

Tips for Maintaining Patient Privacy and Confidentiality

Ensuring privacy and confidentiality is part of delivering a positive patient experience. This resource includes tips to help both clinic administrators and staff maintain privacy and confidentiality in the clinic.

Check-in Desk and Waiting Area

- Do not discuss private matters like a patient's name, reason for visit, medical history, or financial information in front of other patients.
- Ensure computer screens, paper charts, completed forms, and any other sensitive information is not visible to clinic visitors.
- Make intake and history forms as short as possible, avoiding personal questions that are not relevant to patients' clinical care.
- Ask patients to sign Health Insurance Portability and Accountability Act (HIPAA) privacy forms.
- Ensure patients have privacy when signing consent forms and completing intake forms.
- Notify patients about their right to confidential services. See a [Sample Patient Bill of Rights](#).



Exam Room

- Ask all staff to wear clearly-displayed name tags.
- Ensure that patient and staff interactions in exam rooms cannot be heard from the hallway or waiting room.
- Do not discuss patients in hallways or rooms where conversations can be overheard.
- Ask for the patient's permission before bringing staff into the exam room for reasons such as interpretation, assistance, observation, or consultation.
- Introduce staff and explain why staff are in the room with patients.
- Ensure patients can dress and undress in privacy.
- Provide patients with drapes and gowns so they can cover themselves during an exam.
- Ensure patients have the opportunity to discuss private matters like sexuality, sexually transmitted infections, and contraception without other patients hearing.
- Ensure patients only have to answer personal questions (e.g., the number and gender of sexual partners, the number and outcome of pregnancies, history of STIs or abuse) one time per visit, including filling out paperwork.
- During virtual visits, ensure patients are in a private location. If the patient has privacy concerns, suggest alternatives (e.g., agree on a "safe" word for the patient to end the visit or suggest the patient take the visit in another location, such as a car).



Labs and Back Office

- Identify a private space where patients who are upset can have some private time.
- Ensure patients can submit a urine sample (or other self-collected specimen) privately, without other patients seeing the sample or their name on the sample.
- Do not disclose patient information to staff unless required for providing patient care.
- Keep patient medical records in a secure location and implement safeguards to ensure privacy, security, and appropriate access to patients' personal health information.

Check-out Desk

- Do not discuss private matters like a patient's income, living arrangements, costs, payment, services received, follow-up care, referrals, or prescriptions in front of other patients.
- Accommodate patient requests for confidential billing, such as not mailing the Explanation of Benefits (EOB), sending the EOB to a safe location, etc.



Virtual Space

- Use a HIPAA-compliant telehealth platform.
- Use a secure, encrypted connection like a virtual private network (VPN) when communicating virtually or when accessing clinic or patient data.
- Do not share electronic health record login passwords with anyone, including co-workers.
- Do not use a personal email account to send or receive work-related emails.
- Do not forward work emails to personal email accounts.
- Do not send or share clinic-related information and data through personal file-sharing tools.
- Do not share clinic-related information and data through or on social media.
- Only click on verified links in emails.
- Conduct work-related activities on only secure devices and networks.

