Practice Management Center

HIPAA CHECKLIST FOR ELECTRONIC MESSAGING

ARE YOU COMMUNICATING WITH PATIENTS ELECTRONICALLY? KNOW WHAT ISCRITICAL

Create a secure messaging system in order to allow patients to communicate their protected health information (PHI) to you or communicate PHI to other clinicians. Make sure you are following these steps to remain compliant with the Health Insurance Portability and Accountability Act of 1996 (HIPAA):

1. Establish appropriate institutional policies and procedures for remote access to PHI.

2. Use HIPAA-compliant texting or email software. Don't use your general texting app or email app in your phone as they do not usually have the recommended level of encryption. Here are some popular HIPAA-compliant vendors for texting and email:
   - *Texting software examples:* Tiger Connect, OhMD, DrFirst, Spok
   - *Email software examples:* G Suite by Google (with a third party vendor to make it HIPAA compliant), Office 365, Virtru add-on extension for Gmail or Microsoft Outlook, GoDaddy

   The Academy is able to share these options on an informational basis only. It does not represent an endorsement by the Academy. Please feel free to compare, evaluate, and consider which ones best meet your needs.

   a. Ensure this software has the following requirements:
      i. Access to PHI must be limited to authorized users who require the information to do their jobs.
      ii. A system must be implemented to monitor the activity of authorized users when accessing PHI.
      iii. Those with authorization to access PHI must authenticate their identities with a unique, centrally-issued username and PIN.
      iv. Policies and procedures must be introduced to prevent PHI from being inappropriately altered or destroyed.
      v. Data transmitted beyond an organization's internal firewall should be encrypted to make it unusable if it is intercepted in transit.

3. Make sure you have a signed business associate agreement with the texting or email software vendor and keep this on file somewhere safe.

4. Make sure "Short Message Service" (SMS), "Instant Messaging" (IM) text messages, and emails are sent to the correct number/address and forwarded to the intended recipient in order to not mix-up any interceptions while in transit. Add a signature line to all of your messages stating: *This message may contain privileged or confidential information and is for the sole use of the intended recipient(s). Any unauthorized use or disclosure of this communication is prohibited. If you believe you have received this message in error, please notify the sender immediately.*

5. Make sure to have a username and password set up that is difficult for someone to hack into.

6. Set up a lock screen on your phone if you have not already and ensure that others do not have access to your phone.

(continued)

HIPAA CHECKLIST FOR ELECTRONIC MESSAGING

continued

7. If your phone is connected to Wi-Fi, ensure you are connected to a secure platform that requires logging in with a username and password.

8. If patients are sending pictures, make sure those pictures are not saved to any non-HIPAA compliant platforms like iCloud or Google photos; delete pictures that are stored on your phone.

9. Install, use, and regularly update virus-protection software on all portable or remote devices that access PHI.

10. Develop processes to ensure backup of all PHI obtained through remote devices.

11. If you are sharing images or PHI about patients with another clinician for the purposes of treatment, payment, or health care operations, that is completely acceptable, under HIPAA, and you do not need patient authorization for this communication. You must still follow the security requirements for PHI transmitted through SMS, e-mail, etc.

For more information, check out these websites:

- https://www.aad.org/dw/monthly/2017/july/get-smart
- https://www.aad.org/practicecenter/managing-a-practice/compliance/hipaa
- https://www.aad.org/dw/monthly/2014/june/hipaa-compliant-ways-to-communicate-with-other-doctors
- https://www.aad.org/dw/monthly/2018/february/cyber-hacking-in-health-care

18-584