CA BAR · LAW FIRMS

# The Small-Firm Lawyer's Client-Confidentiality Cheat Sheet

*What California's confidentiality and technology-competence rules now expect of the systems holding your client files, for a 1–10 attorney firm in SW Riverside County. On one page, no fluff.*

You already know Rule 1.6 cold. What changed is that your duty to protect client confidences now expressly reaches the that stores and transmits them, and most small firms have never had that layer independently checked. Here's the picture, so you can ask the right questions before a breach or a bar complaint asks them for you.

## 1 The Mandate: What Rules Actually Apply

**Your obligation here is ethical, not statutory, which makes it broader, not narrower. No fine schedule. The standard is reasonableness, and you answer for it.**

- **Rule 1.6 + Bus. & Prof. Code §6068(e)(1): duty of confidentiality.** "Maintain inviolate the confidence... preserve the secrets" of your client, read to require **reasonable efforts to prevent unauthorized access to and disclosure of** information relating to the representation, including the electronic version.
- **Rule 1.1, Comment [1]: duty of technology competence.** Effective **March 22, 2021**, competence expressly includes keeping abreast of the "benefits and **risks associated with relevant technology**." Competence now reaches your tech stack.
- **Cal. State Bar Formal Op. No. 2010-179**: using technology to store/transmit confidential client info requires **reasonable steps** against undue risk of disclosure, *ongoing*, not a one-time setup. Competence may be met by **associating with a qualified outside specialist.**
- **Cal. State Bar Formal Op. No. 2020-203**: a **data breach can trigger an ethical duty to investigate and notify** affected clients, and mishandled client info can itself give rise to a malpractice claim.
- **CCPA / CPRA** may also apply to larger/higher-revenue firms, a separate statutory layer.

**Plain English:** there is **no checklist that makes you "compliant."** Your risk is having to explain, after the fact, why your safeguards were *reasonable*: to the Bar, a malpractice carrier, and a client whose file got out.

*A general summary of published rules and opinions, not our interpretation of how they apply to your firm. That's your call, or your ethics counsel's.*

## 2 What "Reasonable" Actually Looks Like

**The questions you have to be able to answer:**

- **Know where client confidences live and how they're protected**: practice-management and document systems (Clio, MyCase, PracticePanther, NetDocuments, iManage), email, local files, backups. You can't protect what you haven't mapped.
- **Reasonable security controls, on by default**: encryption (devices, backups, email in transit), **unique logins + MFA** (no shared firm password), least-privilege access, audit logging.
- **Vendor diligence**: confirm cloud/IT providers offer security and confidentiality terms consistent with your duties (Op. 2010-179 puts that judgment on the attorney).
- **Supervision of staff and outside help (Rule 5.3)**: duty extends to non-lawyer staff and vendors; written expectations + training, with proof.
- **A breach-response plan before you need one**: who investigates, how you scope affected clients, how you notify.
- **An ongoing review, not a one-time setup**: technology and threats change; the obligation recurs.

**The SSS throughline:** this is the **technical layer we own for you.** You hold the client relationship and the legal judgment; we run the safeguards, document them, and hand you what you'd need to show your diligence was reasonable.

## What It Costs to Get This Wrong

The exposure is not a fine; it's worse.
No per-violation schedule; the consequences are open-ended and personal.

**There's no per-violation penalty schedule; the consequences are open-ended and land on *you personally*:**

- **State Bar discipline.** A confidentiality/competence failure can be charged as misconduct: **reproval → suspension → disbarment.** Your license, not a dollar amount.
- **Legal-malpractice civil liability.** Per Op. 2020-203, mishandled confidential information can be an error giving rise to a malpractice claim: damages, carrier, premiums all in play.
- **Mandatory client breach notification.** Beyond the ethical duty, **California's data-breach statute (Civil Code §1798.82)** requires notice to affected residents; as amended by **SB 446 (effective January 1, 2026)**, that notice must go out **within 30 calendar days** of discovery, with a sample notice to the Attorney General within 15 days for breaches affecting more than 500 residents.
- **Reputational damage and client loss.** A small firm runs on referrals and trust. "My lawyer lost my file to hackers" is the story that doesn't survive in a tight local bar.

## Why "Reasonable, Documented, Ongoing" Is the Only Defense

There's no fine schedule to point at, which cuts the other way. When a client file gets out, the question isn't "did you breach a number," it's *"were your safeguards reasonable, and can you show it?"* You answer that to the State Bar, your malpractice carrier, and the client: after the fact, under pressure, with whatever documentation you actually kept.

**Honest bottom line:** there's no cap and no safe-harbor dollar figure, which is exactly why "reasonable, documented, and ongoing" is the only defense. The firms that get hurt never had the technical layer looked at.

### BUT WHAT ABOUT...

**"Our IT guy / PM vendor handles this."**

Two different jobs. IT keeps the computers running; your vendor (Clio, MyCase, NetDocuments) secures *their* platform, not your network, devices, backups, email, or who still has access after someone leaves. The Rule 1.6 duty is *yours*. Ask: *"Can you show me, in writing, that our client data is encrypted on every device and that our backups would actually restore?"* No document = no answer, just an assumption.

**"We're a small firm. Who'd come after us?"**

A data incident starts with *your own client* asking what happened, and a bar inquiry or malpractice claim asking whether your safeguards were reasonable. Firm size doesn't change the duty; it just means most small firms have never had the technology side checked. (We're a small local shop ourselves, built for firms your size, not the 200-lawyer downtown crowd.)

## Not sure whether your firm's safeguards would hold up as "reasonable"? Find out for free.

We'll run a **free technical security review** of your firm: a local specialist looks at your actual setup (network, backups, EDR, email, MFA, who can access what, and how client data flows through Clio / MyCase / NetDocuments and your other tools) and gives you a **plain-English findings list**: where your technical safeguards are solid and where the gaps are. This is an IT assessment, **not a legal-ethics opinion and not legal advice**; you keep that judgment. No sales pitch, no obligation. **We never ask to see privileged or client information** on the call.

**Book your free security review →**

**simonsayssystems.com/law-firm-review · or call/text Craig direct: (951) 717-3576**

*Local to Menifee. Remote-first, on-site across Temecula, Murrieta, Wildomar, Lake Elsinore & Sun City.*