Learningiscreated.org - HIPAA Compliance Checklist

Visitors

- Do groups or individuals tour your center?
- Can they view client names, or other forms of PHI?
- Do you require visitors to sign a privacy/confidentiality form?

Texting

- Do you text clients?
- What is your procedure for communicating that texting is not encrypted, and therefore not HIPAA compliant?

Email

- Is your email HIPAA compliant?
- What is your procedure if a doctor or hospital request PHI via email?

Front Desk – Do front desk employees or volunteers:

- Write down client name and contact information for appointments?
- Have files not properly secured when not in use?
- Leave the front desk computer open or signed in when away?
- Release PHI to another party (i.e. doctor)?

Client Reminders and Follow Ups

- Is your appointment reminder service/procedure HIPAA compliant?
- Do you have permission to contact the client and leave voicemail?
- Does your staff or volunteers text clients?

Role-based Training

- Do you train for specific roles and maintain training logs?

Healthcare Operation – Reporting

- Is your center using the safe harbor method for statistical reporting?

Compliance Officer

- Who is the point of contact for HIPAA compliance?
- To whom should a volunteer or employee report a suspected breach?

Breach Notification

- What happens when there is a breach of client PHI?

Annual Risk Assessment

- Have you conducted an annual risk assessment?
- Have you revisited a prior risk assessment?
- How often do you check HIPAA compliance measures?
- Does your center have locking file cabinets?
- Does your center limit the amount of PHI to only what is necessary?