



Solutions in Behavioral Healthcare

Responding to a Breach

For any Behavioral Health organization, a breach of confidential information is akin to a nuclear meltdown. You have to move rapidly to stop any further breaches, contain the damage, and conduct a thorough investigation. From my experience as the Compliance Officer of a large community mental health center, the biggest threats come from within your organization, not from an anonymous hacker.

Thanks to HIPAA, organizations have policies and procedures on handling breaches. Breaches can be scaled on a multidimensional continuum from accidental/non-damaging to intentional/severely damaging. The accidental non-damaging types involve accidental disclosures that do not involve protected health information (PHI) nor Personal Identifiable Information (PII – Social Security numbers, credit card numbers, etc.). It is the malicious or just plain dumb mistakes that keep us up at night. For example:

- The staff person that leaves his computer in his trunk while he runs into the store to grab milk and his car is stolen, along with 100 client notes on the computer, contact information, including dates of birth.
- A staff person working on a progress note runs to the mailroom, leaving his computer and door unlocked. Anyone passing by can sit down and roam around the EHR.

The list can go on and on.

So what can you do? Prevention! The best way to respond to a breach – stop it before it happens. Here are some key steps:

1. Have crystal clear policies, procedures, and consequences; enforce them, and remind staff of them often.
 - a) Be sure to include breaches of confidential information in your list of acts you can immediately terminate someone for, particularly if you have a union.
2. Control the data -
 - a) All computers, but particularly laptops, notebooks and netbooks, should have BIOS level passwords (you need a password just to start the machine).
 - b) Don't allow thumb drives (USB drives) to be used. If you have to, use only encrypted password protected ones (so cheap now that there is really no excuse not to use them).
 - c) Make sure your screen savers lock and you change passwords more than every 10 years.

3. Block Social Media sites at work – no need to make it easy to upload data to a site, and you really want staff working, not changing their status on Facebook.
4. Make sure your EHR has strong audit trails – it should track who has been where looking at what.
5. Be sure IT, HR and Medical Records talk to each other – if someone is fired, tell IT before so they can wipe out the data phone, and stop access to email and files.

In the event of a loss, and it will happen, make sure:

1. You ID a “rapid response team” – know who in your organization will deal with a breach and who their back up will be in the event they are not available. Have the team do desk top drills – practice.
2. Your IT department can access and disable portable devices (such as smart phones with PHI on them).
3. Gather as much evidence as you can. Look at computer logs and email. Cut off access so no further damage can be done.
4. Notify your legal counsel and compliance officer as soon as possible – reporting will have to be done and damage control started.

Other things to consider:

- You are now responsible for the loss of data by your business associates. Make sure they have a monitoring system.
- Make sure your policies and procedures are up to date and include: the latest HIPAA, HITECH, and State confidentiality rules.

For more information contact:

Jordan Oshlag
Solutions in Behavioral Healthcare
Jordan@Solutionsinbh.com
www.Solutionsinbh.com