

HIPAA Reasonable Safeguards checklist

INSTRUCTIONS: Establishing reasonable safeguards is a process of thinking how patient information is stored, processed and transmitted over the course of a typical day in the office, and evaluating the potential for unauthorized persons to have access to it, whether purposely or inadvertently. To start the process, here are some questions you should ask yourself, as you walk through your office.

STORAGE OF PATIENT INFORMATION

1. How are patient files stored?

- Paper records
- Electronic records
- Charts
- Other _____

2. Where are patient files stored?

- Examination room
- Reception area
- Patient files area
- Provider's briefcase
- Waiting room
- Other _____

3. Who has access to patient information after business hours?

- Providers
- Nurses
- Assistants
- Staff
- Contractors
- Patients
- Family members/visitors
- Cleaning staff
- Other _____

4. What happens to the in-process patient information (charts etc.) after business hours?

- Left in examination room
- Provider takes home
- Left in common area
- Put back in patient files
- Other _____

5. How is patient information secured after business hours?

HIPAA Reasonable Safeguards checklist

- Locked cabinet
- Locked file room
- Locked fax room
- Locked desk drawer
- Other _____

PROCESSING OF PATIENT INFORMATION

6. How is patient information stored, processed and transmitted?

- Paper
- Fax
- Practice Management System
- Personal computer
- Handheld device
- Computer network
- Other _____

7. Where is in-process patient information stored?

- Examination room
- Reception area
- Patient files area
- Provider's briefcase
- Waiting room
- Other _____

8. How is patient information displayed around the office?

- Charts on examination room doors
- Daily/weekly schedule on the wall, desk in reception area, printout from scheduling system
- Computer monitors
- Other _____

9. Who has access to patient information during business hours?

- Providers
- Nurses
- Assistants
- Staff
- Contractors
- Patients
- Family members/visitors
- Other _____

HIPAA Reasonable Safeguards checklist

10. Who has a right of access to patient information?

- Providers
- Nurses
- Assistants
- Staff
- Contractors
- Patients
- Family members/visitors
- Other _____

TRANSMISSION OF PATIENT INFORMATION

11. Does the patient information leave or come into the office? If so, how?

- Electronic transmission
- Via mail/express mail/courier
- On a diskette or equivalent
- In the provider's/staff member's briefcase
- Transcription service
- Other _____

12. How is patient information disposed of?

- Shredder
- Trash can
- Recycled
- Archived
- Other _____

13. How is the identity of the recipient or source of patient information verified?

- Phone
- Fax
- Fax station number
- Not verified
- Identification number (e.g. physician license number)
- Other _____

14. How is misdirected patient information handled?

- Call back number
- Return address

HIPAA Reasonable Safeguards checklist

- Telephone verification
- Fax privacy statement
- Other _____

APPLYING THE REASONABLE SAFEGUARDS ANALYSIS

Once you've done the privacy and security walkthrough of your office, here are some additional practical questions dealing with how patient information is stored, processed and transmitted:

15. Are patients, family members and visitors escorted to and from the examination room?
16. Are patients, family members and visitors left alone with patient information (other than the patient's own) at any time?
17. Is patient information visible or audible from the waiting area?
18. Where are telephone consultations conducted? Is it out of earshot of other patients/visitors/family members/unauthorized persons?
19. Is the patient's condition or any other information indicating their health status recorded on the sign-in sheet?

TYPES OF SAFEGUARDS

The following are examples of administrative, physical and technical safeguards commercially available.

Administrative

- Policies and procedures
- Staff roles
- Right-to-know

Physical

- Locks
- Doors
- Privacy screens (e.g. computer monitors)
- Physical location (where unauthorized access is unlikely to occur)
- Offices (e.g. for private phone conversations)

Technical

- Alarms
- Access codes
- Passwords
- Secure transmission and storage systems

