

VALLEY! LAWYER

MARCH 2021 • \$5

A Publication of the San Fernando Valley Bar Association

HIPAA: To Preserve and Protect

Earn MCLE Credit

The Value of Experience: SFVBA Past Presidents Share Their Insights

WHAT IS PAST
IS PROLOGUE

Official Sponsors of the San Fernando Valley Bar Association

KRYCLER ERVIN TAUBMAN & KAMINSKY

FULL SERVICE ACCOUNTING FIRM

CONTACT MICHAEL J. KRYCLER, CPA, FCA | SCOTT R. ERVIN, CPA

*When you need more than just numbers...
you can count on us...*

- LITIGATION SUPPORT
- EXPERT WITNESS
- FORENSIC ACCOUNTANTS
- FAMILY LAW MATTERS
- BUSINESS VALUATIONS
- LOSS OF EARNINGS
- DAMAGES

MEMBERS OF
American Institute of Certified Public Accountants
California Society of Certified Public Accountants

15303 Ventura Boulevard, Suite 1040
Sherman Oaks, California 91403

info@ketkcpa.com

t: 818.995.1040

f: 818.995.4124

www.ketkcpa.com





FEATURES

12 HIPAA: To Preserve and Protect | BY ALAN J. SEDLEY
MCLE TEST NO. 149 ON PAGE 21.

22 The Value of Experience: SFVBA Past Presidents
Share Their Insights | BY MICHAEL D. WHITE

28 California's Critical Housing Shortage:
The Housing Accountability Act | BY ALICIA BARTLEY

32 Protecting Your Most Valuable
Asset | BY MARTIN LEVY

36 Working From Home?
Protect Your Critical Data | BY ALFREDO GONZALEZ

DEPARTMENTS

7 President's Message

9 Editor's Desk

11 Event Calendar

35 Bar Notes

39 Retrospective

43 Attorney Referral Service

45 Valley Community Legal Foundation

46 Classifieds



By reading this article and answering the accompanying test questions, you can earn one MCLE credit. To apply for the credit, please follow the instructions on the test answer form on page 21.

By Alan J. Sedley

HIPAA

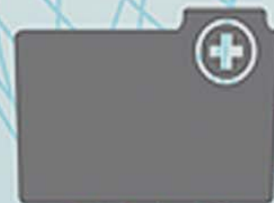
Health Insurance Portability & Accountability Act



To Preserve and Protect



SECURITY



PERSONAL DATA

Every byte of personal, individual identifiable data, such as that stored at banks, schools, places of employment, and online merchant services—name, address, social security number, date of birth, bank account numbers, employers, and the identity of family members, for example—could, with a simple send command and without adequate safeguards in place, effortlessly become the source of exploitation, monetization, and even personal humiliation.



**CLOUD
MEDICAL DATA**



PERSONAL FILES



**SSWORD
SECURITY**



**MEDICAL
INFORMATION**

**HIPAA
SECURITY**



**MEDICAL
COMPLIANCE**

OVER THE PAST THIRTY YEARS, RAPID-FIRE advances in technology have resulted in the massive electronic dissemination of information across countless numbers of networks and platforms.

As a result, it has become essential that effective safeguards be designed and implemented to protect the public from both the inadvertent and deliberate collection and dissemination of personal information by others unauthorized to do so.

Every byte of personal, individual identifiable data, such as that stored at banks, schools, places of employment, and online merchant services—name, address, social security number, date of birth, bank account numbers, employers, and the identity of family members, for example—could, with a simple send command and without adequate safeguards in place, effortlessly become the source of exploitation, monetization, and even personal humiliation.

Not the least of all individual privacy concerns, and a readily available source for potential breaches of security, involves the security of personal health information.

With that in mind, and as information technology and its advancements and growth continue to surge, there is a palpable sense of urgency among those in both the health care industry and in government to address the growing threat to patient confidentiality and privacy.

In response to those concerns, the tech industry went to work to develop a multitude of security hardware and software programs, while federal and state legislators sought to craft laws, rules and regulations to enforce the implementation of such necessary safeguards.

Enter HIPAA

The need for national standards for the privacy of individually identifiable health information gave rise to the promulgation of the Privacy Rule, issued by the Department of Health and Human Services (HHS), to serve as an element of the Health Information Portability and Accountability Act of 1996 (HIPAA).¹

HHS issued the Privacy Rule to implement the requirements of HIPAA and provide standards for the protection of certain sensitive personal health information.

The Privacy Rule standards address the use and disclosure of individuals' health information, called protected health information, or PHI, by organizations or

individuals subject to the HIPAA Privacy Rule, one of a series of rules implemented by HHS under the HIPAA legislation.

Other rules promulgated under the Act include its Transactions and Code Set Standards, Identifier Standards, as well as the Security Rule, and the Enforcement Rule.²

The HIPAA Privacy Rule standards address the use and disclosure of individuals' health information—for example, PHI, by organizations, or covered entities, subject to HIPAA Privacy Rules—as well as setting standards for individuals' privacy rights so as to provide the covered entity with the necessary tools to control exactly how an individual's health information is used.

Within HHS, the Office for Civil Rights has the responsibility for implementing and enforcing the HIPAA Privacy Rule regarding compliance activities. In addition, the Office assesses civil monetary penalties for those covered entities and others who violate these standards.

Basically, a primary goal of the HIPAA Privacy Rule is to ensure that individuals' health information is properly protected, while, at the same time, allowing the flow of information needed to promote and provide high quality health care to individuals.

Who is Covered

The HIPAA Privacy Rule applies to health plans, health care clearinghouses and any health care provider—the aforementioned covered entities—that transmits health information in an electronic form in connection with transactions for which the HHS Secretary has adopted standards under HIPAA.

Health Plans

Individual and group health plans that provide or pay the cost of medical care are designated as covered entities.³

Health plans include health, dental, prescription drug and vision insurers, health maintenance organizations (HMOs), long-term care insurers, and federally provided health plans such as Medicare, Medicaid, or Medi-Cal in California, Medicare Advantage, and Medicare supplement insurers.

Health plans may also include employer-sponsored group health plans, government and religious-sponsored health plans, and multi-employer health plans.

There are certain exclusions to the definition of a health plan for purposes of the HIPAA regulations—a group health plan, for instance, covering fewer than fifty employees that is self-administered by the employer is not deemed a health plan within the province of HIPAA.⁴



Alan J. Sedley serves as Senior Counsel at the firm of Nelson Hardiman in Los Angeles. His career-long focus has been on healthcare and medical-related law. He can be reached at asedley@nelsonhardiman.com.

ADR Services, Inc. Proudly Features
DAVID B. CASSELMAN, ESQ.
Mediator • Arbitrator



Areas of Expertise

Government Liability
Product Liability
Personal Injury
General Business
Professional Malpractice
Insurance Coverage and Bad Faith
Construction
Animal Law



For scheduling, please contact Haward Cho at haward@adrservices.com

www.CasselmanADR.com
(213) 683-1600

Health Care Clearinghouses

Health Care clearinghouses are covered entities for purposes of the HIPAA regulations that process nonstandard information they receive from another entity into a standard—for example, standard format or data content—or vice versa.⁵

Examples of health care clearinghouses include billing services, community health management information systems, and repricing companies.

In most instances, health care clearinghouses receive individually identifiable health information only when they are providing such processing services to a health plan or health care provider in its legal capacity as a business associate.

In these instances, only certain provisions of HIPAA are applicable to the health care clearinghouse's uses and disclosures of protected health information.⁶

Health Care Providers

A health care provider who electronically transmits or receives patient health information in connection with certain standard transactions is designated as a covered entity.

A health care provider deemed to be a covered entity under the HIPAA regulations—the Transactions Rule—is broadly defined as a provider of medical or health services under Medicare Part A—e.g., hospital services—or Part B—e.g., physician services—or any other person or organization that furnishes, bills for services rendered, or is paid for health care in the normal course of business.

Such a provider will include physicians—whether or not the physician in question operates a solo practice or is a member of a large health care provider group—dentists, and chiropractors, as well as hospitals and other institutional providers of health care services such as long term care facilities, health care outpatient clinics, and diagnostic facilities.

For purposes of the HIPAA Privacy Rule, such transactions would include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which HHS has established standards as laid-out in the HIPAA Transaction Rule.⁷

A transaction where, for example, a health care provider transmits PHI to a health plan to obtain authorization for patient care to ensure coverage eligibility falls within the provisions of the Rule.

Business Associates & Covered Entities

For purposes of the HIPAA Privacy Rule, a business associate is a person or organization, other than a member of a covered entity's workforce, "that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable public health information, or PHI."⁸

A business associate functions or activities on behalf of a covered entity include claims processing, data analysis,

utilization review, billing, transcription services, temporary staffing services, and software development/maintenance.⁹

Business associate services to a covered entity are limited to legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.

Note, however, that persons or organizations are not considered business associates “if their functions or services do not involve the use or disclosure of PHI, or where any access to PHI by such individuals would be considered incidental.”

By definition, a covered entity can be the business associate of another covered entity.

When a covered entity uses a business associate to perform such functions or activities on behalf of the covered entity, HIPAA regulations require that the covered entity enter into a business associate agreement with the business associate.

Such an agreement will include provisions imposing specified written security safeguards on the PHI used or disclosed by its business associate, such as administrative, technical, and physical safeguard requirements as laid out in the HIPAA Security Rule.

Effectively, every safeguard provided by the Rule is required unless there is a justifiable reason not to implement the safeguard or an appropriate alternative to the safeguard is implemented and achieves the same objective.

An example of such a reason could be the requirement to encrypt emails containing PHI.

Such a requirement might not be applicable if such emails are not sent beyond a firewalled, internal server.

If a covered entity or business associate only uses such emails as an internal form of communication—or has an authorization from a patient to send their information unencrypted—there would be no need to implement this particular safeguard.

What Information is Protected

The HIPAA Privacy Rule protects all individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether it be electronic, on paper, or by oral communication.

The Rule considers this information protected health information, or PHI.¹⁰

Individually identifiable health information is information that relates to:

- The individual’s past, present or future physical or mental health or condition, The provision of health care to the individual; or,
- The past, present or future payment for the provision of health care to the individual, and that identifies the

individual or for which there is a reasonable basis to believe it can be used to identify the individual.¹¹

De-identified health information is not protected health information, and, therefore, there are no restrictions on the use or disclosure of de-identified health information.¹²

To fall under the de-identified information safe harbor, certain data should not be in the information disclosed—names, in whole or in part; geographical identifiers; phone or fax numbers; email addresses; medical record numbers; account numbers; vehicle identification numbers (VINs); vehicle license plate numbers; web urls; and internet protocol (IP) addresses.

Additional prohibited data includes biometric identifiers, such as retinal and voice prints and fingerprints; full face photographic images; social security numbers (SSNs); health insurance beneficiary numbers; and any other unique identifying number, characteristic, or code.¹³

Patient Privacy Right

The HIPAA Privacy Rule establishes a patient’s right to receive a Notice of Privacy Practices (NPP) from a Covered Entity, which specifies the ways in which the covered entity will use and disclose the patient’s PHI.¹⁴

Under the Rule, the NPP must be written in plain language, include all of the required content and elements


WE SPECIALIZE IN:

MURPHY'S

LAW

- Ransomware & Cybersecurity Protection
- Legal Practice Management Support
- Disaster Recovery Planning
- Network Configuration
- VoIP and Internet

- 24/7 Help Desk
- Office Moves
- Office 365
- Backup



ITSUPPORTLA

6047 Tampa Ave, Suite 305
Tarzana, CA 91356 | (818) 805-0909
www.itsupportla.com

set forth in the Rule, and be either provided or made available at specified times and locations.¹⁵

Among other requirements, the NPP must contain anticipated uses and disclosures of the individual's PHI by the Covered Entity for purposes of treatment, payment and health care operations, as well as a description of each of the other uses or disclosures which the covered entity may make without obtaining the individual's written authorization.

The description must also be sufficiently detailed so that the individual is placed on notice of the anticipated use or disclosure.

The Notice of Privacy Practices must also set forth a statement of the individual's rights with respect to PHI, such as the right to:

- Request restrictions on certain uses and disclosures of PHI;
- Receive confidential information from the covered entity;
- Inspect, copy and amend the individual's own PHI; and,
- Receive an accounting of disclosures (but not uses) of PHI.

A covered entity is required to act on an individual's request to access, inspect a copy of their own PHI with certain exceptions, within thirty (30) days of the request if the PHI is accessible on-site or sixty (60) days if the PHI is located off-site.

A covered entity is permitted to deny access to certain public health information with no opportunity for appeal.

Such information includes psychotherapy notes; information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; information held by prisons on inmates; information held by a research entity when the individual has agreed, as part of the research protocol, to the limitation on access for the duration of the research project; and, information obtained from someone other than a health care provider under a promise of confidentiality.

A covered entity may also deny access to certain PHI if upon review, another licensed health care provider has determined that the request is reasonably likely to endanger the life or physical safety of the individual or another person; the PHI contains a reference to another person; the access requested is reasonably likely to cause substantial harm to such other person; or the request is made by a personal representative and the access is reasonably likely to cause substantial harm to the individual or to another person.

If access is denied on the grounds stated immediately above, the individual has the right to have the denial reviewed by a licensed health care professional, designated

by the covered entity, who did not participate in the original denial.

Patient's Rights to Amend

A patient has the right to have a covered entity amend PHI to ensure that the information is accurate and complete for as long as the covered entity maintains the PHI.¹⁶

Should the covered entity accept the requested amendment, it must make the correction in all affected efforts, make reasonable efforts to inform its business associates and others that have received the PHI of the correction, and notify the patient of those actions.

A covered entity may deny a patient's request to amend its PHI if, for example, the PHI was not created by that covered entity; the PHI is excepted from the right of access such as psychotherapy notes, and information in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding); or, in the covered entity's opinion, the PHI is already accurate and complete.

In such instances of denial, the covered entity must provide the individual with a timely, written denial, the basis for the denial, the individual's right to submit a written statement of disagreement, and a description of how the individual may complain to the appropriate federal agency such as the Department of Health and Human Services.

A covered entity that is informed by another covered entity of an amendment to an individual's public health information must, as well, amend the PHI in its own records.

Violations of HIPAA

The HIPAA Enforcement Rule establishes the framework for compliance and investigations, and determining the amount of civil monetary penalties to be imposed upon covered entities who violate any provision of the HIPAA Privacy and Security Rules, as well as the procedures for hearings.

The Enforcement Rules establish critical definitions that significantly affect the extent of civil monetary penalties.¹⁷

They include reasonable cause, reasonable diligence, and willful neglect.¹⁸

Most critically, the Rules define willful neglect as a "conscious, intentional failure or reckless indifference to the obligation to comply with the provision violated" and could result in significant civil monetary penalties ranging from \$100 per violation up to a maximum of \$25,000 levied by the Office of Civil Rights.¹⁹

The HITECH Act

Despite requiring that the relationship between covered entities and business associates be memorialized in a written agreement that sets forth the several requisite provisions, the original HIPAA regulations offered no avenue for enforcement against business associates who violated their agreements or the provisions of HIPAA.

The HITECH Act was enhanced by subjecting business associates directly to the standards set forth in the HIPAA Security Rule, as well as certain aspects of the HIPAA Privacy Rule. This was done through the promulgation of the Omnibus Rule, which extends direct liability to business associates for HIPAA violations.²⁰

The Omnibus Rule implemented HITECH's requirement that business associates must comply with the HIPAA Security Rule in the same manner applicable to covered entities.

Minimum compliance for business associates includes developing and performing a full risk analysis, as well as developing and implementing internal policies and procedures intended to satisfy the required elements of the HIPAA Security Rule's physical, technical, and administrative ePHI safeguards.

To the extent that the business associate receives or generates PHI, the associate must also comply with the basic provisions of the HIPAA Privacy Rule prohibiting the use and disclosure of PHI in any manner not permitted by the Privacy Rule.²¹

Moreover, a business associate that is engaged to carry out one of the covered entity's responsibilities under the HIPAA Privacy Rule—for example, handling an individual's request for access to their PHI—must comply with the Privacy Rule in carrying out those responsibilities.

A business associate's failure to comply with the requirements of the HIPAA Privacy and Security Rules can possibly give rise to direct liability and potential civil monetary penalties levied by the Office of Civil Rights.

Breach Notification

Before the HITECH Act, there was no express requirement that a covered entity notify an individual, such as a patient, about an unauthorized disclosure of the individual's PHI.

Under the HITECH Act, Congress addressed that omission by defining a breach of PHI as the "unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would reasonably have been able to retain such information."²²

Tossing out the Office of Civil Rights attempt to clarify the instance of a breach of PHI in terms of a risk of harm threshold standard, the subsequent Omnibus Act took a harder stance.

According to the new standard, unauthorized disclosures of PHI are presumed to be a breach requiring reporting, unless the covered entity can demonstrate a low probability that the PHI has been compromised—for example, when that the breach event was remedied before it could constitute a vulnerability or that the information was not accessed.

LIFE INSURANCE IS ONE OF THE MOST IMPORTANT FINANCIAL PLANNING INSTRUMENTS YOU OWN.

IS YOUR
LIFE INSURANCE
POLICY A

TICKING TIME BOMB?

WE'RE WILLING TO BET YOUR POLICY
IS **NOT** WHAT YOU THINK IT IS!

The Life Insurance Audit™
Thinking you are covered
is not the same as knowing **Audit™**

The **Life Insurance Audit™**

is a proven, objective system, which ensures clients have the best possible insurance solution available in the market today. Most people have no idea of the negative impact to their policies. **We'll figure it out!**

If you want
to know the facts,
call us at 1.800.914.3564
LifeAudit@CorpStrat.com
We'll tell you!



CorpStrat

INSURANCE • EMPLOYEE BENEFITS • HR • PAYROLL

This shifts the burden of proof to the covered entity, and requires that the covered entity either assume that every unauthorized disclosure is a breach, or perform a risk analysis on every such incident to determine whether the incident can be mitigated to the extent that it no longer constitutes a breach, using a specific delineated set of factors.

Those factors include the nature and extent of the PHI involved with the covered entity required to conduct an investigation to determine whether the PHI was actually acquired or viewed.


Once the covered entity performs such a risk analysis, it can then determine whether there is a low probability that the PHI has been compromised.

If the analysis does not convincingly demonstrate to the covered entity that the PHI was not compromised, the required course of action dictates notification to the individuals and reporting to the Office of Civil Rights.

Breach Analysis

The breach analysis under the Omnibus Act can best be summarized as a four-step process—discovery; investigation; analysis; and response, whether or not notice and reporting are required.

Any deviation from an analysis, or an attempt to pre-determine an outcome in the course of the investigation such that a non-breach is determined and thus reporting avoided, could very well give rise to severe monetary penalties.

In addition, civil actions could be brought by the individual whose PHI was breached, once the incident is objectively reviewed by the Office of Civil Rights when the occurrence was brought to light. 

¹ 45 CFR. § 164.501; Public Law 104-191.

² 45 CFR. § Part 164.

³ *Id.* §§ 160.102, 160.103.

⁴ *Id.* § 160.103.

⁵ *Id.*

⁶ *Id.* § 164.500(b).

⁷ 45 CFR. §§ 160.102, 160.103. The Transaction Standards are established by the HIPAA Transactions Rule at 45 CFR. Part 162.

⁸ 45 CFR. § 160.103.

⁹ *Id.*

¹⁰ *Id.*

¹¹ *Id.*

¹² 45 CFR. § 164.502(d)(2), 164.514(a) – (b).

¹³ *Id.* § 164.514(c).

¹⁴ *Id.* § 164.520.

¹⁵ *Id.* CFR. § 164.520(b).

¹⁶ *Id.* § 164.526.

¹⁷ *Id.* § 160.401.

¹⁸ *Id.*

¹⁹ *Id.*

²⁰ *Id.* § 164.103(b), 164.302, and 164.500.

²¹ *Id.* parts 160 and 164.

²² American Recovery and Reinvestment Act of 2009, 42 U.S.C.A. § 17921.

VIRTUAL EVENT

SAN FERNANDO VALLEY BAR ASSOCIATION



State of the Courts

Thursday, March 4

12:15 PM - 1:15 PM

Supervising Judge Virginia Keeny of the Northwest District leads a distinguished Judges' Panel to give an update on the courts.

Members' questions are welcome.

Send questions to events@sfvba.org.

Don't miss this important virtual event!

SFVBA Members Registration

<https://members.sfvba.org/calendar/signup/MjMzMzMQ==>

MCBA Affiliate Members and Guests Registration

https://us02web.zoom.us/webinar/register/WN_IVvaSBk9Sd-nopLWKPlvaw



HIPAA: To Preserve and Protect

Test No. 149

This self-study activity has been approved for Minimum Continuing Legal Education (MCLE) credit by the San Fernando Valley Bar Association (SFVBA) in the amount of 1 hour. SFVBA certifies that this activity conforms to the standards for approved education activities prescribed by the rules and regulations of the State Bar of California governing minimum continuing legal education.

1. A transaction where a health care provider transmits PHI to a health plan to obtain authorization for patient care to ensure coverage eligibility falls within the provisions of the HIPAA Transaction Rule.
☐ True ☐ False
2. The HIPAA Privacy Rule protects all individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral communications.
☐ True ☐ False
3. De-identified health information is protected health information, and therefore, there are numerous restrictions on the use or disclosure of such information.
☐ True ☐ False
4. A mobile home license plate number is not considered identifiable information under the HIPAA Privacy Rule.
☐ True ☐ False
5. The HIPAA Enforcement Rule establishes the framework relating to compliance and investigations and determining the amount of civil monetary penalties to be imposed upon covered entities who violate a provision(s) of the HIPAA Privacy and Security Rules.
☐ True ☐ False
6. A dentist who electronically transmits or receives patient health information in connection with certain, standard transactions is designated as a covered entity.
☐ True ☐ False
7. A psychiatrist must comply with a patient's request to view his psychotherapy record, including the psychiatrist's notes taken during the patient's therapy session.
☐ True ☐ False
8. The breach analysis under the Omnibus Act can best be summarized as a four-step process, which includes discovery, investigation, analysis, and response when notice is deemed to be required
☐ True ☐ False
9. One aim of the HITECH Act was to require that a business associate adhere to those same standards required of a covered entity under the HIPAA Security Rule.
☐ True ☐ False
10. A company serving as a business associate to a covered entity cannot also fall within the designation of covered entity under the definitions set forth in the HIPAA Privacy Rule.
☐ True ☐ False
11. An individual's health insurance company is not a covered entity as that term is defined under the HIPAA Privacy Rule.
☐ True ☐ False
12. The HIPAA Privacy Rule is designed to protect an individual's PHI stored in electronic form only, such that the individual's PHI recorded in the form of a paper medical record does not fall within the provisions of the Privacy Rule.
☐ True ☐ False
13. Absent in the provisions of the HITECH Act, the subsequent Omnibus Act provided that a business associate who violates the HIPAA Security Rule could give rise to direct liability and potential civil monetary penalties against the business associate.
☐ True ☐ False
14. The HIPAA Privacy Rule establishes a patient's right to receive a Notice of Privacy Practices from a covered entity.
☐ True ☐ False
15. A prison inmate's demand that he be given access to view his PHI must be granted.
☐ True ☐ False
16. A chiropractor does not have to allow a patient to amend his PHI if the chiropractor believes that in her opinion, the PHI is already accurate and complete.
☐ True ☐ False
17. Contained within the HIPAA Privacy Rule is an express requirement that a covered entity notify an individual about an unauthorized disclosure of the individual's PHI.
☐ True ☐ False
18. PHI is an acronym for Patient Health Information under the HIPAA Privacy Rule.
☐ True ☐ False
19. Three identifiable rules set forth within the HIPAA regulation are the Privacy Rule, Security Rule and Transaction Rule.
☐ True ☐ False
20. A component of individually identifiable health information includes the individual's history of complaints of poor customer service directed at his health insurance company health plan.
☐ True ☐ False

HIPAA: To Preserve and Protect MCLE Answer Sheet No. 149

INSTRUCTIONS:

1. Accurately complete this form.
2. Study the MCLE article in this issue.
3. Answer the test questions by marking the appropriate boxes below.
4. Mail this form and the \$20 testing fee for SFVBA members (or \$30 for non-SFVBA members) to:

San Fernando Valley Bar Association
20750 Ventura Blvd., Suite 140
Woodland Hills, CA 91364

METHOD OF PAYMENT:

- ☐ Check or money order payable to "SFVBA"
☐ Please charge my credit card for

\$ _____.

Credit Card Number _____

CVV code _____

Exp. Date _____/_____/_____

Authorized Signature _____

5. Make a copy of this completed form for your records.
6. Correct answers and a CLE certificate will be mailed to you within 2 weeks. If you have any questions, please contact our office at (818) 227-0495.

Name _____

Law Firm/Organization _____

Address _____

City _____

State/Zip _____

Email _____

Phone _____

State Bar No. _____

ANSWERS:

Mark your answers by checking the appropriate box. Each question only has one answer.

- | | | |
|-----|-------------------------------|--------------------------------|
| 1. | <input type="checkbox"/> True | <input type="checkbox"/> False |
| 2. | <input type="checkbox"/> True | <input type="checkbox"/> False |
| 3. | <input type="checkbox"/> True | <input type="checkbox"/> False |
| 4. | <input type="checkbox"/> True | <input type="checkbox"/> False |
| 5. | <input type="checkbox"/> True | <input type="checkbox"/> False |
| 6. | <input type="checkbox"/> True | <input type="checkbox"/> False |
| 7. | <input type="checkbox"/> True | <input type="checkbox"/> False |
| 8. | <input type="checkbox"/> True | <input type="checkbox"/> False |
| 9. | <input type="checkbox"/> True | <input type="checkbox"/> False |
| 10. | <input type="checkbox"/> True | <input type="checkbox"/> False |
| 11. | <input type="checkbox"/> True | <input type="checkbox"/> False |
| 12. | <input type="checkbox"/> True | <input type="checkbox"/> False |
| 13. | <input type="checkbox"/> True | <input type="checkbox"/> False |
| 14. | <input type="checkbox"/> True | <input type="checkbox"/> False |
| 15. | <input type="checkbox"/> True | <input type="checkbox"/> False |
| 16. | <input type="checkbox"/> True | <input type="checkbox"/> False |
| 17. | <input type="checkbox"/> True | <input type="checkbox"/> False |
| 18. | <input type="checkbox"/> True | <input type="checkbox"/> False |
| 19. | <input type="checkbox"/> True | <input type="checkbox"/> False |
| 20. | <input type="checkbox"/> True | <input type="checkbox"/> False |