

ARTICLE 7 SMALL GROUP HEALTH PLAN HIPAA SECURITY COMPLIANCE

TRAINING – A CORE INGREDIENT OF HIPAA REMEDIATION AND COMPLIANCE

HIPAA Compliance is measured by how well your organization's workforce members carry out the Policies and Procedures that have been implemented.

If a formal training program has already been implemented in response to HIPAA Privacy, or for some other reason, start by reviewing the current program and revising it to include the following:

1. Awareness Training**Error! Bookmark not defined.:** Teach the workforce how to identify threats to the Privacy and Security of Protected Health Information. Failure to protect against these threats can harm *patients/members*.
2. Protection from Malicious Software: Many organizations control updates for antivirus software and other related software via central technical controls. Others allow for the software programs to be bypassed by the end user. It is important to teach the workforce members how the systems are protected, and teach good "systems hygiene" to prevent the introduction of a worm, spyware or malware.
3. Login Attempt Monitoring: Your organization may actively monitor "Log-In Attempts" and report discrepancies as a result. Workforce should be trained to be vigilante in watching other workforce members and reporting suspected or known breaches of confidentiality to Management immediately.
4. Password Management: Consider procedures for creating, changing and safeguarding passwords. A good Password Management methodology would include protocols and direction on creating and maintaining login passwords.
5. Details of Applicable Policies and Procedures: This includes how Privacy and Security Policies affect the job of each member of the workforce and how they define what is expected of each workforce member.
6. Periodic Reminders: Periodic reminders are helpful ways to assure the workforce continues to focus on Security measures.
7. Policy and Procedure Changes: Timely information about changes in Policies and Procedures that affect certain workforce members must be communicated in accordance with job function.

Keeping you informed. Just one more reason to choose GBS.

8. Information About Sanctions: Workforce members should be reminded about their role in carrying out Compliance on behalf of the organization.
9. Make sure training has been and is documented.
10. Make sure there is a process to retrain existing workforce members, and to assure new workforce members, whether they are full-time, temporary or volunteer, are trained as necessary in accordance with their job function.

HINT: Many organizations are using HIPAA as an opportunity to further define appropriate systems usage, e-mail usage, password and other Technical Policies and to refresh users by having them sign statements that they understand and will abide by such Procedures.

Our next and final feature will review Ongoing Compliance and Evaluation.

Group Benefit Services, Inc. has once again employed a HIPAA Consultant to help us through our Risk Analysis as well as assisting us in the preparation for internal training, completing our Policies and Procedures and developing documentation for our clients. GBS has been working with Lesley Berkeyheiser, of The Clayton Group, since last spring on HIPAA Security and how the regulations affect a TPA. We are pleased to be able to offer her consulting services to you as well.

Keeping you informed. Just one more reason to choose GBS.