

It's Not 1996 Anymore

Plaintiff LNCs Must Protect Patient Privacy Too

Katy Jones, MSN, RN, LNC

LNctips®

Version 1.0 — February 2026

© 2026 LNctips®

INTRODUCTION

HIPAA may be nearly 30 years old, but it doesn't cover all health data — and it was never designed to. HIPAA applies to covered entities (healthcare providers, health plans, clearinghouses) and their business associates, which includes defense law firms, defense experts, and independent LNCs working for the defense.

But plaintiff-side LNCs aren't exempt from privacy obligations. They're simply governed by a *different* set of rules: **state-level privacy laws**, many of which were passed long after HIPAA and are often stricter.

These laws apply to **anyone** handling personally identifiable information (PII) — including medical data — regardless of whether HIPAA applies. That means plaintiff LNCs must still protect patient privacy, even if they're not business associates under HIPAA.

Here's how the two frameworks compare:

Aspect	HIPAA	State Privacy Laws ¹
Who Must Comply?	Covered entities and business associates (e.g., healthcare providers, defense LNCs)	Any party handling PII/medical data (e.g., plaintiff LNCs, defense LNCs, small businesses)
Protected Information	PHI (Protected Health Information)	PII (includes medical data, name, SSN, driver's license, account numbers, etc.)
Notification Requirements	Breach notification to affected individuals, HHS, and sometimes media	Varies by state; may require quicker and broader notifications
Penalties	\$10,000–\$50,000 per HIPAA violation	Up to \$250,000 per incident in some states ^{2,3}
Safe Harbor (Encryption)	Encryption may exempt from breach notification	Many states recognize encryption as a safeguard, reducing liability

WHY STATE LAWS MATTER MORE TODAY

HIPAA is a federal law from 1996 — and it hasn't kept pace with how health data is stored, shared, or breached today. In response, many states have passed **modern, consumer-oriented privacy laws** that fill the gaps HIPAA never covered.

Most states enforce these laws through their Attorneys General, who can investigate breaches and issue fines. But in at least one state — **Washington**⁴ — certain privacy laws allow patients to sue directly under narrowly defined circumstances.

This means that even if HIPAA doesn't apply to you, **state law absolutely does**, and the consequences can be significant.

The bottom line is simple: even if HIPAA doesn't apply to your role, privacy obligations absolutely do. Modern state laws, evolving technology, and rising expectations mean LNCs can't rely on assumptions that date back to 1996. Fortunately, protecting patient information doesn't require complex systems or expensive tools — it requires awareness, consistency, and a few practical safeguards. Here are the best practices every LNC should be following today.

BEST PRACTICES FOR LEGAL NURSE CONSULTANTS

1. Encryption

Encrypt your hard drive to scramble data, making it unreadable if your device is lost or stolen. This is a critical defense against data breaches and may qualify you for Safe Harbor protections under both HIPAA and state laws.

For Mac: Use FileVault (built-in encryption).

For Windows: Use built-in BitLocker.

If those don't work for you, both Mac and Windows users can use VeraCrypt (free and robust).

Real-World Example: If your encrypted laptop is stolen from your car, most state laws and HIPAA may not require you to notify affected patients because the data is considered "secured." Without encryption, you could face breach notifications, civil liability, and loss of credibility.

2. Confidentiality Practices

Treat all case materials as confidential by default—regardless of their source or whether HIPAA applies. Never assume you're exempt from safeguarding requirements.

- Restrict access to only those directly involved in the case.
- Never share records with unauthorized individuals, including family or colleagues not retained on the case.
- Do not reuse case examples containing PHI or PII for education or marketing.

3. Secure Storage

Use strong safeguards for both digital and physical records:

- Digital: Password-protected, case-specific folders; enable multifactor authentication.
- Physical: Locked cabinets and desks; no records left out in shared spaces.
- Destroy printed records via shredding when no longer needed.
- Avoid unencrypted USB drives and personal cloud accounts with weak security, such as personal or family OneDrive accounts.

4. Secure Transmission

Always use encrypted portals (e.g., ShareFile) for file transfers. Avoid regular email attachments unless encrypted, never send records via text message or public file-sharing links (e.g., Google Drive, Dropbox, iCloud, Microsoft OneDrive), and ensure access controls are in place.

5. Attorney-Client Privilege and Work Product

Clearly label drafts and summaries as **Confidential Attorney Work Product**. Only share work product as directed by counsel and avoid discussing case details in public or semi-public places (e.g., elevators, cafeterias).

6. AI and Technology Use

Do not input identifiable medical records information into public AI tools (such as ChatGPT, Microsoft Copilot, or Google Gemini). These platforms may incorporate the data into their learning models, resulting in a breach of patient confidentiality.

7. Court Orders and Compliance

Always comply with court orders, confidentiality agreements, and discovery stipulations. If none have been provided, proactively request them from counsel. Violations can lead to severe penalties—including contempt of court and fines up to \$250,000 per incident under some state laws.

8. Case Closure: Retention and Destruction of Records

Confirm with counsel whether to retain or destroy records at the end of a case. For destruction:

- Printed records: Use cross-cut shredding, burning, pulping, or pulverizing.
- Electronic media: Physically destroy thumb drives (e.g., pulverization, melting).

- Hard drives: It is not enough to delete electronic medical records and then empty your recycle bin. You should sanitize your hard drive by securely overwriting data using operating system tools (e.g., Windows Disk Management, macOS Disk Utility) or third-party software (e.g., DBAN).

9. Documentation and Evidence of Compliance

Keep simple documentation of your privacy practices, incident response plans, and proof of secure storage and transfer methods. Even a one-page checklist can protect you if your practices are ever questioned.

- Example: “My hard drive is encrypted using VeraCrypt.”
- “All medical records are in password-protected, case-specific folders.”
- “I use ShareFile for all medical records file transfers.”

10. Mentoring Guidelines: Safe Training with Real Records

Never share actual medical records unless they have been fully de-identified by removing all 18 HIPAA/PII identifiers, such as names, addresses, medical record numbers, and dates directly related to the individual, to ensure patient privacy. Each identifier can potentially reveal a patient’s identity, so it is critical to remove them all to comply with privacy regulations. Be aware that, in addition to medical records, photographs of faces, birthmarks, scars, and tattoos are considered PHI/PII. Once records are de-identified, they are no longer considered PHI/PII. If dates are essential for understanding timelines, use relative labels (e.g., “Day 1,” “Day 2”) instead of actual dates to preserve educational value while staying compliant. Using real, de-identified medical records can be especially helpful for new LNCs, who may be accustomed to a small number of screens to input electronic data and might not realize how extensive printed electronic medical records can be.

Summary: Stay Informed, Stay Secure

Both HIPAA and state privacy laws require LNCs to protect patient data through robust safeguards, secure handling, and clear documentation. State laws may be stricter and carry higher penalties. Following these best practices minimizes your risk, enhances your credibility, and demonstrates your commitment to patient confidentiality.

¹ List of State Privacy Laws. <https://tinyurl.com/4psy9e9c> - accessed February 2026

² \$250,00 per incident – California. <https://tinyurl.com/mumbkv2f> - accessed February 2026

³ \$250,00 per incident – Texas. <https://tinyurl.com/yzd2m3bc> - accessed February 2026

⁴ Washington. <https://tinyurl.com/2puf97r4> - accessed February 2026

LNCTips®