INSTITUTE
For Dental Compliance & Risk Management

HIPAA Executive Summary

The HITECH Act of 2009 and the Omnibus Rule of 2012 gave ~~a~~ sharper focus to the HIPAA Privacy and Security regulations (HIPAA) which were initiated by the U. S. Department of Health & Human Services in 1996. Until that time, almost all practices felt they were adequately HIPAA compliant. That assumption changed with these two new laws. Since then, there have been ongoing questions and confusion about what exactly is required.

Part I of this White Paper outlines the required policies and procedures along with the rationale behind them, and includes a sample policy template.

Protecting a practice's financial assets as well as patients' confidential information requires establishment of a HIPAA compliance program that addresses all potential risks. Compliance with HIPAA regulations is not simply a task that can be checked off a to-do list. HIPAA programs are ongoing processes that go beyond having a manual gathering dust on a shelf or duplicating another organization's forms and policies. All compliance programs—not just HIPAA—should be woven into the fabric of your daily business systems. Additionally, changing technology and business practices, as well as legal requirements, necessitate ongoing oversight and periodic review of your compliance program.

Policies and procedures

Written policies and procedures are not only required by the Privacy and Security Rules, they are essential to prove HIPAA compliance. Even in a small practice with longtime employees who understand compliance concepts, there is still a need for written policies and procedures. Doing so outlines the acceptable behavior and manner for handling protected health information (PHI) in your practice. It strengthens inner-office communication and ensures team members are consistent in their decision-making processes when handling and disclosing PHI.

Policies and procedures must be specific to the practice and incorporate strategies and processes that mitigate potential risks identified in the risk analysis (Note: Risk Analysis to be covered in Part II). For this reason, policies must be unique to each dental practice. If a template is used, incorporate information that tailors the policies to the specific needs of the practice. For example, if a practice files electronic claims, it's wise to address in writing who has access to the information and any restrictions, such as prohibiting download of claims data to a mobile device. If personal mobile devices are used to access and/or transmit patient information, an office policy for that process is required. Review and update policies and procedures annually, or anytime there is a change in your business activities or the privacy laws. (See Appendix A for a sample policy template that can be adapted to your practice.)

INSTITUTE
For Dental Compliance & Risk Management

Examples of key areas in the HIPAA laws that written office policies should address include:

Privacy Rule:

- Processes and forms used to notify patients of privacy rights (Notice of Privacy Practices) and marketing authorization forms, etc.
- Notification protocol if a data breach occurs: regulatory agency and patient notification responsibilities
- Business Associate Contracts and Other Arrangements
- Revocation of access for employees or associates who are terminated or leave the practice
- Proper disposal or destruction of paper and/or electronic data files
- Delineation of staff responsibilities, role-based access to data, and sanctions if staff violate your office policies
- Handling of complaints
- A policy prohibiting retaliation against patients or staff who file a complaint
- Any other area of privacy specific to your practice, such as if staff transport patient information between multiple office locations.

Security Rule:

- Processes and forms related to any patient data that is stored or transmitted electronically
- Mobile device policy
- Management Process—to prevent, detect, contain, and correct security violations.
- Workforce Security—to ensure all staff have appropriate access to electronic protected health information and prevent those who do not have access under HIPAA from obtaining access.
- Information Access Management—for authorizing access to electronic protected health information in a manner consistent with the Security Rule.
- Security Awareness and Training—includes new hire, annual and periodic security awareness reminders, and training.
- Security Incident Procedures—outlines how will you address security incidents.
- Contingency Plan—outlines how you will respond to an emergency or other occurrence (e.g. fire, vandalism, system failure, and natural disaster) that damages computer systems or devices containing electronic protected health information.
- Periodic security risk analyses (sometimes referred to as assessments) and evaluations

INSTITUTE
For Dental Compliance & Risk Management

Roles of Staff

Educating all team members is a critical component of any HIPAA program. In addition to reviewing policies with new team members, all team members should be re-educated annually or anytime there is an update in office policies due to new regulatory rules or changes in the practice, such as adding staff or computer upgrades. Document HIPAA training and keep proof of training for six years as required by law.

Oversight of privacy and security processes is the responsibility of the practice's privacy and security officers — two positions required by HIPAA regulations. Since dentists typically make the final decisions regarding technology or security investments in the practice, they are the best candidates to fill the role of security officer. The office manager may also serve as the privacy officer, who oversees day-to-day responsibilities such as staff training, handling patient questions about privacy, oversight of policy and procedure implementation, and identification of necessary updates to risk assessments and policies. Additionally, job descriptions that name and delineate responsibilities for each of the privacy and security officers are required for HIPAA compliance.

Six Key Words

Whether you're training team members or trying to resolve a privacy or security dilemma, there are six key words that will serve as your mantra—"What does our written policy say?" Develop the habit of referencing your policies and procedures manual when questions, dilemmas or incidents arise. Doing so will help you maintain a strong HIPAA compliance program.

About the Institute for Dental Compliance and Risk Management

Founded in 2014 to meet the growing need for compliance experts in dentistry, the Institute assists dental professionals in navigating regulatory changes and challenges. The Institute offers advanced certification for dental professionals who seek to expand their knowledge and skills in the areas of OSHA, HIPAA and Risk Management. Not ready to take a formal course, just yet? We invite you to join our Compliance Community and stay up-to-date on critical regulatory requirements impacting dentistry.

Learn more about the Institute for Dental Compliance and Risk Management.

Policy Name:
Policy Number:
Effective Date:

1.0 Purpose

What is the reason the policy? What do you want staff to do as a result of following this policy?

2.0 Definitions

Define any key terms here in order to avoid any confusion or clarify new processes, etc. You may or may not have any definitions.

3.0 Procedures

List the steps or procedures necessary to follow this policy.

4.0 Exhibits / Appendices / Forms / Related Policies

Mention any corresponding forms or documentation. For example, if you are writing a policy pertaining to Business Associates (BA), one supporting document would be the Business Associate Agreement. You may also choose to reference other supporting policies. For example, you may have a BA audit form or questionnaire that you require BAs to complete attesting to their adherence to the HIPAA laws that you wish to reference.

Note: additional sections may be added to the policy to meet the specific needs of your practice.