HIPAA Compliance Best Practices

REMARKABLE HEALTH

HIPAA compliance is a major concern for behavioral health agencies as they try to maintain their clients' trust while meeting required reporting and documentation processes.

Many behavioral health agencies want to know: how do you comply with HIPAA in a behavioral health practice?

The first step is to know the difference between the Privacy Rule and the Security Rule.

HIPAA Privacy Rule

The HIPAA Privacy Rule provides your clients and their authorized individuals the "right to review, inspect, and receive a copy of the medical records and billing records that are held by health plans and healthcare providers covered by the Privacy Rule."

However, the Privacy Rule holds mental health records to a higher standard because of their sensitive and subjective nature. Separate the notes taken by a behavioral health professional during therapy sessions related to client treatment from the client's medical and billing records.

HIPAA Security Rule

The HIPAA Security Rule covers administrative, technical, and physical safeguards that govern how you secure your protected health information (PHI).

This guide will discuss best practices to help you achieve compliance with these safeguards. While it is important to protect your PHI, it is also important to plan in case a breach happens.

HIPAA Compliance Best Practices

#1: Perform ongoing risk assessments

How secure is your behavioral health practice physically? One area to consider include how visible your computer monitors are from the reception area or even from an outside window. Another is how audible are sensitive, private conversations between therapist and client to those who should not have access.

You also need to assess how secure your computers and paper records are in the event of a physical break-in. A good way to ensure you're covering everything is to take advantage of the Office of the National Coordinator for Health Information Technology (ONC) and the Office for Remarkable Health Content 2 Civil Rights (OCR) Security Risk Assessment Tool. This tool is designed to help small and medium-sized behavioral health practices tackle the risk assessments for their agencies.

One interesting HIPAA compliance best practice smaller behavioral health agencies can take advantage of is clinical consulting groups. These groups comprise several clinical agencies who band together to mutually develop a risk analysis and management plan for each member of the group. Then they jointly purchase a HIPAA compliance expert's time to get advice on filling in holes in their analyses and getting ideas for ways to reduce their identified risks.

#2: Understand the capabilities and limits of your technology solutions

Behavioral health practices commonly use email for communication. It is important to make sure your email provider follows HIPAA requirements such as encryption during transmission.

If you determine your communication technology has any potential security issues, provide disclosure to your clients and receive acknowledgement before moving forward. The best practice is to discourage communicating PHI through unencrypted channels.

Also, make sure your behavioral health EHR solution can restrict access to a specific client's chart to individual staff. This will help you comply with secure access requirements under HIPAA's Security Rule.

Another key is to make sure each individual has a specific login and password combination not shared with anyone else. In case of a stolen laptop, strong logins and passwords will secure PHI from unauthorized users trying to enter your system.

Create policies and procedures governing the use of your technology, and share them with everyone in your agency. For example, require your clinicians and staff to frequently change passwords for better security. Another step is to use login time-outs to avoid leaving computer screens unattended.

#3: Create a policy for documenting phone calls and texts

Documenting phone calls and text messages is an often-overlooked area in terms of compliance. For example, if a call with a client occurs outside the office, you should have a protocol in place to make sure the clinician reflects the call in your agency's documentation.

The same goes with text messages. As such, staff or clinicians must enter into the client's chart any care-related communications through phone calls or text, no matter how brief.

Distribute your policy to all involved with client care to make sure their understanding and compliance. Your policy addresses the quality of your documentation and helps in the event of legal disputes.

#4: Have a breach protocol in place

While your goal includes strong prevention measures, the risk of a breach happening remains. When a breach occurs, be prepared to describe the breach to clients affected, including the specific PHI compromised.

HIPAA has a Breach Notification Rule you should follow if you think a breach has occurred. A breach occurs when unauthorized use or disclosure of PHI compromises its security or privacy. However, if you can demonstrate through a risk assessment there is a very low chance PHI has been compromised, you may not need to execute the Breach Notification Rule.

If you feel a breach compromised your PHI, you must promptly notify the Secretary of HHS for a breach affecting 500 or more individuals. You must also notify the media if a breach affects over 500 individuals in a single state or jurisdiction.

For breaches of fewer than 500, you must notify the Secretary of HHS and the affected individuals.

However, if you can show the breach didn't compromise PHI, then notification is unnecessary. In particular, encrypt your PHI according to the technical safeguards, and you may avoid having to report a breach.

CONCLUSION

Compliance with HIPAA in behavioral health should be a two-pronged approach, satisfying both the HIPAA Privacy Rule and the HIPAA Security Rule. The best practices outlined in this guide give you actionable steps to achieve compliance, but are not an exhaustive list.

The key point is HIPAA compliance is a daily activity. Policies and procedures distributed to everyone in your behavioral health agency and ongoing security and awareness training help with compliance. Diligence and knowledge should be your foundation.

THE REMARKABLE HEALTH DIFFERENCE

Remarkable Health (formerly known as ClaimTrak) is the leading Provider Success Software Company focused on the behavioral health and human services industries. For more than 25 years we have passionately focused on providing behavioral health, substance abuse and human service organizations the tools they need to provide remarkable client experiences. We offer a purpose-built, integrated platform consisting of Electronic Health Record (EHR)—Clinical, Billing, Scheduling, Reporting, and Medication Management —for inpatient, outpatient, and residential facilities.

For more information, visit **www.remarkablehealth.com**

REMARKABLE HEALTH