THE MONTHLY PUBLICATION FOR CAP MEMBERS

CAPsules®

COOPERATIVE OF AMERICAN PHYSICIANS

Case of the Month

When Does a Physician-Patient Duty of Care Arise?

by Christy Oganesyan, MBA-HM

Have you ever wondered what happens if an on-call specialist says no? What if they refuse to accept a transfer, decide not to treat a patient, or perform a procedure? When an emergency physician consults with an on-call specialist about a patient, what legal duties arise?

It is not uncommon for physicians to routinely interact with patients whom they will never personally examine through on-call coverage, curbside consultations, transfer discussions, and interdisciplinary collaboration. In modern medicine, these interactions are essential but can cause confusion about legal responsibilities and the establishment of the physician-patient relationship.

A 2024 California Court of Appeal's decision, *McCurry v. Singh*, further reinforces the longstanding California law on this matter. In *McCurry*, the plaintiffs argued that an on-call interventional cardiologist owed a duty of care to a patient who died while awaiting transfer for a potential cardiac catheterization procedure. The patient had presented to an emergency department that lacked cardiac catheterization capabilities. The attending emergency physician had consulted with an on-call cardiologist at another facility regarding the patient's condition and the possibility of a transfer. After reviewing the information provided, the physician determined the patient was not a candidate for cardiac catheterization. He neither examined the patient nor issued any orders, and declined to accept the transfer.

The trial court granted summary judgment in favor of the cardiologist, and the Court of Appeal upheld the decision. The court concluded that no physician–patient relationship existed because the doctor never affirmatively undertook the patient's care. His involvement was limited to providing consultation, and his refusal to accept the transfer did not create a duty of care.[1]

McCurry confirms that **on-call status and consultation alone do not establish duty**.

How Is the Physician-Patient Relationship Formed?

Medical malpractice cases are formed on the grounds of professional negligence, which requires proof of duty, breach, causation, and damages.[2] Among these elements, we must first look at whether the physician owed a duty to the patient. If no duty exists, the case should fail as a matter of law before any further inquiry can be made into the physician's clinical judgement or standard of care.

The physician-patient relationship is typically established through express or implied consent or

continued on page 2

Continued from page 1

agreement. Express agreement means that a physician affirmatively agrees to treat or diagnose a patient. Implied agreement arises when the physician examines the patient, writes orders, prescribes medication, and conducts other activities related to directing patient care.

> As a general rule, a physician–patient relationship is established when a physician conducts the initial history and physical examination.[3] Some jurisdictions have held that a relationship exists when a physician gives a patient an appointment for a specific medical service,[4] when a physician agrees by telephone to see a patient,[5] or even based on a telephone call for consultation from another physician for their patient.[6] In practice, however, California generally has not found that a mere telephone conversation is enough to establish a physician–patient relationship.[1,7]

In short, the physician-patient relationship is formed when **the patient seeks medical care, and the physician knowingly accepts the responsibility to render care**.

Courts have historically remained consistent when distinguishing between affirmative treatment and informal consultation. If every call from a colleague were enough to create a legal duty, physicians would be reluctant to provide informal guidance, participate in peer review, or provide second opinions. The Courts recognize that expanding physician duty in this manner would have a negative impact on the collaboration between physician specialties and ultimately lead to patient harm.[8]

Does Ethical Impact Mean Legal Duty?

Physicians often conflate ethical obligations with legal duties. While ethical standards may encourage or even expect physicians to assist, they do not always create a legally enforceable duty of care. The American Medical Association states that "a patient-physician relationship exists when a physician serves a patient's medical needs." They specifically emphasize patient welfare and professional cooperation. In some cases, ethical opinions have recognized a limited physician-patient relationship with or without express agreement (i.e., emergencies or court ordered care).[9]

Key Takeaways for Physicians

- A consultation alone does not create a physician–patient relationship or a duty of care. Legal duty arises from affirmative treatment, not merely from the foreseeability of harm.
- Clear documentation distinguishing consultation from treatment is critical.
- On-call and transfer policies should explicitly define when responsibility for patient care begins.
- Physicians should avoid issuing patient-specific orders unless they are prepared to assume duty.

Disclaimer: This content is for general informational purposes only and is not legal advice. You should not act or refrain from acting based on any content included here without seeking the appropriate legal counsel from a licensed attorney in your jurisdiction. The sender and author are not providing legal services or advice.

Christy Oganesyan, MBA-HM, is a Senior Risk Management and Patient Safety Specialist. Questions or comments related to this article should be directed to COganesyan@CAPphysicians.com

[1] *McCurry v. Singh*, (2024) 104 Cal.App.4th 1170. https://law.justia.com/cases/california/court-of-appeal/2024/c098433.html

[2] *Rainer v. Grossman*, (1973) 31 Cal.App.3d 539. https://law.justia.com/cases/california/court-of-appeal/3d/31/539.html

[3] *Kramer v. Policy Holders' Life Insurance Assn*., 5 Cal. App. 2d 380, 382 (Cal. Ct. App. 1935)

[4] *Lyons v. Grether* (Va. 1977) 239 S.E. 2d 103

[5] *Bienz v. Cent. Suffolk Hosp.* (N.Y. App. Div. 1990) 163 A.D. 2d 269

[6] *Mead v. Legacy Health Sys* (2012) 352 Ore. 267

[7] *Barton v. Owen* (1977) 71 Cal.App.3d 484

[8] *Alexander v. Scripps Memorial Hosp. La Jolla*, (2018) 23 Cal.App.5th 206, 235–236. https://law.justia.com/cases/california/court-of-appeal/2018/d071001.html

[9] American Medical Association. Code of Medical Ethics, Opinion 1.1.1. https://code-medical-ethics.ama-assn.org/ethics-opinions/patient-physician-relationships

Ensuring Safe and Compliant Use of Compounded Medications in the Office

by Monica Ludwick, Pharm. D.

The increased use of compounded medications—particularly driven by the glucagon-like peptide-1 (GLP-1) therapies and ketamine assisted psychotherapy—has drawn renewed attention to their role in modern treatment. This trend raises important questions about the legal considerations of using compounded medications when FDA-approved alternatives are available.

Compounded medications play an important role in individualized patient care when an FDA-approved drug is not suitable—for example, when a patient has an allergy to a specific excipient or requires a unique dosage form. In recent years, physicians have also increasingly used compounded medications for convenience and perceived lower cost, particularly for in-office administration and improved patient access. However, compounded drugs carry distinct clinical, quality, regulatory, and liability risks that must be carefully managed. Unlike FDA-approved medications, compounded drugs do not undergo premarket review for safety, effectiveness, or manufacturing quality, increasing the potential for patient harm if standards are not met.[1,2]

1. Regulatory Framework: Federal and California Considerations

Under the federal Food, Drug, and Cosmetic Act, compounded drugs that meet the conditions of section 503A may be exempt from FDA premarket approval and certain manufacturing requirements but remain subject to prohibitions against unsanitary conditions and unsafe practices. Importantly, compounded medications are not FDA-approved, and outbreaks and serious adverse events linked to poor compounding practices in medical offices and clinics have been documented.[1,2]

In California, compounding is governed primarily by the California Board of Pharmacy under Title 16 of the California Code of Regulations. These rules establish expectations for documentation, beyond-use dating (BUD), ingredient control, and storage practices.[3] Although recent regulatory updates clarify that physician practices are exempt from pharmacy licensure requirements, this exemption does not eliminate a physician's responsibility to ensure safe preparation, handling, and use of compounded medications.

Additional California regulations, including those applicable in workers' compensation cases, require clear documentation of medical necessity when compounded drugs are prescribed or dispensed, emphasizing that compounded products should not be used as a convenience substitute for commercially available drugs without justification.[4,5]

2. Quality and Preparation Standards

Medical necessity is a requirement. Compounded medications should be used only when a patient's

continued on page 4

Continued from page 3

specific clinical needs cannot be met by an FDA-approved product. The clinical rationales such as allergies, dosage requirements, or route of administration should be clearly documented in the medical record.[3]

Written procedures are critical. Best practices and California regulations call for written master formulas or procedures describing ingredients, compounding steps, equipment, quality checks, storage requirements, and assigned BUDs.[6] This documentation not only supports patient safety but is also essential for defending care decisions in the event of a claim.

Staff training and oversight matter. Personnel involved in compounding should be appropriately trained and supervised, with competency assessments documented. Even when compounding is limited, lack of training or deviation from recognized standards can significantly increase malpractice exposure.[6]

Physicians should be aware that compounded drugs are not subject to Good Manufacturing Practice (GMP) requirements applicable to commercial manufacturers. Variability in strength, sterility, and stability has been documented, and adverse outcomes may expose both the compounder and the prescriber to liability.[7]

3. Storage and Handling Risks

Improper storage and handling are common sources of risk.

- Environmental controls: Ingredients and finished compounded products must be stored under appropriate temperature, light, and humidity conditions consistent with United States Pharmacopeia (USP) standards and regulatory expectations.[1]
- Labeling and integrity: Containers should be clearly labeled with contents, lot numbers when available, preparation dates, and beyond-use dates. Altered or repackaged products must be relabeled accurately.[1]
- Beyond-use dating: Products should never be used beyond their assigned BUD. Inadequate justification for BUDs is a frequent compliance issue and a vulnerability in litigation.[1]

Failure to follow these practices can result in reduced potency, contamination, or patient injury—outcomes that are often difficult to defend.

4. Documentation, Consent, and Monitoring

From a risk management perspective, documentation is your strongest defense. The medical record should clearly reflect:

- Why a compounded medication was necessary
- Why commercially available alternatives were not suitable
- How and where the medication was prepared or sourced
- Storage conditions and administration details
- For higher-risk compounded products, particularly sterile injectables, physicians should consider an informed consent discussion, explaining that the medication is not FDA-approved and may carry additional risks.[5]
- Practices should also have a process for identifying and responding to adverse events, including internal review and reporting to appropriate regulatory bodies when required.

5. Risk Management Recommendations

To reduce exposure while supporting patient care:

- Limit in-office compounding unless your practice has appropriate facilities, policies, and trained personnel.

continued on page 5

Continued from page 4

- Use reputable, licensed compounding pharmacies or outsourcing facilities whenever possible.
- Collaborate with pharmacists for formulation, storage guidance, and quality assurance.
- Stay current on California regulatory changes, including Board of Pharmacy guidance and documentation requirements.[1-3]
- Confirm that your professional liability coverage applies to the prescribing or manufacturing of compounded medications.

Compounded medications can be clinically appropriate, but they require heightened vigilance. Thoughtful use, careful documentation, and adherence to recognized standards are essential to protecting your patients and your practice.

Monica Ludwick, Pharm.D., is a Senior Risk Management and Patient Safety Specialist. Questions or comments related to this article should be directed to MLudwick@CAPphysicians.com.

[1]California Code of Regulations, Title 16, Section 1735.2. Compounding Limitations and Requirements; Self-Assessment. Accessed December 2025. https://www.law.cornell.edu/regulations/california/16-CCR-1735.2

[2]California Code of Regulations, Title 8, Section 9792.27.9. Compounded Drugs. Accessed December 2025. https://www.dir.ca.gov/t8/9792_27_9.html

[3]California Code of Regulations, Title 8, Section 9789.40.7. Compounded Pharmaceuticals Dispensed by a Physician on or after July 1, 2025. Accessed December 2025. https://www.dir.ca.gov/t8/9789_40_7.html

[4]U.S. Food and Drug Administration. "FDA Highlights Concerns with Compounding of Drug Products by Medical Offices and Clinics under Insanitary Conditions." Accessed December 2025. https://www.fda.gov/drugs/human-drug-compounding/fda-highlights-concerns-compounding-drug-products-medical-offices-and-clinics-under-insanitary

[5]U.S. Food and Drug Administration. "Compounding and the FDA: Questions and Answers." Accessed December 2025. https://www.fda.gov/drugs/human-drug-compounding/compounding-and-fda-questions-and-answers

[6]California Board of Pharmacy. Compounding Regulations and Guidance (16 CCR §§ 1735 et seq.). Accessed December 2025. https://www.pharmacy.ca.gov/publications/compounding_faqs.pdf

[7]Federation of State Medical Boards. White Paper on Physician Compounding. 2020. Accessed December 2025. https://www.fsmb.org/siteassets/advocacy/publications/white-paper-on-physician-compounding-2020-for-posting.pdf

Ask My Practice

by Andie Tena

The Essential Annual Compliance and Regulatory Training Checklist for Every Medical Practice

Staying compliant isn't optional for medical practices. It's essential for protecting patients, staff, and the practice itself. Each year, healthcare teams are required to complete a range of regulatory, safety, and professional conduct trainings that reduce risk, strengthen operational readiness, and ensure the practice meets state and federal requirements. From OSHA and HIPAA to emergency preparedness, CPR, fraud prevention, and workplace violence prevention trainings, these annual and biennial courses create a safer, more secure environment for both staff and patients.

The following checklist outlines the key trainings every medical practice should complete to remain compliant and maintain the highest standard of care.

☐ OSHA Training

- Hazard Communication
- Bloodborne Pathogen
- Personal Protective Equipment (PPE)
- Fire Safety
- Chemical Safety
- Biomedical Waste Management
- Slips, Trips, and Fall Prevention
- Emergency Response Procedures

OSHA training should be conducted annually. CAP members can access discounted OSHA compliance training and more at: **www.evolveelearning.com**. To receive your discount use code **CAP10OFF** at checkout.

☐ HIPAA Training

- Privacy and Security Rules
- Patients' Rights
- Electronic Health Records (EHR) Security
- Breach Notification Procedures

HIPAA training should be done annually. CAP members can access free courses at: **https://cap.nascybernet.com/**

continued on page 7

Continued from page 6

☐ Harassment Avoidance Training

- Prevention
- Reporting Procedures
- Legal Implications

Harassment Avoidance Training should be done every two years for practices with five or more employees (physicians, nurses, nurse practitioners, and physician assistants count as employees). CAP members can access free courses at: **https://register.traliant.com/customer/cooperative/6695/**

☐ Diversity, Equity and Inclusion (DEI) Training

- Unconscious Bias
- Cultural Competency
- Inclusive Leadership

DEI training is optional. CAP members can access free courses at:
https://register.traliant.com/customer/cooperative/6695/

☐ Workplace Violence Prevention Training

- Identifying Warning Signs
- Reporting and Prevention Procedures

Workplace Violence Prevention Training should be done annually. Please contact *My Practice* at **213-473-8630** or via email at **MyPractice@CAPphysicians.com** for training links and discount codes.

☐ Fraud, Waste, and Abuse

- Medicare/Medicaid Fraud Detection
- Proper Billing Practices
- Identifying Red Flags

☐ Emergency Preparedness Training

- Disaster Response Planning
- Business Continuity Procedures
- Evacuation Plans for Different Emergencies

☐ First Aid & CPR Training

- CPR (Adult, Child, Infant)
- Basic First Aid Procedures
- Automated External Defibrillator (AED) Usage

continued on page 8

Continued from page 7

☐ Identity Theft Prevention Training

- Protecting Patient Data and Personal Information
- Recognizing Signs of Identity Theft
- Keeping Sensitive Information Secure

☐ Fire/Evacuation Drill

- Conduct an Evacuation Drill With All staff
- Practice Fire Safety and Evacuation Routes

For recommendations on where to access these additional trainings, please contact *My Practice* at 213-473-8630 or via email at MyPractice@CAPphysicians.com.

Important Notice: Telemedicine Update on the Ryan Haight Act — 2026 Temporary Extension

The Drug Enforcement Agency (DEA) and the U.S. Department of Health and Human Services (HHS) have announced a temporary extension of telemedicine flexibilities under the Ryan Haight Act, allowing clinicians to continue prescribing controlled substances via telemedicine without an initial in-person visit. The temporary extension is through December 31, 2026.

This temporary extension can help ensure continuity of care and prevent disruptions of care amongst seniors, rural residents, and those receiving treatment for mental health conditions while federal agencies finalize permanent telemedicine regulations.

For more information and official guidance, visit:
https://www.hhs.gov/press-room/dea-telemedicine-extension-2026.html

Andie Tena is Assistant Vice President, Practice Management Services. Questions or comments related to this column should be directed to ATena@CAPphysicians.com.

California 2026-2027 Proposed Healthcare Budget Outlook

by Gabriela Villanueva

In early January, Governor Newson presented his 2026-2027 proposed budget.

While the budget proposal generally maintains funding for existing services, the governor incorporated increases to offset the pending deficits that will impact the state as a result of the deep cuts imposed by federal legislation, H.R.1, signed last July.

H.R. 1 cuts roughly $800 billion from federal Medicaid spending in the next decade. With reduced federal support, the state general fund will face great pressure starting in the 2026-2027 cycle to backfill healthcare costs, inevitably pushing the state and the future governor to make tough choices on coverage, eligibility, services, and access.

The state budget proposal allocated a spending total of $343.6 billion in 2026-2027 to Health and Human Services, with Medi-Cal accounting for the largest share of spending from $196.7 billion in 2025-2026 to $222.4 billion in 2026-2027.

Another significant H.R.1 provision will disrupt California's existing Managed Care Organization (MCO) tax structure, rendering it noncompliant with federal requirements. The funds raised from this tax were intended to leverage federal matching funds earmarked for Medi-Cal. In 2023, the tax was expanded through 2026. However, in 2024, voters passed Prop 35 to make it permanent. Because California's MCO tax raises much more from Medi-Cal enrollments than from commercial plans, the tax structure now violates the standards set in H.R. 1. This misalignment with federal statute threatens this source of revenue for the state. Once the tax structure is compliant, it will generate significantly less revenue than the original structure.

In numbers, the governor proposed a $348.9 billion budget for fiscal year 2026-2027, with $248.8 billion in General Fund expenditures and a projected reserve of $23 billion that refills the state's "Rainy Day Fund."

The projected deficit in the governor's proposal is approximately $3 billion, while the estimate projected by the nonpartisan Legislative Analyst's Office (LAO) is around $18 billion. The governor's plan assumes much higher tax revenues due to the current boom in AI technologies and paints a much more optimistic picture.

This budget is the governor's opening "offer." From this point on, legislative leaders and the governor will negotiate, restructure, and recalculate. We will see a much more conclusive outlook when the governor once again issues his revised budget in May, called the "May Revise," after which legislators will have until June 15th to vote and pass a final adoption. Until then, all these numbers can shift.

For more information:

H.R.1 Medicaid Cuts: https://www.kff.org/medicaid/which-states-might-have-to-reduce-provider-taxes-under-the-senate-reconciliation-bill/

Legislative Analyst's Office (LAO) Budget Overview: https://lao.ca.gov/Publications/Report/5101

Health and Human Services Budget Breakdown chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://ebudget.ca.gov/2026-27/pdf/BudgetSummary/HealthandHumanServices.pdf?

Gabriela Villanueva is CAP's Government and External Affairs Analyst. Questions or comments related to this article should be directed to GVillanueva@CAPphysicians.com.

PUBLIC POLICY

Cyber Risk in Healthcare —The Scary Reality

Healthcare cyber claims data tell a consistent and troubling story: cyberattack frequency surged dramatically in 2025, roughly a 90% increase from the prior year, while loss costs more than doubled. These increases can be attributed to both ransomware attacks and the near-automatic class action lawsuits that follow such incidents. In parallel, continued lawsuits tied to online tracking technologies are increasing risk.

Healthcare organizations are facing ransomware attacks that are costing between two and three times more than those against non-healthcare entities.

Ransomware attacks are happening more frequently and are causing more damage. Double extortion, where attackers not only encrypt a victim's data but also steal and threaten to publish patient data unless a ransom is paid, has become standard. This type of attack can trigger nearly every part of a cyber policy: breach response, liability, business interruption, data recovery, and extortion payments.

The healthcare sector has consistently been featured among the top industries targeted by ransomware groups, and it's not just direct attacks that threaten the industry. The February 2024 Change Healthcare attack disrupted 94% of US healthcare providers and impacted nearly half of the US population.

Several factors converge to make healthcare organizations prime targets for cybercriminals. Healthcare networks are uniquely complex and interconnected. Legacy systems, vendor-managed devices, complex and interconnected IT environments and limited cybersecurity resources expand the attack surface, making it one of the most challenging environments to secure. Also, when hospital systems are disabled, the consequences extend far beyond operational disruption. Patient care is delayed, safety is compromised, and the financial and human costs become intertwined.

This combination creates significant vulnerabilities that attackers are eager to exploit, especially given the value of healthcare data. A single medical record can sell for $50-$250 on the black market compared to just $1-$2 for a stolen credit card number, making healthcare data more lucrative.

One of the main vulnerabilities for healthcare organizations are their virtual private networks. Most think their SSL/VPN (Secure Sockets Layer/Virtual Private Network) system is secure, but in reality, 50–60% of ransomware incidents come from VPN accounts that didn't have multi-factor authentication (MFA) properly enforced. Attackers now commonly break into networks through VPN login portals using automated password-guessing tools. This is often called brute-force. To defend against this, it's critical to not only require strong and complex passwords and enforce the use of MFA on all accounts, but to also set up account lockouts after failed login attempts and block connections coming from anonymous or high-risk networks like public VPNs, proxies, or the onion router (TOR).

Regular software updates (patching) are still essential, but as seen in recent ransomware attacks like Akira's campaign targeting SonicWall devices, even fully patched systems can be compromised if MFA and secure remote access aren't enforced. Healthcare teams need to ensure remote access to patient data remains secure without sacrificing ease of access for staff.

continued on page 11

Continued from page 10

The Legal Challenge

The legal aftermath of an attack is also quite challenging. When breaches must be disclosed under HIPAA and state privacy laws, it invites public scrutiny and rapid legal action. As a result, class actions often follow within days.

Meanwhile, litigation over website tracking tools has increased exposure for healthcare organizations, especially as some courts appreciate the sensitivity around personal medical data. One recent example was the use of Meta Pixel—a tool that helps analyze online traffic—in patient portals, not realizing the tool can share sensitive details with Meta, the social-media platform.

Although only about 200-300 of the roughly 3,000 cases filed* so far on website tracking involved healthcare providers, those few accounted for around two-thirds of the total settlement costs. Data from published class action cases show healthcare settlements averaging $5–6 million.

The Call to Action

Members of the Cooperative of American Physicians (CAP) are reminded of the value-added insurance benefits CAP provides as part of their membership, including CyberRisk liability coverage This cyberliability policy covers up to $50,000 and 5,000 patient notifications per covered claim should you experience a data breach in your practice. CAP members should note that their CyberRisk benefit includes a $2,500 deductible per covered claim.

While the built-in $50,000 limit provides essential baseline protection, modern cyber incidents frequently exceed that amount due to rising breach response costs, system restoration needs, and regulatory obligations.

Advantages of Securing Additional Coverage

- Expanded coverage beyond what is included in the built-in benefit for eligible CAP members
- Eligible CAP members may qualify for certain coverage or pricing advantages
- Access to apply for MEDEFENSE® Plus, which helps address expenses related to regulatory investigations and billing audits, with the option to include coverage for disciplinary proceedings—an increasingly important complement to cyber and professional liability protection

CyberRisk insurance is available for purchase at excellent rates through Symphony Health, a division of Symphony Risk Solutions. Contact Symphony Health at **213-576-8529** or via email at **HealthCareServices@SymphonyRisk.com** to learn more or request a free consultation.

*Das, Shanti. “NHS Data Breach: Trusts Shared Patient Details with Facebook without Consent.” The Guardian. 2023. https://www.theguardian.com/society/2023/may/27/nhs-data-breach-trusts-shared-patient-details-with-facebook-meta-without-consent

How Protected Health Information (PHI) Hides in Your Network, and How to Stop It

From CAPAdvantage partner, Acentec

One of the primary goals of a HIPAA compliance risk assessment is to document where PHI is stored for your organization. More often than not, it's in far more places than most realize. There can be several reasons why this happens. Let's consider the three most common causes.

Where's My PHI?

First, most web browsers have a default path for storing downloaded documents, and it's commonly into a folder named "Downloads." In a typical scenario, a user will access a web-based application like the Cardiac Arrest Registry to Enhance Survival (CARES) database and download a patient record. For many users, the PDF file will download and then open in their default PDF viewer, where they will then save it to its intended, proper folder. However, a copy of the downloaded file remains in the Downloads folder, and the name is usually not identifiable as a medical record. To avoid this often-overlooked scenario:

1. Change the download destination folder in the browsers you use to a protected folder where you save PHI.
2. Purge the Downloads folder on a regular basis. Depending on how your network is configured, it's possible to do this second step automatically.

Second, scanners and fax machines are notorious for saving PHI either locally on their own device, or, for networked systems, on a network folder in a path unique to the device. Again, this is a configuration issue, and unless you have manually configured every instance of the printer/scanner/fax software, then it's being saved in places you may not be aware of. Practices should:

1. Manually configure every workstation where the software is installed; or
2. Install a server-based version of the software where all of the stored documents are pathed to the same central folder.

Third, and most difficult for smaller offices to troubleshoot, are cached folders where PHI files may reside. A typical example of this would be a temporary folder where open documents are stored. Quite often, these files don't get fully erased when closed, and while the file names may not be recognizable, they are accessible and readable by unauthorized users. Practices can resolve this issue by knowing where the software you use stores its temporary files and purging that folder periodically. Again, this is a process that can be managed automatically by a professional IT management company, or you can do it manually.

Keeping PHI secure is a constant process that requires vigilance. It's required that you document where your PHI is stored and that it's encrypted when at rest.

This article is presented by Acentec, a participant in the CAPAdvantage program, CAP's suite of no-cost or discounted practice management products and services.

Acentec provides dedicated IT support to help manage and monitor your IT infrastructure. They also offer a complete HIPAA compliance program that includes required documentation, a risk assessment, and annual training for employees. If you have any questions or if you are concerned about your organization's cybersecurity practices, contact Acentec at **(949) 474-7774**.

Hippocratic Financial

Federal Student Loan Overview

The information below is general in nature and may affect each borrower's strategy differently. A personalized student loan analysis with Hippocratic Financial will be the best way to determine your strategy.

UPDATES ON INCOME-DRIVEN REPAYMENT (IDR) PLANS

- SAVE (Saving on Valuable Education) is effectively dead. Borrowers will be phased out of SAVE in the coming months
- The two currently active IDR plans that are good options are Pay-As-You-Earn (PAYE) and Income-Based Repayment (IBR)
- Payments on PAYE are 10% of discretionary income. IBR payments are also 10% if you have no loans from before July 1, 2014; those that do pay 15% on IBR
    - *Partial financial hardship is no longer required to apply for IBR, but does still apply for PAYE (i.e. No income limit on applying to IBR)*
    - *PAYE will cease to exist by July 2028 due to recent legislation*
- The new Repayment Assistance Plan (RAP) is supposed to begin in July 2026 and may be the best option during residency and fellowship
    - *Payment Calculation is based strictly on a percentage of Adjusted Gross Income (AGI), and the calculation changes based on income brackets. Minimum payment is $10.*
    - *Payment is reduced based on tax dependents, not family size*
    - *Payments are not adjusted proportionally for spouses who both have federal loans*
    - *Provides both an interest and principal subsidy for some borrowers*
- For the latest about IDR plans, visit: https://studentaid.gov/manage-loans/repayment/plans/income-driven
- To estimate your IDR payment, visit: https://studentaid.gov/loan-simulator/

PUBLIC SERVICE LOAN FORGIVENESS (PSLF)

- All IDR plans listed above qualify for PSLF
- Changes to PSLF require an act of Congress
- PSLF continues to be granted and is guaranteed as an option in your Master Promissory Note (MPN)
- PSLF buybacks are currently available to those affected by the SAVE forbearance
    - *You can only apply for buybacks when your current qualifying payments plus the buyback months = 120 payments*
    - *PSLF Buybacks were created through executive order and are not enshrined in law*
    - ***Because of this legal vulnerability to buybacks, there are no circumstances where you should forego a known PSLF-qualifying payment***

- Proposed changes to PSLF in July 2026 will face significant legal challenges, so PSLF is still seen as a viable strategy for the vast majority of those who qualify

CHANGES TO IDR PLANS IN THE 2025 BIG BEAUTIFUL BILL

- Borrowers with ANY new loans after July 1, 2026 (including consolidations) will only have access to the RAP or Standard repayment plans. Therefore, consolidations are a bad choice for nearly all borrowers
- The PAYE and Income-Contingent Repayment (ICR) plans are eliminated after July 1, 2028. Therefore, all borrowers must enroll in IBR, RAP, or Standard repayment plans

INCOME CERTIFICATION OPTIONS

- You have three options to certify your income when you apply for an IDR plan or have your annual IDR recertification: Tax returns, a statement of income letter, or using a paystub
- Depending on your circumstances, there may be benefits to either of the three. Identifying which strategy is best depends on your overall strategy (PSLF vs. IDR forgiveness vs. payoff) and your income during recent and current years

CREATING A "LITIGATION FILE"

- Due to potential legal challenges and data deletion at the federal level, as seen during early 2025, Hippocratic recommends creating a Litigation File to protect yourself. This involves the following documents and information from your profile on StudentAid.gov:
    - *Your Master Promissory Note (MPN)*
    - *Your National Student Loan Data System (NSLDS) file*
    - *Records of all payment history and PSLF employment certifications. We recommend keeping your own payment tracker to ensure payment and employment data on the website are correct*
    - *All IDR and buyback applications*
    - *All correspondence from or with your loan servicer and the Department of Education*

This information is presented by longtime CAPAdvantage participant Hippocratic Financial.

Have questions or want to schedule an analysis? Email Andrew Van Treeck, CFP, at andrew@hippocratic.com

Hippocratic Financial is a comprehensive, physician specialized wealth management firm that integrates investments, retirement planning, insurance, tax, legal, and student loan services. For more information, visit: https://hippocratic.com.

COOPERATIVE OF AMERICAN PHYSICIANS

Cooperative of American Physicians, Inc.
333 S. Hope St., 12th Floor
Los Angeles, CA 90071

IN THIS ISSUE

FEBRUARY 2026

333 S. Hope St., 12th Floor, Los Angeles, CA 90071 | 800-252-7706 | www.CAPphysicians.com

We welcome your comments! Please submit to communications@CAPphysicians.com.