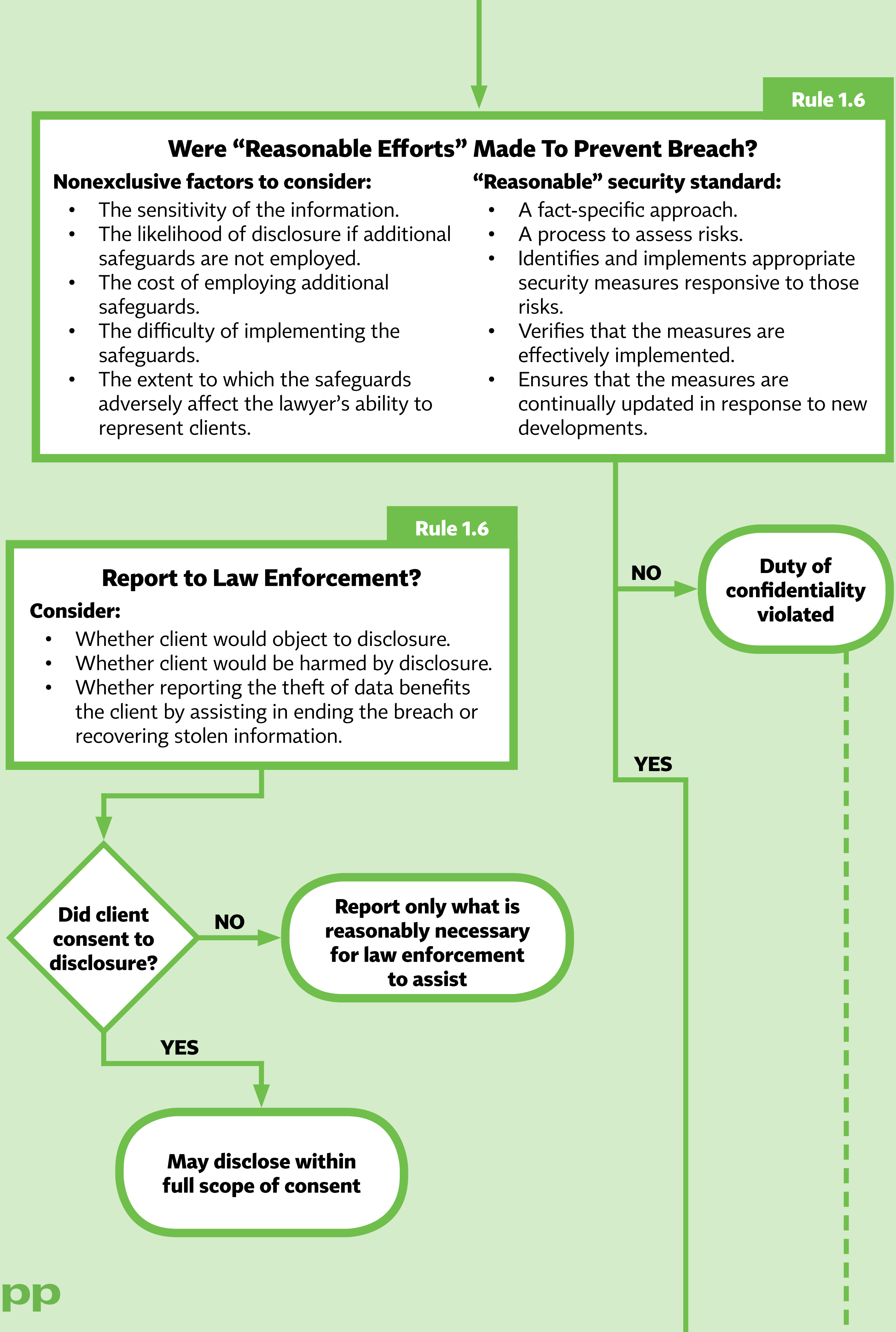
Rules 1.4, 8.4(c)

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?

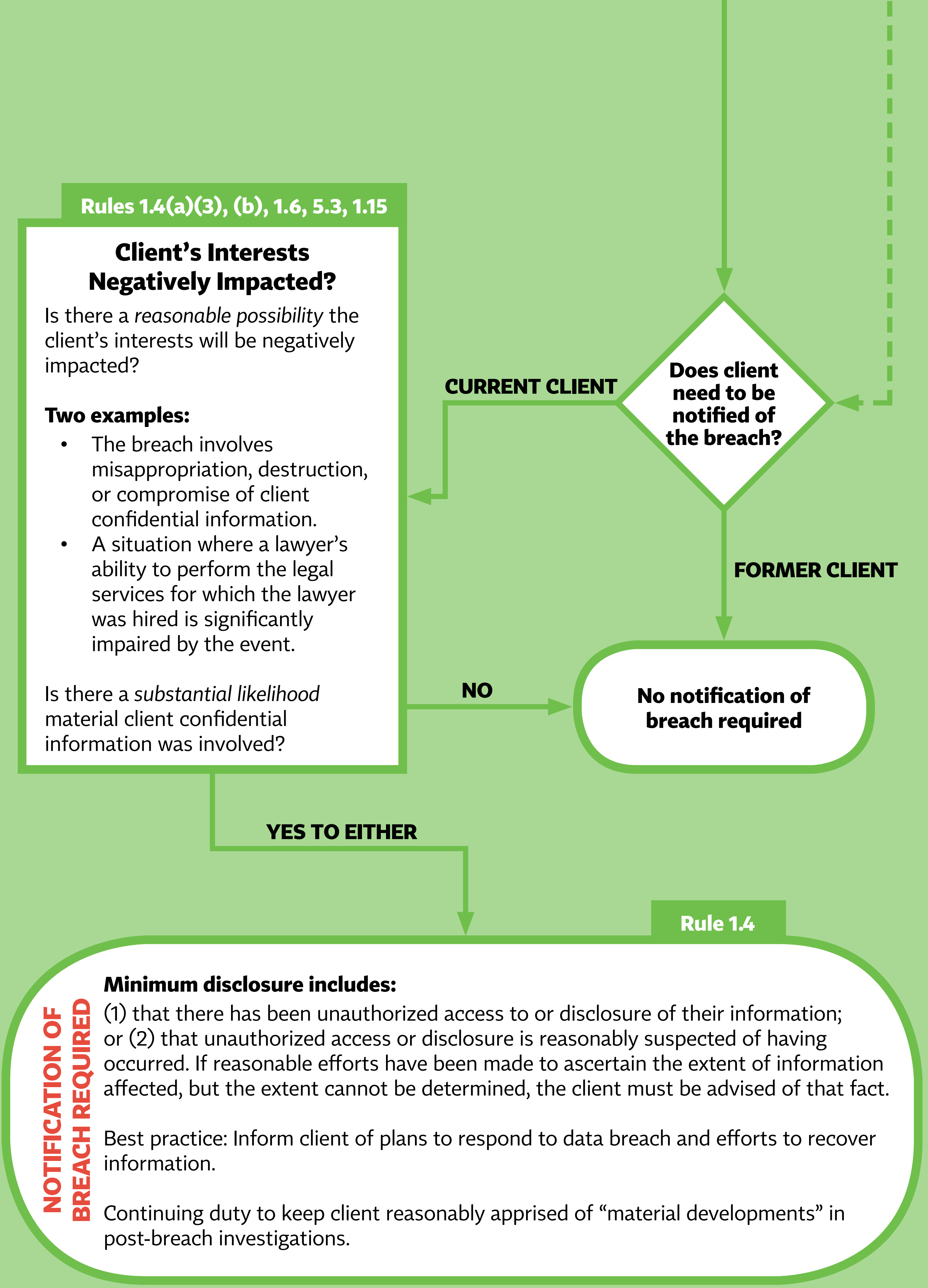
NO

Report only what is reasonably necessary for law enforcement to assist

YES

May disclose within full scope of consent

DUTY TO KEEP THE CLIENT INFORMED



Does client need to be notified of the breach?

CURRENT CLIENT

FORMER CLIENT

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?

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