Document #4101

HIPAA Privacy Rule

CMA Legal Counsel, January 2016

The privacy and security regulations enacted pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA Privacy Rule) sets national standards for the protection of individually identifiable health care data or PHI regardless of how maintained (paper, oral or electronic form). These standards protect an individual's medical records and other personal health information, and apply to covered entities that conduct certain health care transactions electronically. It requires appropriate safeguards to protect privacy and confidentiality of protected health information (PHI) and establishes limits and conditions on the uses and disclosures of such information without an individual's authorization. The Privacy Rule also sets forth certain patient rights over their health information, including rights to examine and obtain copies of their health records and request corrections.

This document provides an overview of the HIPAA Privacy Rule's administrative requirements and a general outline for physicians and their staff to use in developing a HIPAA compliance plan. It does not, however, purport to provide instruction on all aspects of compliance for all physician offices. You can also find sample HIPAA Notice of Privacy Practices and office privacy and security policies at the end of the document. Physician practices must customize any sample policies they use to reflect exactly how their practice uses PHI.

For more information on other aspects of the HIPAA Privacy Rule, *see* CMA ON-CALL document #4001, "Accounting of Disclosures," CMA ON-CALL document #4251, "Special Confidentiality Requests," CMA ON-CALL document #4205, "Patient Access to Medical Records," and CMA ON-CALL document #4207, "Request by Other Third Parties: CMIA, IIPPA, and the HIPAA Privacy Rule."

COMPLIANCE WITH CALIFORNIA LAW REQUIRED

The HIPAA Privacy and Security Rules do not override state laws that are more protective of patient rights or privacy controls. (45 C.F.R. §§160.201 *et seq*.) Physicians would have to comply with any such state laws in addition to the requirements of HIPAA. Because California law is often more protective of patients, many HIPAA rules must be customized for California. Thus, California physicians should not rely on templates which have been produced by national organizations which do not reflect California law. For more information on California's patient privacy law, the Confidentiality of Medical Information Act (CMIA) (Civil Code §§56 *et seq*.), *see* CMA ON-CALL document #4207, "Request by Other Third Parties: CMIA, IIPPA, and the HIPAA Privacy Rule."

APPLICABILITY

The HIPAA Privacy Rule applies to physicians and other providers that use electronic means to perform HIPAA-covered transactions, such as the transmission of health claims, remittance or payment advice or any of the other electronic transactions included in the HIPAA Transaction and Code Sets rules. HIPAA also applies to those who pay for health care (health plans) and clearinghouses. The HIPAA Privacy Rule applies with respect to all PHI, whether in paper, oral or electronic form. For more detailed information on HIPAA, including the definition of "covered entity," *see* CMA ON-CALL document #4100, "HIPAA Overview/Enforcement." For information on the HIPAA Security Rule, *see* CMA ON-CALL document #4102, "HIPAA Security Rule."

COMPLIANCE AND IMPLEMENTATION

Every practice is different. While this document should be helpful to physicians in maintaining and establishing their own compliance program, no "one size fits all" program exists. A HIPAA compliance program should meet the internal needs of the practice and address any specific risks. Depending on the size, standards might be more or even less detailed than those presented here. Accordingly, any of the recommendations set forth in this document should be modified to accommodate your practice's specific needs.

A compliance program must be more than a series of papers—rather, there must be an overall commitment on behalf of everyone on staff to comply with standards and procedures which are reasonably capable of resulting in a good faith effort at compliance with the HIPAA Privacy and Security Rules. The HIPAA Privacy and Security Rules clearly contemplate a commitment to enhancement of patients' control of their protected health information and of a physician's obligation to protect the confidentiality of this information.

The establishment of a compliance plan alone is not enough to satisfy the requirements of the HIPAA Privacy and Security Rules. As discussed herein, physicians must demonstrate and document that they have properly-trained staff (45 C.F.R. §§164.308(a)(5) and 164.530(b)), provided safeguards for unintended or intended disclosures in violation of the standards (45 C.F.R. §§164.308(a)(6) and 164.530(c)), instituted appropriate sanctions against employees for non-compliance with the HIPAA Privacy and Security Rule requirements (45 C.F.R. §§164.308(a)(1) and 164.530(e)), and have a process for receiving complaints related to HIPAA Privacy Rule violations (45 C.F.R. 164.530(d)).

The HIPAA Security Rule requires physicians to conduct a security risk analysis (an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information), ongoing risk management, information system activity review and response and reporting of security incidents to mitigate to the extent practical the harmful effects of such incidents. (45 C.F.R. §164.308(a)(1) and (6).)

Without a committed staff that understands how the HIPAA Privacy and Security Rules impact their daily work responsibilities, a compliance program for the Privacy and Security Rules will not be effective in deterring non-compliance.

ADMINISTRATIVE REQUIREMENTS

The HIPAA Privacy and Security Rules provide for specific administrative requirements to be implemented in a compliance program by the covered entity to protect patient medical information. An effective compliance program is one which has been reasonably designed, implemented and enforced so that it will generally be effective in preventing and detecting non-compliance with the HIPAA Privacy and Security Rules.

Designate Privacy and Security Official

The HIPAA Privacy and Security Rules require that a physician covered by HIPAA designate privacy and security officials who are responsible for the development and implementation of the policies and procedures of the physician's office. The Rules also require that a contact person be designated who is responsible for receiving complaints for HIPAA Privacy Rule violations, and who is able to provide information about policies and procedures, such as the Notice of Privacy Practices discussed below. (45 C.F.R. §§164.308(a)(2) and 164.530(a)(1).) For many covered entities, particularly in smaller organizations, the security official may be the same person as the privacy official.

The physician must document and maintain a written or electronic record of these personnel designations. (45 C.F.R. §§164.530(a)(2) and (j); 45 C.F.R. §164.316(b).)

Staff Training

The HIPAA Privacy Rule requires covered physicians to train their workforces on the policies and procedures developed to comply with HIPAA. The training must be necessary and appropriate for the members of the workforce to carry out their function within the physician's office, and specifically address security risks associated with computer usage. (45 C.F.R. §§164.308(a)(5) and 164.530(b)(1).) "Workforce" is defined as employees, volunteers, trainees and others whose work is under the control of a covered entity. (45 C.F.R. §160.103.)

All physician office staff should now have been trained on both the Privacy and Security Rules, as this training must have been completed when these rules took effect and within a reasonable period after new employees join the workforce. Physicians must also conduct trainings within a reasonable time after any material change in a policy or procedure. (45 C.F.R. §§164.308(a)(5) and 164.530(b)(2).) Additionally, the Security Rule requires ongoing security awareness through the use of periodic security updates and reminders. (45 C.F.R. §164.308(a)(5)(ii)(A).)

The physician must document the training activity and maintain a written or electronic record of the training. (45 C.F.R. §§164.316(b); 45 C.F.R. §164.530(b)(2)(ii) and (j).) The documentation concerning training must be kept for six (6) years from the date of its creation or the date when it last was in effect, whichever is later. (45 C.F.R. §164.530(j)(2).) If possible, it is best to document the training program showing what types of training occurred, how often, and who attended or received the written or electronic information. To comply with the documentation requirement, a practice may wish to require a certification of compliance and training signed by all office employees stating that they have read and understood the policies and procedures and that they will report any suspected or known violation of the HIPAA Privacy or Security Rules to the Privacy and Security Officer.

Physician practices with employee handbooks may wish to further strengthen the commitment to compliance through personnel standards which incorporate the following points:

- Both employees and supervisors will be evaluated on the basis of whether they have adhered to the compliance program;
- Appropriate action will be taken against anyone who has engaged in unlawful behavior;
- Employees will be disciplined for failure to detect or report violations of the HIPAA Privacy or Security Rule; and
- Reports of alleged non-compliance will be kept confidential wherever possible, and a good faith report will not be cause for discipline or affect performance evaluations.

Training can be accomplished through a variety of means, including in-person training sessions, conducted within the physician's practice, and conducted through "outside seminars." The training program should address the operation and importance of compliance with the HIPAA Privacy and Security Rules, and the consequences of violating those rules. It should include guidance on how to identify violations of privacy or security policies and procedures, and should encourage employees to report these violations without concern about retaliation or discrimination.

Business Associates

In addition to training employees and requiring that they comply with the HIPAA Privacy and Security Rules and policies and procedures of the medical practice, physicians should ensure that contractors, agents and others who act on their behalf not engage in conduct that violates the HIPAA Privacy and Security Rules. The HIPAA Privacy and Security Rules require that physicians execute business associate agreements with business associates that contain specified requirements that the business associate will appropriately safeguard the information. (45 C.F.R. §164.502(e).) For a detailed discussion of Business Associates Agreements, *see* CMA ON-CALL document #4103, "Business Associate Agreements."

Implement Safeguards

The HIPAA Privacy and Security Rules require that physicians have appropriate administrative, technical and physical safeguards to protect the privacy of PHI. These safeguards apply to all PHI whether electronic, written or oral, and are in addition to the more detailed requirements established by the HIPAA Security Rule for electronic PHI (*e*PHI) only. These safeguards must include protections against any intentional or unintentional uses or disclosures in violation of the HIPAA Privacy Rule, and safeguards to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure. (45 C.F.R. §164.530(c).) The HIPAA Security Rule further requires that all ***electronic*** health information the physician practice creates, receives, maintains or transmits retain its integrity, confidentiality and availability, and that the practice protect against reasonably anticipated threats or hazards to the security of that information and against reasonably anticipated uses or disclosures that are unauthorized. (45 C.F.R. §164.306(a).) For more information on the Security Rule, *see* CMA ON-CALL document #4102, "HIPAA Security Rule."

The HIPAA Privacy and Security Rules do not specifically address how these safeguards should be accomplished. However, an ongoing evaluation process is important to a successful compliance program. This ongoing evaluation can include not only whether the practice's standards and procedures are in fact current and accurate, but also whether or not the compliance program is effective, i.e., individuals are properly carrying out their responsibilities and protected health information is, in fact, being protected.

Given the requirements that policies and procedures be updated as necessary, it is recommended that the privacy and security officer or other individuals also be charged with the responsibility of periodically reviewing the policies and procedures to see if they are current and complete. Furthermore, the Security Rule requires periodic technical and nontechnical evaluation of security safeguards. (45 C.F.R. §164.308(a)(8).)

Each physician practice needs to decide for itself how to monitor and review the HIPAA Privacy and Security Rules standards and procedures given the particularities of the office setting. Further, the physician must mitigate, to the extent practicable, any known harmful effect of a use or disclosure of protected health information in violation of the practices policies and procedures. (45 C.F.R. §§164.308(a)(6) and 164.530(f).) Physicians can have an outside consultant provide an audit, or do it themselves. The CMA/PrivaPlan HIPAA Toolkit contains an audit checklist as well as guidance on conducting a self-assessment and audit.

Incidental Disclosure of PHI. Physicians must have safeguards to limit incidental uses or disclosures. (45 C.F.R. §164.530(c).) Because of the nature of customary health care communications and practices, the potential exists for an individual's health information to be disclosed incidentally. The Office for Civil Rights (OCR) has discussed incidental disclosures as follows:

> It is not expected that a covered entity's safeguards guarantee the privacy of protected health information from any and all potential risks. Reasonable safeguards will vary from covered entity to covered entity depending on factors, such as the size of the covered entity and the nature of its business. In implementing reasonable safeguards, covered entities should analyze their own needs and circumstances, such as the nature of the protected health information it holds, and assess the potential risks to patients' privacy. Covered entities should also take into account the potential effects on patient care and may consider other issues, such as the financial and administrative burden of implementing particular safeguards.
>
> Many health care providers and professionals have long made it a practice to ensure reasonable safeguards for individuals' health information—for instance:
>
> - By speaking quietly when discussing a patient's condition with family members in a waiting room or other public area;
> - By avoiding using patients' names in public hallways and elevators, and posting signs to remind employees to protect patient confidentiality;
> - By isolating or locking file cabinets or records rooms; or
> - By providing additional security, such as passwords, on computers maintaining personal information.

> Protection of patient confidentiality is an important practice for many health care and health information management professionals; covered entities can build upon those codes of conduct to develop the reasonable safeguards required by the Privacy Rule.

(OCR HIPAA Privacy Guidance, Significant Aspects of the Privacy Rule, available at www.hhs.gov/hipaa/for-professionals/privacy/guidance/incidental-uses-and-disclosures/index.html.)

Complaints

Physician practices covered by HIPAA must provide a process by which individuals can make complaints regarding any policies and procedures required by the HIPAA Privacy Rule or the practice's compliance with such policies. All complaints received by the physician must be documented and retained for six (6) years. (45 C.F.R. §164.530(d) and (j).)

Sanctions to Enforce Standards and Policies

The HIPAA Privacy and Security Rules require that a physician have and apply appropriate sanctions against members of the office workforce who fail to comply with the privacy or security policies and procedures of the physician's practice or the requirements of the HIPAA Privacy or Security Rules. (45 C.F.R. §§164.308(a) and 164.530(e).) However, sanctions do not apply to whistleblowers. (45 C.F.R. §164.502(j).) Further, a physician must document the application of any sanction.

Again, the HIPAA Privacy and Security Rules do not specifically address what sanctions should be used. However, appropriate and consistent educational and disciplinary mechanisms should be in place for all individuals who have failed to comply with the practice's standard of conduct, policies and procedures and other requirements of the HIPAA Privacy and Security Rules. These standards should be enforced through "well publicized" disciplinary guidelines.

Discipline should be applied consistently, regardless of the level of the individual in question or his or her economic value to the practice, and should be fair. While the appropriate discipline should be considered on a case-by-case basis, potential measures range from oral warning, to temporary suspension, to termination. Any communication resulting in a finding of non-compliant conduct and subsequent educational and/or disciplinary measures should be documented.

The HIPAA Privacy Rule also prohibits physicians from intimidating, threatening, coercing, discriminating against, or taking other retaliatory action against any individual who exercises any right established or participates in any process to enforce the HIPAA Privacy Rule, including the filing of a complaint under the HIPAA Privacy Rule, or participating in an investigation, or opposing any activity which the individual in good faith believes is in violation of the Rule. (45 C.F.R. §164.530(g).)

Finally, a physician may not require patients to waive their rights under the HIPAA Privacy Rule as a condition of treatment, payment, or eligibility for benefits under a health plan. (45 C.F.R. §164.530(h).)

Policies and Procedures

The HIPAA Privacy and Security Rules require various policies and procedures to demonstrate compliance with the Rules. Physicians are required to change or update their policies and procedures as necessary and appropriate to comply with changes in the law. (45 C.F.R. §§164.316(a) and 164.530(i)(2).) They are also required to retain the policies and procedures in electronic or written form for six (6) years from the date of creation of the document or the date when it was last in effect, whichever is later. (45 C.F.R. §§164.316(b) and 164.530(j)(2).) Some of these specific policies and procedures are discussed herein.

The HIPAA Privacy and Security Rules expressly state that the policies and procedures developed by physicians "must be reasonably designed, taking into account the size of and the type of activities that relate to protected health information undertaken by the covered entity, to ensure such compliance." (45 C.F.R. §§164.530(i)(1) and 164.306(b).)

Response and Prevention

If, despite all the efforts described above, a violation of the HIPAA Privacy or Security Rules is detected, physicians should take all reasonable steps to respond appropriately to the offense and to prevent similar offenses. Upon receipt of a report that there has been a violation of the Rules, the Privacy and Security Officer (or his/her designee), should investigate the complaint and determine whether a material violation of the law

has occurred, and if so, take the necessary steps to redress the problem.

NOTICE OF PRIVACY PRACTICES REQUIRED

Physicians covered by HIPAA are required to provide to all patients a notice of the uses and disclosures of PHI that may be made by the physician or his/her employees, the patient's rights concerning PHI and the physician's legal obligations with respect to PHI. (45 C.F.R. §164.520(a).)

The Notice of Privacy Practices (Notice) will likely be the first knowledge many patients have of the HIPAA Privacy Rule. This notice gives patients the opportunity to learn how PHI will be used and disclosed by their physicians and also alerts them to their rights with regard to access and other issues related to their health information.

Physicians are required to provide the Notices of Privacy Practices to their patients no later than the date of the first point of service, in-person or electronically. (45 C.F.R. §164.520(c)(2).)

Many medical offices have simply copied a form off the Internet or borrowed from friends. This is not adequate. The notice must be customized to the practice to reflect exactly how it uses PHI. In addition it must reflect California law where that is more protective of patients' rights than the federal rule. Most forms created national organizations are not customized for California law, which contains a number of additional patient rights.

Content of Notice of Privacy Practices: Required Elements

The Notice must be written in plain language and contain the following:

- **Header.** The Notice must contain the following statement prominently displayed:

  THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

- **Uses and Disclosures.** The Notice must include:

  1. A description, including at least one example, of how the physician may use and disclose the PHI for purposes of treatment, payment and health care operations. One example of such use or disclosure must be provided for each purpose.
  2. A description of each of the other purposes for which the physician is permitted or required to use or disclose PHI without the patient's written authorization.
  3. A description of the types of uses and disclosures that require authorization related to psychotherapy notes, marketing, sale of PHI, a statement that other uses and disclosures not described in the notice will be made only with the patient's written authorization, and a statement that the individual may revoke an authorization.

     Note that all descriptions in the Notice of how PHI will be used in the absence of the patient's written authorization must be consistent with any more stringent requirements imposed by California law, and must include "sufficient detail to place the individual on notice" of the uses and disclosures that are permitted or required by law.

  (45 C.F.R. §164.520(b)(1)(ii).)

- **Separate Statements for Certain Uses or Disclosures.** A separate statement of intended disclosure must be provided if the physician intends to:

  1. Contact the patient to raise funds for the physician's office and the patient has the right to opt out of receiving such communications;
  2. The group health plan, health insurance issuer or HMO with respect to a group health plan, may disclose PHI to the sponsor of the plan; or
  3. If a health plan intends to use or disclose PHI for underwriting purposes, a statement that such a covered entity is prohibited from using or disclosing PHI that is genetic information for such purposes.

  (45 C.F.R. §164.520(b)(1)(iii).)

- **Individual Rights.** The Notice must contain a statement of the individuals' rights with respect to PHI and a brief description of how the individual may exercise the following rights:

  1. The right to request restrictions on certain uses and disclosures of protected health information, including a statement that the physician is not required to agree to a requested restriction, except a request that a health plan not be informed of treatment for which the patient paid entirely out of pocket. (42 U.S.C. §17935(a), 45 C.F.R. §164.522(a); *see* CMA ON-CALL document #4251, "Special Confidentiality Requests";
  2. The right to receive confidential communications of protected health information, "by alternative means or at alternative locations" (45 C.F.R. §164.522(b); *see* CMA ON-CALL document #4251, "Special Confidentiality Requests");
  3. The right to inspect and copy protected health information (45 C.F.R. §164.524; *see* CMA ON-CALL document #4205, "Patient Access to Medical Records");
  4. The right to amend protected health information (45 C.F.R. §164.526; *see* CMA ON-CALL document #4003, "Contents of Medical Records");
  5. The right to receive an accounting of disclosures of protected health information (45 C.F.R. §164.528; *see* CMA ON-CALL document #4001, "Accounting of Disclosures"); and
  6. The right of an individual, including an individual who has agreed to receive the notice electronically to obtain a paper copy of the Notice of Privacy Practices from the physician upon request.

  (45 C.F.R. §164.520(b)(1)(iv).)

- **Physician's Duties.** The Notice of Privacy Practices must include the physician's various duties under the HIPAA Privacy Rule as follows:

  1. A statement that the physician has a duty to maintain the privacy of PHI, and to provide patients with notice of its legal duties and privacy practices with respect to PHI, and to notify affected individual following a breach of unsecured PHI;
  2. A statement that the physician is required to abide by the terms of the Notice of Privacy Practices currently in effect; and
  3. A statement that the physician reserves the right to change the terms of its Notice of Privacy Practices and to make the new notice provisions effective for all PHI that the physician maintains. If the physician wants the ability to change the terms of its notice and to make the new notice provisions effective for all protected health information it maintains, the physician must include a statement that the physician has reserved this right. The notice must also describe how the physician will provide patients with a revised notice.

  (45 C.F.R. §164.520(b)(1)(v).)

- **Complaints.** The Notice of Privacy Practices must also contain a statement that patients may complain to the physician or to the Secretary of the U.S. Department of Health and Human Services (HHS) if they believe their privacy rights have been violated. The notice must provide a brief description of how the patient may file a complaint with the physician and state that the individual will not be retaliated against for filing a complaint. (45 C.F.R. §164.520(b)(1)(vi).)
- **Contact.** The Notice of Privacy Practices must contain the name or title and telephone number of the person or office to contact for further information. This person is generally the designated privacy or security officer. (45 C.F.R. §164.530(a)(1)(ii); (45 C.F.R. §164.520(b)(1)(vii).)
- **Effective Date.** The Notice of Privacy Practices must contain the date on which the notice is first in effect, which may not be earlier than the date the notice was printed or otherwise published. (45 C.F.R. §164.520(b)(1)(viii).)

Content of Notice of Privacy Practices: Optional Elements

If the physician elects to have more stringent limitations on the use or disclosures of PHI than is required by the HIPAA Privacy Rule, the physician may describe its more limited uses or disclosures in its Notice of Privacy Practices. However, the physician may not limit uses or disclosures required by law, such as the various reporting requirements, or the right, to

the extent it is otherwise permitted by law and standards of ethical conduct, to disclose information the physician believes in good faith is necessary to prevent or lessen a serious and unwarranted threat to the health or safety of a person or the public. If a voluntary limitation is included, it must be enforced. (45 C.F.R. §164.520(b)(2).)

Dissemination of the Notice of Privacy Practices

Physicians covered by the HIPAA Privacy Rule who have a direct treatment relationship with a patient must disseminate the Notice of Privacy Practices as follows:

- The physician must provide the notice to the patient no later than the date of the first service delivery, including service delivered electronically, except with respect to emergencies.
- The physician must make a good faith effort to obtain a written acknowledgment of receipt of the notice provided, and if the acknowledgment is not obtained, the physician must document his/her good faith efforts to obtain such acknowledgment and the reason why it was not obtained, except with respect to emergencies.
- If treatment is provided under an emergency situation, the notice must be provided as soon as reasonably practicable after the emergency treatment situation. (45 C.F.R. §164.520(c)(2)(i)(B).)
- The notice must be available at the physician's office for patients to request and take with them.
- The notice must be posted in a clear and prominent location where it is reasonable to expect individuals seeking treatment from the physician to be able to read the notice.
- Whenever the notice is revised, the physician must make the notice available upon request and must post the revised notice.
- If the physician maintains a website that provides information about the physician's services or benefits, the notice must be posted on the website and available electronically through the site.
- The physician may provide the Notice of Privacy Practices to a patient by e-mail if the patient agrees to electronic notice and does not withdraw the agreement. If the first service from the physician was delivered electronically, the physician must provide the electronic notice automatically and contemporaneously in response to the patient's first request for service.
- Even if a patient receives the notice electronically, the patient has a right to obtain a paper copy of the notice from a physician.

(45 C.F.R. §164.520(c).)

Revisions to the Notice of Privacy Practices

Physicians must promptly revise and distribute their Notice of Privacy Practices whenever there is a material change to the uses or disclosures, the patient's rights, the physician's legal duties, or other privacy practices stated in the Notice. Implementation of material changes may not be accomplished until the effective date of the notice, except when the change is required by law. (45 C.F.R. §164.520(b)(3).)

When a physician has changed a privacy practice that is included in the Notice of Privacy Practices and makes corresponding changes to its policies and procedures, it may make the changes effective for PHI that the physician created or received prior to the effective date of the notice revision only if the physician has, in the Notice of Privacy Practices, reserved the right to make such a change. (45 C.F.R. §164.530(i)(2)(ii).) If the physician did not reserve this right to change a privacy practice, the physician is bound by the privacy practices as stated in the Notice with respect to PHI created or received while such notice is in effect. (45 C.F.R. §164.530(i)(4)(ii).) As noted above, physicians are generally best advised to reserve this right to avoid the administrative complexity which would otherwise ensue.

Physicians may change any other policy or procedure that does not materially affect the content of the Notice of Privacy Practices if such change complies with the HIPAA Privacy Rule and such change is documented. (45 C.F.R. §164.530(i)(5).)

Notice of Privacy Practices Updates

On January 25, 2013, the HHS published a final rule implementing sweeping changes to HIPAA based on the statutory changes mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA). The final rule, known as the "HIPAA Omnibus Final

Rule," was effective March 26, 2013 and covered physicians must have complied with the applicable requirements by September 23, 2013. (78 Fed.Reg. 5566 (January 25, 2013).)

Pursuant to the HIPAA Omnibus Final Rule, physician practices will have had to update their Notice of Privacy Practices to reflect the changes made to the HIPAA Privacy Rule. To the extent that some practices have already revised their Notice of Privacy Practices to reflect the HITECH Act requirements, so long as the current Notice is consistent with the final rule and patients have been informed of all material revisions made to the Notice, the physician practice is not required to revise and distribute another Notice upon publication of the HIPAA Omnibus Final Rule.

A sample Notice of Privacy Practices designed for a typical physician office and which reflects California law can be found at the end of this document. The Office for Civil Rights and the National Coordinator for Health Information Technology recently developed a model Notices of Privacy Practices for health care providers that can be found at www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/index.html.

MINIMUM NECESSARY STANDARD

Generally, with some exceptions identified in the Privacy Rule, when using or disclosing PHI or when requesting PHI from another physician, covered entity or business associate, a physician must make reasonable efforts to limit use or disclosure of PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. (45 C.F.R. §164.502(b)(1).) OCR has explained its interpretation of the minimum necessary requirement as follows:

> The minimum necessary standard, a key protection of the HIPAA Privacy Rule, is derived from confidentiality codes and practices in common use today. It is based on sound current practice that protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function. The minimum necessary standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information. The Privacy Rule's requirements for minimum necessary are designed to be sufficiently flexible to accommodate the various circumstances of any covered entity.

(OCR HIPAA Privacy Guidance.)

Exceptions to Applications of Minimum Necessary Rule

The minimum necessary rule does not apply to the following circumstances:

- Disclosures to or requests by a health care provider for treatment purposes;
- Disclosures to the individual who is the subject of the information;
- Uses or disclosures made pursuant to an individual's written authorization;
- Uses or disclosures that are required by law; and
- Uses or disclosures required for compliance with the HIPAA Privacy Rule, or to HHS pursuant to a HIPAA investigation or compliance review.

(45 C.F.R. §164.502(b)(2).)

Physician's Workforce

The HIPAA Privacy Rule requires covered physicians to identify which members of its workforce need access to PHI to carry out their duties, and for each such person or class of persons, the category or categories of PHI to which access is needed, and any conditions appropriate to this access. Physician offices must make reasonable efforts to limit the access of certain workforce members or class of persons to PHI. (45 C.F.R. §164.514(d)(2).) In addition, one of the addressable administrative safeguards under the HIPAA Security Rule deals with workforce security. A covered physician may implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic PHI and prevent those workforce members who do not have access from obtaining access to electronic PHI. (45 C.F.R. §164.308(a)(3) and (4).)

Requests For and Disclosures of PHI

Physicians must adopt policies and procedures governing 1) requests for PHI, and 2) disclosures of PHI as follows:

If a request or disclosure is made on a routine and recurring basis, physicians must implement policies and procedures that limit the PHI requested or disclosed to that reasonably necessary to achieve the purpose of the disclosure or accomplish the purpose for which the request is made. (45 C.F.R. §164.514(d)(3) and (4).)

For all other requests for or disclosures of protected health information, physicians must develop criteria designed to limit the request or disclosure to the information reasonably necessary to accomplish the purpose for which the request is made or disclosure is sought. Physicians must also review such requests for disclosure on an individual basis in accordance with criteria. (*Id.*)

For all uses, disclosures or requests where the minimum necessary rule is applicable, a physician may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure or request. (45 C.F.R. §164.514(d)(5).)

Reliance on Representations as to Minimum Necessary

The HIPAA Privacy Rule permits physicians to rely on the judgment of the requesting party as to the minimum necessary amount of information for a stated purpose. Such reliance must be reasonable under the particular circumstances of the request. Such reliance is allowed when the request is made by:

- A public official or agency that is authorized to access the information and states that the information requested is the minimum necessary for the stated purpose.
- A health plan, health care clearinghouse, or other health care provider covered by HIPAA, or a professional who is a workforce member or business associate of a health plan, clearinghouse or covered health care provider who requests the information for the purpose of providing professional services to that covered entity, and states that the information requested is the minimum necessary for the stated purpose. (Note that the minimum necessary rule does not apply to requests by health care providers for treatment purposes, so generally speaking physicians will not need to determine whether a physician is or is not covered by HIPAA in applying this rule.)
- A researcher with appropriate documentation from an Institutional Review Board (IRB) or Privacy Board.

(45 C.F.R. §164.514(d)(3)(iii).)

Caution: It is unclear how this regulation will be applied following the enactment of the HITECH Act requirement that the "covered entity or business associate disclosing the PHI determines what constitutes the minimum necessary to accomplish the intended purpose of the disclosure." Until HHS issues further guidance on the minimum necessary rule, physicians should still be able to rely on certain representations of what constitutes minimum necessary but can exercise their discretion to restrict the use or disclosure of PHI as to what constitutes minimum necessary to accomplish the intended purpose. (42 U.S.C. §17935(b)(2).)

Disclosures under the HITECH Act

Effective February 17, 2010, the HITECH Act requires disclosures to be limited to the limited data set or the minimum necessary. When the minimum necessary standard applies, HIPAA covered entities, including physicians, must use, disclose, or request only the ***limited data set*** to the extent that is practicable to accomplish the intended purpose of that use, disclosure or request. Moreover, the party disclosing the PHI determines what constitutes the minimum necessary to accomplish the intended purpose of the disclosure. (42 U.S.C. §17935(b).) HHS is expected to issue future guidance on the minimum necessary standard in accordance with the HITECH Act provision. This standard does not apply to the use, disclosure or request of de-identified PHI.

Limited Data Set Defined

To be a "limited data set" the PHI *must not include any of the following identifiers* of the individual and any relatives, employers or household members of the individual:

- Names;
- Postal address information other than town or city, State and zip code;
- Telephone numbers;
- Fax numbers;

- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints; and
- Full face photographic images and any comparable images.

Essentially, a "limited data set" is the same as fully de-indentified information except it may contain town or city and zip code, and dates directly related to an individual, including birth date, admission date, discharge date, age and date of death. (45 C.F.R. §164.514(e)(2).)

OTHER REQUIRED OFFICE POLICIES AND PROCEDURES

As discussed above, physician offices are required to have written policies and procedures to demonstrate compliance with the HIPAA rules. Policies and other required documentation include, but are not limited to:

- **Notice of Privacy Practice.** *See* discussion above.
- **Privacy Policy.** Physicians must adopt and implement an office privacy policy that ensures that the practice fully complies with the federal and state privacy laws. This policy may include policies and procedures with regard to the use and disclosure of PHI, how complaints about privacy violations are handled, appropriate safeguards to protect PHI, workforce training, monitoring compliance, sanctions and anti-retaliation provisions.
- **Security Policy.** Physicians must adopt and implement an office security policy to ensure that the practice appropriately complies with the applicable federal and state security laws. The security policy can include provisions related to risk analysis and management, sanctions, workforce training, device and media control, and security incident identifications. For more information, *see* CMA ON-CALL document #4102, "HIPAA Security Rule."
- **Business Associate Agreements.** For more information, *see* CMA ON-CALL document #4103, "Business Associate Agreements."
- **Breach Notification Policy and Procedures.** Physicians must document its policies and procedures related to the discovery of an actual or suspected breach of unsecured PHI. For more information, *see* CMA ON-CALL document #4006, "Security Breach of Health Information." For a sample policy, *see* CMA ON-CALL document #4176, "HIPAA Breach Notification Policies and Procedures."
- **Document Retention Policy.** Physicians must document how long policies and procedures and related documentation (investigation files, training and compliance files, risk analysis report, etc.) should be retained by the practice.

Sample Privacy and Security Policies

A sample privacy and security policy designed for the typical physician office and which reflects California law may be found at the end of this document.

HIPAA OMNIBUS FINAL RULE

The HIPAA Omnibus Final Rule made sweeping changes to the Privacy and Security Rules based on the statutory changes mandated by the HITECH Act. Pursuant to the final rule, physician practices must have updated policies and procedures, including the Notice of Privacy Practice, breach notification policies and business associate agreements to reflect the changes made to the HIPAA rules. The HIPAA Omnibus Final Rule was effective March 26, 2013 and covered physicians must have complied with the applicable requirements by September 23, 2013. (78 Fed.Reg. 5566 (January 25, 2013).)

CMA's HIPAA Omnibus Rule Compliance FAQ may be found at the end of this document as Attachment A. This document answers the most commonly asked questions related to the HIPAA Omnibus Rule that

CMA's Center for Legal Affairs have received from its member physicians.

CMA/PRIVAPLAN HIPAA TOOLKIT

The CMA/PrivaPlan HIPAA ToolKit is a comprehensive online resource to assist physicians in complying with the HIPAA Privacy, Security, and Breach Notification Rules and California law. It contains detailed forms, sample policies and procedures tailored for California physicians, training materials, and resources to help physicians with implementation and planning. Physicians can order the CMA/PrivaPlan HIPAA ToolKit by calling (877) 218-7707 or at www.privaplan.com. CMA members may purchase the CMA/PrivaPlan HIPAA ToolKit as well as other HIPAA services such as the CMA/PrivaPlan Online HIPAA Training tool, HIPAA Security Risk Analysis, HIPAA Breach Notification Review and Remediation, and HIPAA Policies and Procedures Review at discounted prices.

We hope this information is helpful to you. CMA is unable to provide specific legal advice to each of its more than 41,000 members. For a legal opinion concerning a specific situation, consult your personal attorney.

For information on other legal issues, use CMA's online health law library, CMA ON-CALL, or refer to the *California Physician's Legal Handbook* (CPLH). CPLH is a comprehensive health law and medical practice resource containing legal information, including current laws, regulations and court decisions that affect the practice of medicine in California. Written and updated by CMA's Center for Legal Affairs, CPLH is available in an eight-volume, softbound print format or through an online subscription to www.cplh.org. To order your copy, call (800) 882-1262 or visit CMA's website at www.cmanet.org.

HIPAA Omnibus Rule Compliance
Frequently Asked Questions

California Medical Association

On January 25, 2013, the U.S. Department of Health and Human Services published new regulations that made significant changes to the privacy and security requirements under the Health Insurance Portability and Accountability Act (HIPAA). These new regulations, known as the HIPAA Omnibus Final Rule implement many of the key provisions of the Health Information Technology for Economic and Clinical Health Act (HITECH) Act of 2009. Covered entities and their business associates have until September 23, 2013, to comply with the new rule.

Answers to the most commonly asked questions related to the HIPAA Omnibus Final Rule compliance requirements are found below. This information does not constitute, and is no substitute for, legal or other professional advice. Physician offices should consult their personal attorneys or professional advisors for specific guidance on their HIPAA compliance plan.

Note: In this document you will find references to "CMA On-Call documents." These documents are available free to members in the California Medical Association (CMA) online health law library at http://www.cmanet.org/cma-on-call. Nonmembers can purchase documents for $2/page.

Privacy and Security Officials

1. Do I need to designate a Privacy Official and Security Official in my office?

Yes. HIPAA requires covered entities to designate a Privacy Official and Security Official who is responsible for the development and implementation of policies and procedures of the physician's office. For many offices, the Privacy Official and Security Official may be the same person.

Notice of Privacy Practices

2. Do I need to update my Notice of Privacy Practices? If so, when do I need to update it by?

Yes. The HIPAA Omnibus Final Rule requires physician practices to make material changes to their existing Notice of Privacy Practices (NPP). These changes must be made by September 23, 2013. If your office already revised its NPP in response to the 2009 HITECH Act provisions, so long as the current NPP is consistent with the new rules, you are not required to revise and distribute another NPP.

Specifically, the new rules require the NPP to include a statement informing individuals of their right to be notified following a breach of their unsecured protected health information and their right to obtain a copy of their PHI in electronic format if the covered entity maintains the PHI electronically. The NPP must also inform individuals of their right to restrict certain disclosures of PHI to a health plan when the patient pays out-of-pocket and in full for a health care item or service. Further, the new rules require changes to NPP provisions related to the use and disclosure of psychotherapy notes, the sale of PHI, marketing and the right to opt-out of fundraising solicitations. For an updated sample NPP, see CMA On-Call document #4101, "HIPAA Privacy Rule."

3. Do I need to redistribute the updated NPP and have patients re-sign acknowledgments?

Providers are only required to give a copy of the updated NPP to, and obtain a good faith acknowledgment of receipt from, new patients. Physician offices must make the NPP available to all patients upon request on or after the effective date of the revision and must have the NPP available at the point of care. The updated NPP must also be posted in a clear and prominent location and on the physician practice website.

4. My NPP is long. Do I have to post the entire thing in my waiting room?

No. Providers may post a summary of the notice in a clear and prominent location in the office, such as the waiting room, so long as the full notice is immediately available (such as on a table directly under the posted summary) for individuals to pick up without any additional burden on the patient. If a summary is posted, it would not be appropriate to require a patient to ask for a copy of the full NPP.

Risk Analysis

5. My office has not conducted a risk analysis. Is this necessary to be in compliance with HIPAA?

Yes. Physician practices that maintain electronic PHI must comply with the HIPAA Security Rule requirements and perform a risk analysis of office security. A risk analysis must be an accurate and thorough assessment of the potential risks and vulnerabilities to electronic PHI and its integrity and confidentiality. A risk analysis is more complex than filling out a checklist and physician practices should obtain assistance in completing this task. For more information, see CMA's on-demand webinar "HIPAA Risk Analysis for Meaningful Use." This webinar is available free to members in CMA's online resource library at http://www.cmanet.org/webinars.

For additional guidance on complying with the risk analysis requirement, see the Office for Civil Rights website at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html. For more information on the HIPAA Security Rule requirements, see CMA On-Call document #4102, "HIPAA Security Rule."

Breach Notification

6. Do I need to update my breach notification policy and procedures?

Yes. Under HIPAA's Breach Notification Rule, covered entities must provide notification following a breach of unsecured PHI. The HIPAA Omnibus Final Rule made a significant change in assessing what is a reportable breach of PHI. The new rules now presume that there is a breach unless the practice can demonstrate that there is a low probability that the PHI has been compromised. This is a change from the previous standard where a breach was not reportable unless it posed a significant risk of harm to an individual. Covered entities must update their office breach notification policies and procedures to reflect this change and train their workforce accordingly. For more information on breach notification and a sample office policy, see CMA On-Call document #4006, "Security Breach of Health Information."

Business Associates

7. Do I need to update my business associate agreements and when do I have to it by?

Yes. All business associate agreements must be revised and updated. The HIPAA Omnibus Final Rule broadened the definition of business associate, which means that some contractors that have not been business associates in the past may now be considered business associates. Physician practices should review their third party vendors and contractors to determine whether they are business associates. Covered entities and business associates may continue to operate under existing business associate agreements for up to one year beyond the September 23, 2013, compliance date. All business associate agreements must be by the earlier of (1) the date the agreement is renewed or modified on after September 23, 2013, or (2) by September 22, 2014. For more information on business associates and an updated sample business associate agreement, see CMA On-Call document #4103, "Business Associate Agreements."

8. We contract with a health care clearinghouse to provide services on our behalf. Do we need to sign a business associate agreement with them if they are a covered entity?

A covered entity can be a business associate of a covered entity. To the extent that the health care clearinghouse performs services such as electronic billing transactions of the physician practice's behalf, it is also a business associate and there must be a business associate agreement in place.

9. Do I need to sign business associate agreement with my employees or individuals who provide janitorial services for my office?

No. A physician practice's employees are not business associates, but rather a part of the covered entity's workforce. In addition, people or organizations whose functions or services do not involve PHI and whose access to PHI would be incidental, such as maintenance or janitorial workers are not business associates.

10. I store my old paper records with a storage company. Do I need to sign a business associate agreement with them?

Yes. The definition of a business associate has been broadened to include entities that create, receive, maintain or transmit PHI on behalf of the physician office. The regulations clarify that companies that maintain or store PHI on behalf of a covered entity are business associates, even if they do not view or access the PHI.

Workforce Training

11. Do I have to retrain my staff after I update my office policies to reflect the new requirements of the HIPAA Omnibus Final Rule?

Yes. All employees, volunteers, trainees and others who work under the control of the covered entity must be trained on the policies and procedures developed to comply with HIPAA. All new employees must be trained within a reasonable time after they join the workforce and additional training must occur within a reasonable time after any material change in a policy or procedure. All training activity must be documented and kept for six years. CMA and PrivaPlan jointly publish a HIPAA Training Manual that provides general training and overview and can be used as part of your HIPAA training program. It is available on CMA's website at http://www.cmanet.org.

Email and Mobile Technology

12. I heard that the HIPAA Omnibus Final Rule prohibits emailing and texting patients after the compliance deadline. Is this true?

No. Physicians who are covered entities have always been prohibited from emailing or texting patient information without the proper privacy and security safeguards. While the patient can consent to receiving certain communications by email, this does not excuse the physician practice from implementing the proper safeguards (encryption/policies/training) to satisfy the HIPAA Privacy and Security Rules. The HIPAA Omnibus Final Rule does not change these requirements. For more information on the use of email and mobile technology, see CMA On-Call documents #0402, "Physician Websites, Internet Advice and Email," and #3301, "Physician Use of Mobile Devices and Cloud Computing."

HIPAA Compliance Resources

13. What do I need to do to get my office in compliance with the HIPAA Omnibus Final Rule?

This will depend on each physician practice and the current status of their HIPAA compliance. A practice that has already updated their policies and procedures to reflect the provisions of the HITECH Act may have very little to do in terms of the September 23, 2013, compliance deadline. Physician practices who have not updated their HIPAA policies and procedures in some time will have more work to do. At a minimum, a practice should:

- Designate a Privacy Official and Security Official
- Review and implement office policies and procedures
- Make sure a risk analysis has been completed
- Update your Notice of Privacy Practices
- Update office privacy policies
- Review third-party vendors and contractors to update business associate list
- Amend business associate agreements
- Update breach notification policies and procedures
- Train workforce

14. Where can I find more resources to assist me?

- **CMA's health law library, CMA On-Call,** is a comprehensive collection of law, ethical opinions and case law of interest to the practice of medicine in California, including chapters on eMedicine, HIPAA, and Medical Records. These documents are available free to CMA members at www.cmanet.org/cma-on-call. Nonmembers can purchase documents for $2 per page.
- **"HIPAA Compliance: The Final HITECH Rule" On Demand Webinar** is available on CMA's website at http://www.cmanet.org/webinars.
- **Office for Civil Rights website** contains guidance documents and up to date information on new regulations regarding the HIPAA Privacy and Security Rules at http://www.hhs.gov/ocr.
- **American Medical Association website** contains an extensive HIPAA Resource Page at http://www.ama-assn.org.
- **CMA/PrivaPlan ToolKit** is a comprehensive online resource to assist physicians in complying with the HIPAA Privacy and Security Rules and California law. It includes a step-by-step compliance plan and numerous California specific sample forms, policies and procedures. It also contains an audit tool designed to assess the degree of compliance in a practice. Physicians can order the CMA/PrivaPlan ToolKit by calling (877) 218-7707 or visiting http://www.privaplan.com. CMA members can purchase the CMA PrivaPlan HIPAA Online ToolKit and PrivaPlan's online HIPAA training programs at discounted prices.

SAMPLE LETTERS AND FORMS: INSTRUCTIONS

The following sample forms do not constitute and is not a substitute for legal or other professional advice:

1. HIPAA Notice of Privacy Practices—Sample Notice
2. HIPAA Notice of Privacy Practices—Sample Acknowledgment of Receipt
3. HIPAA Notice of Privacy Practices—Sample Acknowledgment Tracking Information
4. HIPAA Privacy Policy Statement—Sample Policy
5. HIPAA Security Policy Statement—Sample Policy

Users should consult their own legal and other professional advisors as necessary for individualized guidance with respect to each particular situation.

These samples are excerpted from the CMA/PrivaPlan HIPAA ToolKit, a comprehensive HIPAA compliance online tool, available by calling (877) 218-7707 or at www.privaplan.com. **Instructions for customizing these templates appear on the cover page of each template.**

HIPAA Notice of Privacy Practices—Sample Notice (Updated May 2013)

Disclaimer: CMA/PrivaPlan Template Notice of Privacy Practices (45 C.F.R. §164.520)

The information provided in this document does not constitute, and is no substitute for, legal or other professional advice. Users should consult their own legal or other professional advisors for individualized guidance regarding the application of the law to their particular situations, and in connection with other compliance-related concerns.

To customize this template document, replace all of the text that is presented in brackets (i.e., "[" and "]") with text that is appropriate to your organization and circumstances. After completing the customization of this document, the document should be reviewed by an attorney who is familiar with health privacy laws and regulations in the state(s) in which the organization maintains its offices or facilities, and who is in a position to provide legal counsel to your organization.

NOTE: The Notice should be completed based on the organization's actual practices which must be documented in policies and procedures. Thus, a physician practice must have completed its policies and procedures regarding uses and disclosures, authorizations and consents, inspection and copying, accounting, alternative methods for giving information to patients, amendments, changes in the Notice and restrictions of uses and disclosures prior to finalizing this Notice.

In determining their participation in organized health care arrangements (OHCA), as set forth in Section A.3, physicians should generally list: 1) every hospital where they have staff privileges; 2) every IPA with which they participate; 3) every health plan with which they contract; and 4) any other organization that has informed the physician that the physician is an OHCA participant.

In addition, each patient right described in Section C below should be explained in enough detail so that the individual understands that each right is not absolute and is subject to some limitations and conditions. While some of these rights have been expanded to include the basic limitations provided under the law, each should be considered in light of the organization's actual practices.

NOTICE OF PRIVACY PRACTICES

[Physician Practice Name and Address]

[Name or Title and Telephone Number of Privacy Officer]

Effective Date: [insert effective date]

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

We understand the importance of privacy and are committed to maintaining the confidentiality of your medical information. We make a record of the medical care we provide and may receive such records from others. We use these records to provide or enable other health care providers to provide quality medical care, to obtain payment for services provided to you as allowed by your health plan and to enable us to meet our professional and legal obligations to operate this medical practice properly. We are required by law to maintain the privacy of protected health information, to provide individuals with notice of our legal duties and privacy practices with respect to protected health information, and to notify affected individuals following a breach of unsecured protected health information. This notice describes how we may use and disclose your medical information. It also describes your rights and our legal obligations with respect to your medical information. If you have any questions about this Notice, please contact our Privacy Officer listed above.

TABLE OF CONTENTS

A. How This Medical Practice May Use or Disclose Your Health Information

The medical record is the property of this medical practice, but the information in the medical record belongs to you. The law permits us to use or disclose your health information for the following purposes:

1. Treatment. We use medical information about you to provide your medical care. We disclose medical information to our employees and others who are involved in providing the care you need. For example, we may share your medical information with other physicians or other health care providers who will provide services that we do not provide or we may share this information with a pharmacist who needs it to dispense a prescription to you, or a laboratory that performs a test. We may also disclose medical information to members of your family or others who can help you when you are sick or injured, or following your death.

2. Payment. We use and disclose medical information about you to obtain payment for the services we provide. For example, we give your health plan the information it requires for payment. We may also disclose information to other health care providers to assist them in obtaining payment for services they have provided to you.

3. Health Care Operations. We may use and disclose medical information about you to operate this medical practice. For example, we may use and disclose this information to review and improve the quality of care we provide, or the competence and qualifications of our professional staff. Or we may use and disclose this information to get your health plan to authorize services or referrals. We may also use and disclose this information as necessary for medical reviews, legal services and audits, including fraud and abuse detection and compliance programs and business planning and management. We may also share your medical information with our "business associates," such as our billing service, that perform administrative services for us. We have a written contract with each of these business associates that contains terms requiring them and their subcontractors to protect the confidentiality and security of your medical information. Although federal law does not protect health information which is disclosed to someone other than another healthcare provider, health plan, healthcare clearinghouse, or one of their business associates, California law prohibits all recipients of healthcare information from further disclosing it except as specifically required or permitted by law. We may also share your information with other health care providers, health care clearinghouses or health plans that have a relationship with you, when they request this information to help them with their quality assessment and improvement activities, their patient-safety activities, their population-based efforts to improve health or reduce health care costs, protocol development, case management or care coordination activities, their review of competence, qualifications and performance of health care professionals, their training programs, their accreditation, certification or licensing activities, their activities related to contracts of health insurance or health benefits, or their health care fraud and abuse detection and compliance efforts. [*Participants in organized health care arrangements only should add*: We may also share medical information about you with the other health care providers, health care clearinghouses and health plans that participate with us in "organized health care arrangements" (OHCAs) for any of the OHCAs' health care operations. OHCAs include hospitals, physician organizations, health plans, and other entities which collectively provide health care services. A listing of the OHCAs we participate in is available from the Privacy Official.]

4. [Optional: Appointment Reminders. We may use and disclose medical information to contact and remind you about appointments. If you are not home, we may leave this information on your answering machine or in a message left with the person answering the phone.]

5. Sign-in Sheet. We may use and disclose medical information about you by having you sign in when you arrive at our office. We may also call out your name when we are ready to see you.

6. Notification and Communication with Family. We may disclose your health information to notify or assist in notifying a family member, your personal representative or another person responsible for your care about your location, your general condition or, unless you have instructed us otherwise, in the event of your death. In the event of a disaster, we may disclose information to a relief organization so that they may coordinate these notification efforts. We may also disclose information to someone who is involved with your care or helps pay for your care. If you are able and available to agree or object, we will give you the opportunity to object prior to making these disclosures, although we may disclose this information in a disaster even over your objection if we believe it is necessary to respond to the emergency circumstances. If you are unable or unavailable to agree or object, our health professionals will use their best judgment in communication with your family and others.

7. Marketing. Provided we do not receive any payment for making these communications, we may contact you to encourage you to purchase or use products or services related to your treatment, case management or care coordination, or to direct or recommend other treatments, therapies, health care providers or settings of care that may be of interest to you. We may similarly describe products or services provided by this practice and tell you which health plans we participate in., We may receive financial compensation to talk with you face-to-face, to provide you with small promotional gifts, or to cover our cost of reminding you to take and refill your medication or otherwise communicate about a drug or biologic that is currently prescribed for you, but only if you either: 1) have a chronic and seriously debilitating or life-threatening condition and the communication is made to educate or advise you about treatment options and otherwise maintain adherence to a prescribed course of treatment, or 2) you are a current health plan enrollee and the communication is limited to the availability of more cost-effective pharmaceuticals. If we make these communications while you have a chronic and seriously debilitating or life-threatening condition, we will provide notice of the following in at least 14-point type: 1) the fact and source of the remuneration; and 2) your right to opt out of future remunerated communications by calling the communicator's toll-free number. We will not otherwise use or disclose your medical information for marketing purposes or accept any payment for other marketing communications without your prior written authorization. The authorization will disclose whether we receive any financial compensation for any marketing activity you authorize, and we will stop any future marketing activity to the extent you revoke that authorization.

8. Sale of Health Information. We will not sell your health information without your prior written authorization. The authorization will disclose that we will receive compensation for your health information if you authorize us to sell it, and we will stop any future sales of your information to the extent that you revoke that authorization.

9. Required by Law. As required by law, we will use and disclose your health information, but we will limit our use or disclosure to the relevant requirements of the law. When the law requires us to report abuse, neglect or domestic violence, or respond to judicial or administrative proceedings, or to law enforcement officials, we will further comply with the requirement set forth below concerning those activities.

10. Public Health. We may, and are sometimes required by law to disclose your health information to public health authorities for purposes related to: 1) preventing or controlling disease, injury or disability; 2) reporting child, elder or dependent adult abuse or neglect; 3) reporting domestic violence; 4) reporting to the Food and Drug Administration problems with products and reactions to medications; and 5) reporting disease or infection exposure. When we report suspected elder or dependent adult abuse or domestic violence, we will inform you or your personal representative promptly unless in our best professional judgment, we believe the notification would place you at risk of serious harm or would require informing a personal representative we believe is responsible for the abuse or harm.

11. Health Oversight Activities. We may, and are sometimes required by law to disclose your health information to health oversight agencies during the course of audits, investigations, inspections, licensure and other proceedings, subject to the limitations imposed by federal and California law.

12. Judicial and Administrative Proceedings.We may, and are sometimes required by law, to disclose your health information in the course of any administrative or judicial proceeding to the extent expressly authorized by a court or administrative order. We may also disclose information about you in response to a subpoena, discovery request or other lawful process if reasonable efforts have been made to notify you of the request and you have not objected, or if your objections have been resolved by a court or administrative order.

13. Law Enforcement. We may, and are sometimes required by law, to disclose your health information to a law enforcement official for purposes such as identifying of locating a suspect, fugitive, material witness or missing person, complying with a court order, warrant, grand jury subpoena and other law enforcement purposes.

14. Coroners. We may, and are often required by law, to disclose your health information to coroners in connection with their investigations of deaths.

15. Organ or Tissue Donation. We may disclose your health information to organizations involved in procuring, banking or transplanting organs and tissues.

16. Public Safety. We may, and are sometimes required by law, to disclose your health information to appropriate persons in order to prevent or lessen a serious and imminent threat to the health or safety of a particular person or the general public.

17. Proof of Immunization. We will disclose proof of immunization to a school where the law requires the school to have such information prior to admitting a student if you have agree to the disclosure on behalf of yourself or your dependent.

18. Specialized Government Functions. We may disclose your health information for military or national security purposes or to correctional institutions or law enforcement officers that have you in their lawful custody.

19. Workers' Compensation. We may disclose your health information as necessary to comply with workers' compensation laws. For example, to the extent your care is covered by workers' compensation, we will make periodic reports to your employer about your condition. We are also required by law to report cases of occupational injury or occupational illness to the employer or workers' compensation insurer.

20. Change of Ownership. In the event that this medical practice is sold or merged with another organization, your health information/record will become the property of the new owner, although you will maintain the right to request that copies of your health information be transferred to another physician or medical group.

21. Breach Notification. In the case of a breach of unsecured protected health information, we will notify you as required by law. If you have provided us with a current email address, we may use email to communicate information related to the breach. In some circumstances our business associate may provide the notification. We may also provide notification by other methods as appropriate. [Note: Only use email notification if you are certain it will not contain PHI and it will not disclose inappropriate information. For example if your email address is "digestivediseaseassociates.com" an email sent with this address could, if intercepted, identify the patient and their condition.]

[*Add the following three activities, or any of the three, only if the organization engages or intends to engage in these activities.*]

22. Psychotherapy Notes. We will not use or disclose your psychotherapy notes without your prior written authorization except for the following: 1) your treatment, 2) for training our staff, students and other trainees, 3) to defend ourselves if you sue us or bring some other legal proceeding, 4) if the law requires us to disclose the information to you or the Secretary of HHS or for some other reason, 5) in response to health oversight activities concerning your psychotherapist, 6) to avert a serious threat to health or safety, or 7) to the coroner or medical examiner after you die. To the extent you revoke an authorization to use or disclose your psychotherapy notes, we will stop using or disclosing these notes.

23. Research. We may disclose your health information to researchers conducting research with respect to which your written authorization is not required as approved by an Institutional Review Board or privacy board, in compliance with governing law.

24. Fundraising. We may use or disclose your demographic information, the dates that you received treatment, the department of service, your treating physician, outcome information and health insurance status in order to contact you for our fundraising activities. If you do not want to receive these materials, notify the Privacy Officer listed at the top of this Notice of Privacy Practices and we will stop any further fundraising communications. Similarly, you should notify the Privacy Office if you decide you want to start receiving these solicitations again.

B. When This Medical Practice May Not Use or Disclose Your Health Information

Except as described in this Notice of Privacy Practices, this medical practice will, consistent with its legal obligations, not use or disclose health information which identifies you without your written authorization. If you do authorize this medical practice to use or disclose your health information for another purpose, you may revoke your authorization in writing at any time.

C. Your Health Information Rights

1. Right to Request Special Privacy Protections. You have the right to request restrictions on certain uses and disclosures of your health information by a written request specifying what information you want to limit, and what limitations on our use or disclosure of that information you wish to have imposed. If you tell us not to disclose information to your commercial health plan concerning healthcare items or services for which you paid for in full out-of-pocket, we will abide by your request, unless we must disclose the information for treatment or legal reasons. We reserve the right to accept or reject any other request, and will notify you of our decision.

2. Right to Request Confidential Communications. You have the right to request that you receive your health information in a specific way or at a specific location. For example, you may ask that we send information to a particular email account or to your work address. We will comply with all reasonable requests submitted in writing which specify how or where you wish to receive these communications.

3. Right to Inspect and Copy. You have the right to inspect and copy your health information, with limited exceptions. To access your medical information, you must submit a written request detailing what information you want access to, whether you want to inspect it or get a copy of it, and if you want a copy, your preferred form and format. We will provide copies in your requested form and format if it is readily producible, or we will provide you with an alternative format you find acceptable, or if we can't agree and we maintain the record in an electronic format, your choice of a readable electronic or hard-copy format. We will also send a copy to any other person you designate in writing. We will charge a reasonable fee which covers our costs for labor, supplies, postage, and if requested and agreed to in advance, the cost of preparing an explanation or summary, as allowed by federal and California law. We may deny your request under limited circumstances. If we deny your request to access your child's records or the records of an incapacitated adult you are representing because we believe allowing access

would be reasonably likely to cause substantial harm to the patient, you will have a right to appeal our decision. If we deny your request to access your psychotherapy notes, you will have the right to have them transferred to another mental health professional.

4. Right to Amend or Supplement. You have a right to request that we amend your health information that you believe is incorrect or incomplete. You must make a request to amend in writing, and include the reasons you believe the information is inaccurate or incomplete. We are not required to change your health information, and will provide you with information about this medical practice's denial and how you can disagree with the denial. We may deny your request if we do not have the information, if we did not create the information (unless the person or entity that created the information is no longer available to make the amendment), if you would not be permitted to inspect or copy the information at issue, or if the information is accurate and complete as is. If we deny your request, you may submit a written statement of your disagreement with that decision, and we may, in turn, prepare a written rebuttal. You also have the right to request that we add to your record a statement of up to 250 words concerning anything in the record you believe to be incomplete or incorrect. All information related to any request to amend or supplement will be maintained and disclosed in conjunction with any subsequent disclosure of the disputed information.

5. Right to an Accounting of Disclosures. You have a right to receive an accounting of disclosures of your health information made by this medical practice, except that this medical practice does not have to account for the disclosures provided to you or pursuant to your written authorization, or as described in paragraphs 1 (treatment), 2 (payment), 3 (health care operations), 6 (notification and communication with family) and 18 (specialized government functions) of Section A of this Notice of Privacy Practices or disclosures for purposes of research or public health which exclude direct patient identifiers, or which are incident to a use or disclosure otherwise permitted or authorized by law, or the disclosures to a health oversight agency or law enforcement official to the extent this medical practice has received notice from that agency or official that providing this accounting would be reasonably likely to impede their activities.

6. You have a right to notice of our legal duties and privacy practices with respect to your health information, including a right to a paper copy of this Notice of Privacy Practices, even if you have previously requested its receipt by email.

If you would like to have a more detailed explanation of these rights or if you would like to exercise one or more of these rights, contact our Privacy Officer listed at the top of this Notice of Privacy Practices.

D. Changes to this Notice of Privacy Practices

We reserve the right to amend our privacy practices and the terms of this Notice of Privacy Practices at any time in the future. Until such amendment is made, we are required by law to comply with this Notice. After an amendment is made, the revised Notice of Privacy Protections will apply to all protected health information that we maintain, regardless of when it was created or received. We will keep a copy of the current notice posted in our reception area, and a copy will be available at each appointment. [*For practices with websites add*: We will also post the current notice on our website.]

E. Complaints

Complaints about this Notice of Privacy Practices or how this medical practice handles your health information should be directed to our Privacy Officer listed at the top of this Notice of Privacy Practices.

If you are not satisfied with the manner in which this office handles a complaint, you may submit a formal complaint to:

Region IX
Office for Civil Rights
U.S. Department of Health & Human Services
90 7th Street, Suite 4-100
San Francisco, CA 94103
(800) 368-1019; (800) 537-7697 (TDD)

The complaint form may be found at www.hhs.gov/hipaa/filing-a-complaint/index.html. You will not be penalized in any way for filing a complaint.

HIPAA Notice of Privacy Practices—Sample Acknowledgment of Receipt

[Physician Practice Name and Address]

[Name or Title and Telephone Number of Privacy Officer]

I hereby acknowledge that I received a copy of this medical practice's Notice of Privacy Practices. I further acknowledge that a copy of the current notice will be posted in the reception area, and that a copy of any amended Notice of Privacy Practices will be available at each appointment.

☐ I would like to receive a copy of any amended Notice of Privacy Practices by email at: _____.

Signed: _____ Date: _____

Print Name: _____ Telephone: _____

If not signed by the patient, please indicate relationship:

☐ parent or guardian of minor patient

☐ guardian or conservator of an incompetent patient

Name and Address of Patient: _____

_____

_____

HIPAA Notice of Privacy Practices—Sample Acknowledgment Tracking Information

Name of Patient: _____

Address: _____

_____

For Office Use Only:

Date received:	Processed by:
Practice Follow-up: □ Yes □ No	Date of Practice Follow-up:

Complete the following only if the Patient refuses to sign the Acknowledgment:

Efforts to obtain:

_____

_____

Reasons for refusal:

_____

_____

HIPAA Privacy Policy Statement—Sample Policy (Updated September 2013)

Disclaimer: CMA/PrivaPlan Privacy Policy Statement (45 C.F.R. §164.530)

The information provided in this document does not constitute, and is no substitute for, legal or other professional advice. Users should consult their own legal or other professional advisors for individualized guidance regarding the application of the law to their particular situations, and in connection with other compliance-related concerns.

To customize this template document, replace all of the text that is presented in brackets (i.e. "[" and "]") with text that is appropriate to your organization and circumstances. After completing the customization of this document, the document should be reviewed by an attorney who is familiar with health privacy laws and regulations in the state(s) in which the organization maintains its facilities, and who is in a position to provide legal counsel to your organization.

NOTE: Each of the following sections contains a basic element of HIPAA privacy protection. To the extent possible, you should reword each section to reflect the specific practices to be followed in this organization. For example, you may decide that certain functions may only be performed by certain personnel or within certain departments or with a certain form of management approval. Where appropriate, you may wish to include sanctions provisions. Sanctions are the disciplinary measures to be taken in the event of careless disregard or deliberate violation of any of these provisions. You may also wish to keep the documentation of sanctions in a separate sanctions policy.

PRIVACY POLICY STATEMENT
[Physician Practice Name and Address]
[Name or Title and Telephone Number of Privacy Officer]

Purpose: The following privacy policy is adopted to ensure that [Name of Physician Practice] complies fully with all federal and state privacy protection laws and regulations. Protection of patient privacy is of paramount importance to this medical practice. Violations of any of these provisions will result in severe disciplinary action including termination of employment and possible referral for criminal prosecution.

Effective Date: This Policy is in effect as of [effective date].

Expiration Date: This Policy remains in effect until superseded or canceled.

Privacy Official

It is the policy of this medical practice that a specific individual or individuals within our workforce are assigned the responsibility of implementing and maintaining the privacy policies and procedures of this medical practice in compliance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rule requirements and California law. Furthermore, it is the policy of this medical practice that these individuals will be provided sufficient resources and authority to fulfill their responsibilities. At a minimum, this medical practice will designate one individual the Privacy Official and that individual or his/her designee shall be the contact person to handle all questions, concerns or complaints regarding the privacy and security of protected health information.

Uses and Disclosures of Protected Health Information

This medical practice shall only use or disclose protected health information as required or permitted by our Notice of Privacy Practices, HIPAA and California law and the individual who is the subject of the information has received our Notice of Privacy Practices and acknowledged receipt of the Notice.

This medical practice may use protected health information it obtains or creates for the proper management and administration of this medical practice or to carry out its legal responsibilities as permitted or required by the law.

Notice of Privacy Practices

It is the policy of this medical practice that we will adopt, maintain and comply with our Notice of Privacy Practices, which shall be consistent with HIPAA and California law.

It is the policy of this medical practice that a Notice of Privacy Practices must be published, which describes in sufficient detail this medical practice's privacy practices. This notice must be provided to all subject individuals at the first patient encounter if possible, and good faith efforts made to obtain a written acknowledgment of receipt, and that all uses and disclosures of protected health information be done in accordance with this medical practice's Notice of Privacy Practices. The most current Notice of Privacy Practices will be posted in our "waiting room" area and copies will be available for distribution at our reception desk.

NOTE: Organizations with practice websites should include the following: It is the policy of this medical practice to prominently post the Notice of Privacy Practices on our website.

This medical practice's Notice of Privacy Practices will be revised whenever there are material changes to our privacy policy or practices including changes in law.

Restriction Requests

It is the policy of this medical practice that consideration must be given to all requests for restrictions on uses and disclosures of protected health information as published in this medical practice's Notice of Privacy Practices. It is the policy of this medical practice that if a particular restriction is agreed to, then this medical practice will document the restriction in writing and abide by that restriction unless the use or disclosure is necessary to provide emergency treatment. To the extent restricted information is disclosed for emergency treatment, this medical practice must request that the information is not further used or disclosed.

Additionally, it is the policy of this medical practice that any request by a patient or their personal representative for a restriction on disclosure of protected health information to a health plan (to whom the patient is a subscriber or plan member) will be honored if the patient pays out-of-pocket and in full for the services rendered, and where the disclosure is for purposes of carrying out payment or health care operations and is not otherwise required by law. Such requests may be rescinded for failure to make or maintain payment for services.

Workforce Access to Protected Health Information

It is the policy of this medical practice that access to protected health information must be granted to each employee or contractor based on the assigned job functions of the employee or contractor. It is also the policy of this medical practice that such access privileges should not exceed those necessary to accomplish the assigned job function.

Access to Protected Health Information by the Individual

It is the policy of this medical practice that access to protected health information must be granted to the person who is the subject of such information upon request. Individuals must be permitted to inspect their records during business hours within five (5) working days after receipt of the request and upon payment of reasonable clerical costs incurred in locating and making the records available. If an individual requests copies of their records, this medical practice must transmit the copies within fifteen (15) days after receipt of the written request. Access may be granted as either physical or electronic copies or inspection based upon the preference of the patient.

For protected health information that is maintained electronically, it is the policy of this medical practice to provide electronic copies of the protected health information in the form and format requested by the patient if it is readily reproducible and if not in a mutually agreeable form and format, or in paper form if a mutually agreeable form and format is not available. Electronic copies will be provided to third parties at the patient's specific direction where such request is in writing.

It is the policy of this medical practice to inform the person requesting access, of the location of protected health information if we do not physically possess such protected health information but have knowledge of its location.

All requests will be reviewed to determine that access does not create endangerment or is contrary to HIPAA or California law.

This medical practice will charge a reasonable cost based fee to the patient for paper or electronic copies; where applicable this cost based fee may include the cost of skilled labor to assemble and create an electronic copy and/or the cost of media requested by the patient for the copy.

Amendment of Incomplete or Incorrect Protected Health Information

It is the policy of this medical practice that all requests for amendment of incorrect protected health information maintained by this medical practice will be considered in a timely fashion. If such requests demonstrate that the information is actually incorrect, this medical practice will allow amending language to be added to the appropriate document and this addition will be done in a timely fashion. This medical practice will make reasonable efforts to give notice of such corrections to any organization with which the incorrect information has been shared. This medical practice will deny amendment requests where the protected health information is accurate and complete, has not been created by this practice, or if this practice does not have the information. This medical practice will provide the patient with written notice of the denial with information about the denial, and how the patient can disagree with the denial, including contact information to file complaints to this practice and to U.S. Department of Health and Human Services (HHS). In cases of denial, the patient will be allowed the opportunity to provide a written statement with respect to any item or statement the patient believes to be incomplete or incorrect. These statements are limited to 250 words per incomplete or incorrect item. Such a statement must be attached to the patient's record and included with each disclosure of the contested portion of the patient's records.

Integrity of Protected Health Information

It is the policy of this medical practice to protect and preserve the integrity of protected health information. Erroneous information or entries will be corrected in a manner that indicates the error, date in which it was corrected, and the identity of the person making the correction. No person may change, remove or strike through protected health information related to treatment or diagnosis without the proper documentation of the change.

NOTE: Organizations with electronic health record systems should include the following: This medical practice will ensure that the electronic health record system automatically records and preserves any change or deletion of any electronically stored medical information and record the identity of the person who accessed and/or changed the patient's record, the date and time it was accessed, and the change that was made to the information.

Access by Personal Representatives

It is the policy of this medical practice that access to protected health information must be granted to personal representatives of individuals as though they were the individuals themselves, except in cases where granting access to the personal representative would be detrimental to the individual or to a third-party.

Access to Minor's Records

It is the policy of this medical practice that access to protected health information of minors will be granted to the minor's parent or legal guardian, except in cases where the records related to treatment in which the minor is legally authorized to consent or where granting access to the parent or legal guardian would be detrimental to the minor.

Confidential Communications Channels

It is the policy of this medical practice to provide patients with the right to request communications of protected health information in a specific way or at a specific location. This practice will comply with all reasonable requests for confidential communications channels requested by the individuals, to the extent possible.

Disclosure Accounting

It is the policy of this medical practice that an accounting of all disclosures of protected health information be provided to individuals upon request pursuant to 45 C.F.R. §164.528. Such accounting of disclosures of protected health information will be maintained for at least six (6) years after the disclosure was made.

Communicating with a Patient's Family, Friends or Others

It is the policy of this medical practice that a patient may grant limited access to their medical information to a family member, other relative, domestic partner, personal friend or any other person identified by the patient who is not the legal personal representative of patient based upon written, verbal or implied permission by the patient and this medical practice is unaware of any expressed preference to the contrary. Such disclosures must be limited to medical information that is directly relevant to that person's involvement with the patient's care or payment related to the patient's health care. Any permission shall be documented and periodically confirmed with the patient.

It is the policy this medical practice to provide a family member, other relative, domestic partner, personal friend of a deceased patient, or any other person previously identified by the deceased patient, limited access to protected health information under the same circumstances that disclosures of this information would have been made when the patient was alive. Such disclosures must be limited to medical information that is directly relevant to that person's involvement with the patient's care or payment related to the patient's health care and this medical practice is unaware of any expressed preference to the contrary.

Immunizations

It is the policy of this medical practice to provide immunization data to a patient's school where such data is required for admission and where the patient or their personal representative has provided an informal request for such release such as a verbal request. This medical practice will document in the medical record the date and time of such informal requests. Immunization data will be disclosed in a secure manner.

Deceased Individuals

It is the policy of this medical practice that privacy protections extend to information concerning deceased individuals including protection of a decedent's protected health information for fifty (50) years after the date of their death.

Minimum Necessary Use and Disclosure of Protected Health Information

It is the policy of this medical practice that for all routine and recurring uses and disclosures of PHI (except for uses or disclosures made:1) for treatment purposes, 2) to the individual who is the subject of the information, 3) pursuant to the patient's written authorization, 4) as required by law, 5) for HIPAA investigations and compliance purposes) the uses and disclosure of protected health information must be limited to the minimum amount of information needed to accomplish the purpose of the use or disclosure. Non-routine uses and disclosures will be handled pursuant to established criteria. All requests for protected health information (except as specified above) must be limited to the minimum amount of information needed to accomplish the purpose of the request.

Verification of Identity

It is the policy of this medical practice that the identity and authority of all persons who request access to protected health information be reasonably verified before such access is granted.

Marketing Activities

It is the policy of this medical practice that any uses or disclosures of protected health information for marketing activities will be done only after a valid authorization is in effect. Marketing is defined as any communication about a product or service intended to induce or encourage the purchase or use of a product or service where this medical practice receives financial remuneration in exchange for making the communication. Marketing does not include communications that are made for: 1) case management or care coordination or to direct or recommend alternative treatments, therapies, health care providers or settings of care; 2) the use of products and services in treatment, 3) or a face-to-face communication made by us to the patient, or a promotional gift of nominal value given to the patient to be marketing, unless direct or indirect remuneration is received from a third party and the communication is not to a health plan enrollee concerning: 1) a provider's participation in the health plan's network, 2) the extent of covered benefits, or 3) the availability of more cost-effective pharmaceuticals.

This medical practice may make remunerated communications tailored to individual patients with chronic and seriously debilitating or life-threatening conditions for the purpose of educating or advising them about treatment options or maintaining adherence to a prescribed course of treatment, without a signed patient authorization. If we do so, we will disclose in at least 14-point type the fact that the communication is remunerated, the name of the party remunerating us, and the fact the patient may opt-out of future remunerated communications by calling a toll-free number. This medical practice will stop any further remunerated communications within 30 days of receiving an opt-out request.

Authorizations

It is the policy of this medical practice that a valid authorization will be obtained for all disclosures that are not required or permitted under the CMIA and HIPAA.

Mental Health Records

It is the policy of this medical practice to require a specific authorization for any use or disclosure of psychotherapy notes, as defined in the HIPAA regulations, except for treatment, payment or health care operations as follows: 1) use by originator for treatment; 2) use for training physicians or other mental health professionals as authorized by the regulations; 3) use or disclosure in defense of a legal action brought by the individual whose records are in issue; 4) use or disclosures as required by law, to HHS in conjunction with HIPAA enforcement, or as authorized by law to enable health oversight agencies concerning the originator of the psychotherapy notes; 5) use or disclosure to the coroner or medical examiner; or 6) use or disclosure necessary to comply with obligations to make Tarasoff warnings.

Complaints

It is the policy of this medical practice that all complaints relating to the protection of health information be investigated and resolved in a timely fashion. Furthermore, it is the policy that all complaints will be addressed to [name or job title of person authorized to handle complaints (i.e., Privacy Official)] who is duly authorized to investigate complaints and implement resolutions if the complaint stems from a valid area of non-compliance with the HIPAA Privacy and Security Rule.

Prohibited Activities—No Retaliation or Intimidation

It is the policy of this medical practice that no employee or contractor may engage in any intimidating or retaliatory acts against persons who file complaints or otherwise exercise their rights under HIPAA regulations. It is also the policy of this medical practice that no employee or contractor may condition treatment, payment, enrollment or eligibility for benefits on the provision of an authorization to disclose protected health information except as expressly authorized under the regulations.

Responsibility

It is the policy of this medical practice that the responsibility for designing and implementing procedures to implement this policy lies with the Privacy Official.

Mitigation

It is the policy of this medical practice that the effects of any unauthorized use or disclosure of protected health information be mitigated to the extent possible.

Safeguards

It is the policy of this medical practice that appropriate physical safeguards will be in place to reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the HIPAA Privacy Rule. These safeguards will include physical protection of premises and PHI, technical protection of PHI maintained electronically and administrative protection. These safeguards will extend to the oral communication of PHI. These safeguards will extend to PHI that is removed from this organization.

Social Media

It is the policy of this medical practice to maintain appropriate restrictions and guidance related to the use of social media and disclosure of PHI.

Business Associates

It is the policy of this medical practice that business associates must be contractually bound to protect health information to the same degree as set forth in this policy. It is also the policy of this medical practice that business associates who violate their agreement will be dealt with first by an attempt to correct the problem, and if that fails by termination of the agreement and discontinuation of services by the business associate. Business associate agreements must provide sufficient protection and communication in the event of a breach of unsecured protected health information, and agreements must contain sufficient language regarding the business associate's agents and subcontractors similar protections.

Training and Awareness

It is the policy of this medical practice that all members of our workforce have been trained on the policies and procedures governing protected health information and how this medical practice complies with the HIPAA Privacy and Security Rules. It is also the policy of this medical practice that new members of our workforce receive training on these matters within a reasonable [you may elect to enter the exact time frame] time after they have joined the workforce. It is the policy of this medical practice to provide training should any policy or procedure related to the HIPAA Privacy and Security Rule materially change. This training will be provided within a reasonable time [you may elect to enter the exact time frame] after the policy or procedure materially changes. Furthermore, it is the policy of this medical practice that training will be documented indicating participants, date and subject matter.

Material Change

It is the policy of this medical practice that the term "material change" for the purposes of these policies is any change in our HIPAA compliance activities.

Sanctions

It is the policy of this medical practice that sanctions will be in effect for any member of the workforce who intentionally or unintentionally violates any of these policies or any procedures related to the fulfillment of these policies. Such sanctions will be recorded in the individual's personnel file.

Retention of Documentation

It is the policy of this medical practice that the HIPAA Privacy Rule document retention requirement of six (6) years will be strictly adhered to. All documentation designated by HIPAA in this retention requirement will be maintained in a manner that allows for access within a reasonable period of time. This documentation retention time requirement may be extended at this medical practice's discretion to meet with other governmental regulations or those requirements imposed by our professional liability carrier.

Regulatory Currency

It is the policy of this medical practice to remain current in our compliance program with HIPAA regulations.

Cooperation with Privacy Oversight Authorities

It is the policy of this medical practice that oversight agencies, including but not limited to, the Office for Civil Rights of the Department of Health and Human Services be given full support and cooperation in their efforts to ensure the protection of health information within this organization. It is also the policy of this medical practice that all personnel must cooperate fully with all privacy compliance reviews and investigations.

Investigation and Enforcement

It is the policy of this medical practice that in addition to cooperation with federal or State authorities, this medical practice will follow procedures to ensure that investigations are supported internally and that members of our workforce will not be retaliated against for cooperation with any authority. It is our policy to attempt to resolve all investigations and avoid any penalty phase if at all possible.

HIPAA Security Policy Statement—Sample Policy (Updated September 2013)

Disclaimer: CMA/PrivaPlan Security Policy Statement (45 C.F.R. §§164.302 et seq.)

The information provided in this document does not constitute, and is no substitute for, legal or other professional advice. Users should consult their own legal or other professional advisors for individualized guidance regarding the application of the law to their particular situations, and in connection with other compliance-related concerns.

To customize this template document, replace all of the text that is presented in brackets (i.e. "[" and "]") with text that is appropriate to your organization and circumstances. After completing the customization of this document, the document should be reviewed by an attorney who is familiar with health privacy laws and regulations in the state(s) in which the organization maintains its facilities, and who is in a position to provide legal counsel to your organization.

Some of these suggested policies are addressable security measures and not required by HIPAA. Your organization should determine which addressable measure it will implement and the subsequent documentation if you decide that it is not reasonable or appropriate to implement the measure or if an equivalent alternative exists.

NOTE: Each of the following sections contains a basic element of HIPAA security protection. To the extent possible, you should reword each section to reflect the specific practices to be followed in this organization. For example, you may decide that certain functions may only be performed by certain personnel or within certain departments or with a certain form of management approval. Where appropriate, you may wish to include sanctions provisions. Sanctions are the disciplinary measures to be taken in the event of careless disregard or deliberate violation of any of these provisions. You may also wish to keep the documentation of sanctions in a separate sanctions policy.

SECURITY POLICY STATEMENT
[Physician Practice Name and Address]
[Name or Title and Telephone Number of Security Officer]

Purpose: The following security policy is adopted to ensure that [insert Physician Practice name] complies appropriately with applicable federal and state security protection laws and regulations. Protection of electronic protected health information (PHI) is of great importance to this organization. Violations of any of these provisions will result in appropriate disciplinary action including possible termination of employment.

Effective Date: This policy is in effect as of [effective date].

Expiration Date: This policy remains in effect until superseded or canceled.

Security Official: For questions or comments concerning this policy, contact:

Name: [Insert Name of Security Official]
Title: [Insert Job Title]
Contact: [Insert Contact Information]

[Include additional introductory material as appropriate.]

Assigning Privacy and Security Responsibilities

It is the policy of this medical practice that a specific individual or individuals within our workforce are assigned the responsibility of implementing and maintaining the HIPAA Privacy and Security Rule's requirements. Furthermore, it is the policy of this medical practice that these individuals will be provided sufficient resources and authority to fulfill their responsibilities. One individual shall be designated as the HIPAA Security Official.

Risk Analysis

It is the policy of this medical practice that a risk analysis has been completed and is periodically updated to assess potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic PHI. It is the policy of this medical practice that the risk analysis includes a review of the critical nature of electronic PHI and related applications or business processes with a subsequent ranking or prioritization (criticality analysis).

[Insert the following if your medical practice attests to meaningful use of an electronic health record system under Medicare or Medi-Cal incentive program.]

It is also our policy to conduct or review a HIPAA Security Risk Analysis as a core objective of electronic health record meaningful use with each meaningful use attestation year, if applicable.

Risk Management

It is the policy of this medical practice that security measures are in place and maintained sufficient to reduce risks and vulnerabilities to reasonably appropriate level to:

- Ensure the confidentiality, integrity and availability of all electronic PHI that this medical practice creates, maintains, stores, or transmits;

- Protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI;
- Protect against any reasonably anticipated uses or disclosures of electronic PHI that is not permitted by HIPAA or applicable state law;
- Ensures that all members of the workforce are aware of these requirements and comply with them.

It is our policy to use the results of a HIPAA Security Risk Analysis and any security incidents or breaches of protected health information to identify new risks and manage those as feasible.

Sanctions

It is the policy of this medical practice that sanctions will be applied to workforce members who fail to comply with the security policies and procedures.

Information System Activity Review

It is the policy of this medical practice that information system activity records are regularly reviewed such as security incident tracking reports, intrusion detection logs or alerts, and there is appropriate review of systems such as the practice management or electronic health record.

Supervision

It is the policy of this medical practice that an authorized, knowledgeable person must supervise maintenance personnel whenever work is being done on a system that contains or processes electronic PHI. It is also the policy of this medical practice that access authorization for maintenance personnel must be set appropriately for the jobs assigned to each.

Personnel Clearance

It is the policy of this medical practice that personnel be cleared before access to electronic PHI is allowed.

Personnel and Workforce Termination

It is the policy of this medical practice that personnel and workforce will have all access to electronic PHI terminated as soon as practicable after they are terminated. This will include physical access to our facility as well as technical access to systems including web-based applications.

Training and Awareness

It is the policy of this medical practice that all employees and contractors receive training in security awareness and in the security procedures to be followed during the performance of their duties, including specific security training in the use of our electronic systems including remote and mobile computing use. It is the policy of this medical practice that periodic reminders and training will be provided to the workforce.

Protection from Malicious Software

It is the policy of this medical practice that it will implement and maintain procedures for detecting, reporting and guarding against malicious software. It is the policy of this medical practice that all members of the workforce will be periodically reminded and trained regarding this policy. It is the policy of this medical practice to restrict access to our networks and introduction of media or workstations that are not trusted.

Log in Monitoring

It is the policy of this medical practice that log in attempts and discrepancies will be monitored to the extent practicable. It is the policy of this medical practice to disable access after a pre-determined number of failed log in attempts.

Password Management

It is the policy of this medical practice that a written procedure will be followed to create and assign passwords, which will include periodic changing and safeguarding of passwords including sufficient password complexity and the prohibition against sharing of passwords.

Security Incident Policy

It is the policy of this medical practice that all security incidents (suspected or actual) will be identified and an appropriate response developed, including but not limited to documentation in writing. Any harmful effects or violations will be mitigated to the extent practicable. All responses and follow up actions will be documented. It is the policy of this medical practice to coordinate security incident response with Breach Notification policies.

Contingency Plans

It is the policy of this medical practice that a contingency plan is in place and maintained. The contingency plan includes procedures for data backup, disaster recovery including restoration of data, and emergency mode operations. It is the policy of this organization that the contingency plan includes a procedure to allow facility access in support of restoration of lost data and to support emergency mode operations in the event of an emergency. It is the policy of this medical practice that access control will include procedures for emergency access to electronic PHI.

Testing

It is the policy of this medical practice that all security controls and measures in place be periodically tested to ensure proper functioning. It is also the policy of this medical practice that all procedures adopted to protect the confidentiality, integrity and availability of information and information services be tested to ensure that important security considerations have not been overlooked. It is also the policy of this medical practice that contingency plans and related measures will be periodically tested to ensure proper functioning and to maintain readiness in the event of a contingency.

Evaluation

It is the policy of this medical practice that a periodic technical and non-technical evaluation will be conducted to audit the effectiveness of the security controls and measures in place in consideration of environmental or operational changes.

Audit

It is the policy of this medical practice that audit controls are in place to record and examine the activity of all information systems that contain or use electronic PHI. This organization will maintain procedures to protect electronic PHI from improper alteration or destruction and to routinely authenticate that electronic PHI retains its integrity (including but not limited to version control, read only privileges). It is the policy of this medical practice to not disable audit controls.

Authentication

It is the policy of this medical practice that all information system users be authenticated before access to information processing resources is allowed. Specifically, each user must have his or her own system account, and passwords must never be shared. It is the policy of this medical practice that authentication controls are required for every system accessing PHI and the controls are sufficiently strong.

Access and Termination

It is the policy of this medical practice that authority to access electronic PHI be granted or supervision be provided to users who will work with electronic PHI. When these users no longer require their access or are terminated, all authorization will cease including the revocation and deletion of passwords, user IDs and system privileges. It is the policy of this medical practice to control access modification and document all actions where access, modification or termination takes place noting the user/individual, date and action.

Access to Protected Health Information

It is the policy of this medical practice that all access control mechanisms must be configured to allow access only to the information and information processing functions needed by each employee or contractor to perform their assigned duties. It is also the policy of this medical practice that proper procedures must be followed whenever access to health information is authorized, established or modified and that records of access authorizations must be maintained. Access will be granted and maintained to the extent possible at a system level, role or job function (and application software) level, and workstation or device level. It is the policy of this medical practice that access control will include unique name/ and or numbers to identify and track user identity. It is the policy of this medical practice that access controls will include automatic log offs for unattended computer sessions and, as appropriate, applicable encryption of electronic PHI (including system level encryption for stored data, and stored data on other devices such as workstations, portable devices and backup media). It is the policy of this medical practice that appropriate password protection will be implemented. It is the policy of this medical practice that emergency access will be maintained by relying on a backup list of user IDs and passwords.

Automatic Logoff

It is the policy of this medical practice to enable automatic log off after a period of inactivity for both workstations and applications with PHI. Log off times will be evaluated based on risk.

Encryption

It is the policy of this medical practice to deploy encryption for all transmissions of electronic PHI. Data at rest will be encrypted wherever feasible.

Device and Media Access Control

It is the policy of this medical practice that reusable and portable media, such as tapes, removable storage drives, USB memory sticks, hardware (including hard drives and SSI flash drive memory in workstations), or any other device that may contain PHI (including multifunction printers, facsimile machines, and diagnostic devices) that contains electronic PHI must be securely erased or otherwise destroyed before being discarded to prevent unauthorized access to electronic PHI. This policy extends to media that will be re-used by another party. It is the policy of this medical practice to safeguard and account for the receipt and removal of all hardware and media containing electronic PHI. It is the policy of this medical practice to backup devices that contain critical electronic PHI or applications prior to their relocation as appropriate.

Physical Access Control

It is the policy of this medical practice that areas to limit physical access to electronic information systems (including diagnostic equipment that maintains electronic PHI) to those properly authorized. It is also the policy of this medical practice that appropriate safeguards are in place to protect these systems and the electronic PHI they contain from tampering, theft or destruction. It is the policy of this medical practice that visitors sign in and are verified and monitored. It is the policy of this medical practice to review and supervise any repairs or modifications to the facility that could compromise security. It is the policy of this medical practice to maintain a facility security plan documenting these controls.

Workstation Use Guidelines

It is the policy of this medical practice that workstations be positioned in such a manner as to avoid accidental, unauthorized exposure of health information. It is the policy of this medical practice that displays be locked or logged off when unattended. It is the policy of this medical practice that access to workstations be restricted to authorized users. This workstation policy extends to desktop computers, laptop computers, smartphones, tablet PCs, mobile devices, electronic diagnostic equipment and all storage media connected or stored in the immediate environment. It is the policy of this medical practice to document the movements of all hardware and electronic media to sufficiently control and safeguard these devices and their PHI. It is the policy of this medical practice to backup data and PHI on equipment prior to it being moved.

Secure Data Transmission

It is the policy of this medical practice that data communications that contain electronic PHI must be encrypted or transmitted using a secure transmission protocol if they traverse public networks such as the Internet. It is also the policy of this medical practice that all data transmission methods must incorporate data integrity and authentication controls.

Configuration Management

It is the policy of this medical practice that proper procedures be followed for the installation or removal of all hardware devices or software programs. It is also the policy of this medical practice that the hardware/software inventory must be kept current and that the configuration must be documented in sufficient detail to be rebuilt in the case of an emergency.

Business Associates

It is the policy of this medical practice that business associates must be contractually bound to protect electronic PHI as required in applicable federal regulations. It is also the policy of this medical practice that business associates who violate their agreement will be dealt with first by an attempt to correct the problem, and if that fails by termination of the agreement and discontinuation of services by the business associate.

Breach Notification

It is the policy of this medical practice that it will comply with HIPAA and California breach notification requirements including investigation of any breach of unsecured PHI or unencrypted PHI upon discovery, appropriate risk assessments to determine probability of impermissible use of PHI and as appropriate individual notification (including substitute notices and media notice where applicable) and notification to the California Attorney General and the Secretary of the U.S. Department of Health and Human Services.

[Note: Be sure to implement and train your workforce on the breach notification policies and procedures]

Document Retention, Availability and Currency

It is the policy of this medical practice that these policies and all related procedures be retained for six (6) years from the date of its creation or the date when it was last in effect, whichever is later. It is also the policy of this medical practice to make this documentation available to those persons responsible for implementing the related procedures and that this documentation and policy will be kept current in response to relevant environmental or operational changes or changes in law.

Investigation and Enforcement

It is the policy of this medical practice that in addition to cooperation with federal and state security oversight authorities, this medical practice will follow procedures to ensure that investigations are supported internally and that members of our workforce will not be retaliated against for cooperation with any authority. It is our policy to attempt to resolve all investigations and avoid any penalty phase if at all possible.