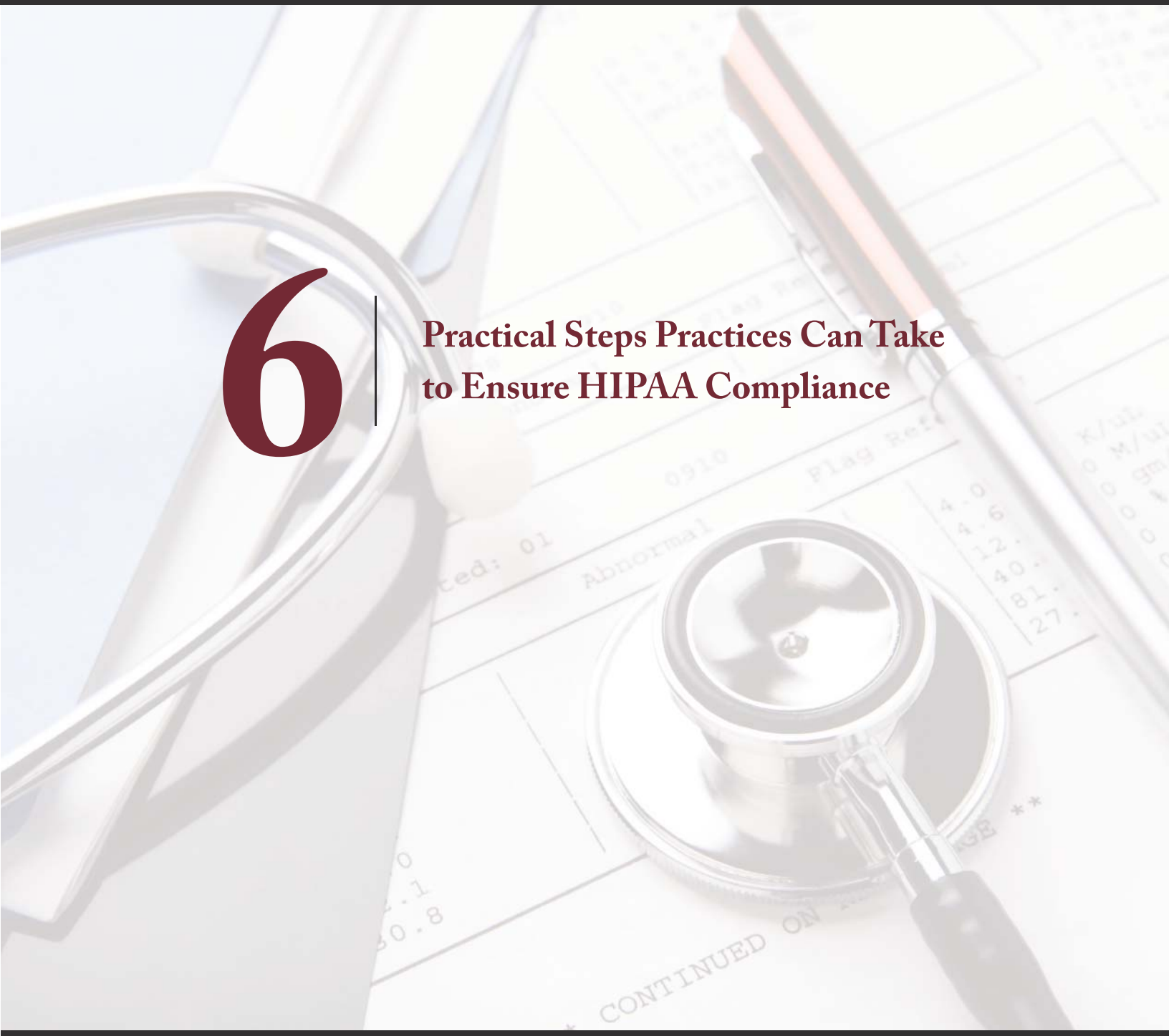
Best Practices

A guide for improving the efficiency and quality of your practice



6 Practical Steps Practices Can Take to Ensure HIPAA Compliance

CMA FOUNDATION

CMA California Medical Association

6

Practical Steps Practices Can Take to Ensure HIPAA Compliance

By David Ginsberg, PrivaPlan Associates

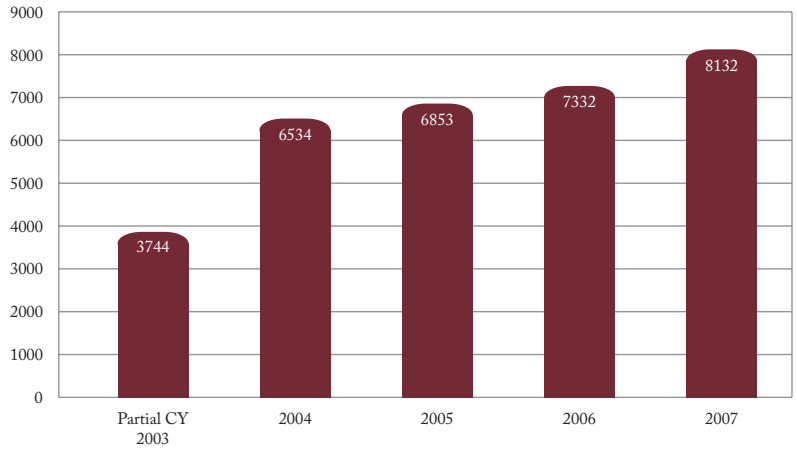
Most medical practices feel they have done all they need to do to satisfy Health Insurance Portability and Accountability Act (HIPAA) requirements and are reluctant to dedicate precious resources to additional compliance efforts. However, a number of gaps can expose medical practices to patient identity theft and violation of state laws that may be far stricter than HIPAA requirements.

Rather than reviewing HIPAA regulations in depth, this chapter provides an overview of information that will help you remain HIPAA compliant.

HIPAA ENFORCEMENT

HIPAA enforcement is real. The latest data from the Office of Civil Rights (OCR) show that complaints and investigations are increasing. As seen in Figure 1 below, HIPAA complaints have increased since 2003 by 117%. Most complaints are initiated by disgruntled employees.

Figure 1 - Health Information Privacy Complaints Received by Calendar Year



HIPAA COMPLIANCE RESOURCE

For an in-depth guide to HIPAA compliance, medical practices can purchase a complete do-it-yourself tool for HIPAA compliance developed by the California Medical Association (CMA) and its HIPAA partner, PrivaPlan Associates, at www.privaplan.com. Physicians in other areas should contact their state and local medical associations or PrivaPlan for more specific information about HIPAA compliance.

For these reasons, it is more critical than ever for physicians to review their current policies and procedures and upgrade them, if necessary.

Federal law does not create what is known as a private cause of action under HIPAA. In other words, individuals cannot sue for a privacy or security violation citing the HIPAA regulation. Only the federal government can enforce HIPAA and take covered entities to court for violations. However, some states have allowed private parties to bring actions seeking remedies for violations of HIPAA.

So, while HIPAA enforcement has been driven by complaints to either OCR or the Centers for Medicare & Medicaid Services (CMS), these cases have opened the door for successful private lawsuits against physicians when a privacy or security violation occurs.

HOW CAN YOU LOWER YOUR RISK?

The best defense against a HIPAA-related action is to not have a privacy or security violation occur. Here are the minimum steps any HIPAA-covered entity should take:

1. Periodically review your HIPAA privacy and security compliance efforts.
2. Ensure your policies and procedures are up-to-date.
3. Ensure that your policies and procedures actually "work," are understood by employees, and are implemented.
4. Ensure your training is up-to-date for all employees, board members, key contractors, etc. Employees should be required to annually review and sign a statement that they have read and understand the office's HIPAA privacy policies. (This information should be stored in personnel files.)
5. Ensure that key procedures are in place (such as the complaint procedure).
6. Ensure that your business associates have written agreements in place.
7. Ensure that you report and respond to any and all privacy and security incidents.
8. Ensure that your workforce and patients understand they will not be retaliated against if they complain about or notify you of a privacy or security breach.

MEDICAL IDENTITY THEFT

Medical identity theft is on the rise. In some cases protected health information is stolen to submit fraudulent claims; in others the information is being used to obtain health care coverage itself (i.e., the identity of an insured individual is assumed). And the risk comes not only from outside sources such as hackers. You must also ensure that sensitive patient data is available only to staff who need to access that data.

Some Practical Steps You Can Take

Establish (and Follow) Workforce Clearance Procedures

It has become increasingly important to do effective criminal background checks on employees who will have access to protected health information. Be sure to follow state and federal laws regarding how you notify a new employee of an impending background check and how you apply the findings.

Develop Effective Workforce Access and Authorization Protocols

In the "old days" it would take a large truck to steal information on even a small solo practice's patients. Today it requires a USB thumb drive and a few minutes. As more and more organizations convert to electronic health records and use portable devices, this threat becomes greater.

Are employees restricted to accessing only the information needed for their jobs? If not, most practice management systems have security features that will allow you to limit access by user. We strongly recommend contacting your vendor to find out how to use this feature.

Establish Effective Workforce Termination Procedures

Policies should be in place to terminate all access to protected health information, including systems and building access, immediately upon the termination of an

employee. Policies should be in place to discourage the sharing of system passwords. If you provide staff with keys to your office, make sure each key is clearly stamped "Do not duplicate." This will alert locksmiths not to make duplicate keys. Finally, be cautious when giving employees or others access to your Medicare and Medicaid provider transaction access numbers (PTAN). There have been many cases where these numbers have been acquired fraudulently to submit bogus claims. This also applies to other personal information that can be used to obtain Medicare and Medicaid provider numbers. If you suspect your provider number has been stolen, report it immediately. Check with your local Medicare and Medicaid fiscal intermediary about how to report fraud.

Routinely Review System Activity

It is important to routinely review system activity and conduct technical audits to monitor suspicious activity. Your practice management system should have auditing capabilities to track employee activity in patient accounts. You may not have doubts about the integrity of your staff, but even trusted staff may be inappropriately accessing/using patient information. Schedule enough time every month to go over reports with your office manager or administrator. Make sure you understand the data and ask questions if you don't.

Maintain Data and Equipment in an Encrypted Mode

All electronic devices and data should be password protected to prevent theft.

Use Security Reminders

Use periodic security reminders and alerts to keep your workforce vigilant and on the lookout for security incidents.

These steps are, of course, just part of your overall HIPAA compliance program. Make certain your organization has done everything it can to protect sensitive data.

COMPLIANCE REVIEWS AND INVESTIGATIONS

In the case of a complaint or investigation, HIPAA requires cooperation from covered entities, sometimes including allowing investigators access to facilities, records, and other information at any time, without notice. Ω

Ω TOOLS

A list of information that might be requested in a HIPAA investigation or compliance review is included in the Appendix.

NOTICE OF PRIVACY PRACTICES

All physicians covered by HIPAA are required to provide their patients with a written notice of the privacy practices (NPP) they use to protect patients' health information. Covered physicians that maintain a physical delivery site must post their privacy practices in a prominent place likely to be seen by patients.

HIPAA also requires that providers with a "direct treatment relationship" use their best effort to have the patient sign an acknowledgement of receipt.

If you at some point revise your privacy practices, you need only make the revised version available *upon request* (and of course replace your existing posted NPP as well as the one you provide to new patients). You do not need to resend the revised NPP to all existing patients.

Also remember that if you have a website, you must prominently post the NPP on your website and make it available to viewers who request a copy.

Sample NPPs in English and Spanish are available as part of PrivaPlan's HIPAA compliance toolkit.

PROTECTING INDIVIDUALS WHO COMPLAIN

Covered entities should be especially vigilant when handling complaints so there is not the impression of retaliation. Such a signal may not always be obvious to you, but to your employees or patients who complain, sometimes even subtle and unrelated actions can feel like retaliation. For example:

- Rescheduling patients who have complained or "passing them off" to other providers
- Disciplining an employee who has complained for an unrelated workplace action

Some Practical Tips

1. Be sure you have written policies and procedures and that every member of your workforce has been trained in these procedures.
2. Review your current Notice of Privacy Practices and be sure it clearly states that the individual will not be penalized or retaliated against for filing a complaint.
3. Review your complaint and whistleblower policies and procedures. The CMA/PrivaPlan HIPAA Privacy and Security Compliance Toolkit contains appropriate language for this. The toolkit is available for purchase at www.privaplan.com.
4. Whenever a patient or member of the workforce files a complaint, immediately ensure that your key managers, owners, and other relevant supervisors understand they should be careful not to act in a way can been interpreted as retaliatory or intimidating.
5. Of course, handle complaints immediately and with full documentation.
6. If you find you have legitimately violated HIPAA, implement a corrective action plan. ■