

**HIPAA Privacy and Security Procedures For
Gynecologic Oncology Of Middle TN**

I.

Waiting Room

A. Privacy

1. Patients will be called by first or last name before escorted back to exam rooms or labs.
2. Sign in: patients will be allowed to use sign-in sheet.
3. Patients will be offered a copy of the privacy notice. A good faith effort will be made to have patients sign an acknowledgment that they received the notice. This signature sheet will be kept on file in the patient's chart. Copies of privacy notices will be given to any patients who request a copy to keep or to take home.
4. Discussions with patients about treatment, payment or operations will not be conducted in the waiting room. Patients will be asked to speak to the receptionist, nurse or doctor in the secondary waiting room, exam room, or other private area.

B. Security

1. When employees have not arrived in reception area, the front door will remain locked.
2. Outside doors to the office will be kept locked from close of the office until 7:30 am of the next of the next business day. Cleaning personnel will be asked to honor this policy.
3. The office may be opened at 8:00 am Monday thru Friday. The outside door will be opened but the inside doors to the clinic will remain locked at all times. The door to the back office will be locked until office personnel are present. Charts and PHI will be kept out of the receptionist's desk in a way that patient's information cannot be seen from the waiting area.

II.

Reception Area

A. Privacy

1. All efforts will be made to keep Identifiable Patient Information from view of patients in waiting room. This includes checks, charts, claims appointment books, etc.
2. Conversations with patients or family members relating to health or financial issues should be done in privacy, i.e. at the check-out area rather than the waiting room or in a second waiting room or empty examining room.
3. If confidential issues are to be discussed, patients are to be ushered into an examining room or the secondary waiting room.
4. Cleaning personnel will be called periodically (once a week or so) to clean the file room at a time when office personnel are present.

B. Security

1. Computer screen will be visible only to receptionist (or staff in reception area)
2. At the end of each day, reception area will be locked, and identifiable patient information will be kept from view of windows.
3. At the end of the day trashcan will be placed outside the (locked) reception area
4. Passwords to secured web sites are kept concealed.
5. Passwords remembering by computer's is not allowed.

III.

Record File Room

A. Privacy

1. Employees will not review patient information from the record except in the performance of her (his) task and job. For the nurse and receptionist, this may include the entire record.
2. Employees are not to read medical records of a friend or relative without permission of the doctor.
3. Part-time clerical personnel will have access to the outside of the chart (names) but not to clerical information within the chart unless it is necessary to their job (copying chart).

B. Security

1. Patients are not allowed in the medical record room.
2. Drug reps are not allowed in the file room.
3. Identifiable patient information on discarded papers will be shredded before disposal this includes faxes, appointment schedule copies, phone messages, etc.

IV. Lab

A. Privacy

1. Identifiable patient information will be removed from the lab or shredded at the end of the day.
2. Patients will not be allowed in the lab unless accompanied by an employee.
3. Couriers will pick up only their company's specimens and will not loiter in the lab.

B. Security

1. Secure cabinets will be locked at night and when office is closed.

V. Examining Rooms

A. Privacy

1. To preserve modesty and privacy, employees should knock on the door before entering.
2. Charts in the chart rack must be positioned so as not to identify the patient to a hallway passer-by (name facing in to door or upside down)
3. The doctor and employees will take steps to respect patient modesty.
4. Patients should not leave the examining room to go to the bathroom without dressing except in emergencies.
5. Family members who leave examining rooms during a part of an examining will wait in the waiting room or in the secondary waiting room, not in the hallway, lab or other area where private conversation with other patients may be heard.

B. Security

V. Office Storage Closet and back entry hallway

A. Privacy

1. Non-employees are not allowed in the storage closet. Deliveries are to be made in the front office and then stored products are to be moved into storage closet by office employees.
2. Worksheets and statements, aging and end of the month financial information will be kept in locked in the controller's office.

B. Security

1. The drug sample closet is to be kept locked at all times. Employees will have keys.
2. Outdated charts, transferred patient chart, deceased patient charts, and other inactive charts are to be kept separate from other charts.

Sample Closet

A. Privacy

1. Drug reps are to supply the sample closet and give papers to be signed to the nurse who will bring them to the doctor. Only staff and Physicians will have access to sample closet. Reps will not loiter near the door while he or she is dictating.
2. Drug reps are not to enter the sample closet.
3. Identifiable patient information is not to be kept in employee lounge at any time.

B. Security

1. Sample closet is to be locked at all times.
2. Employees must notify the doctor of any personal request for medications from the sample closet.
3. No identifying information is to be taken into the sample closet.

Conference Room

A. Privacy

1. When meeting with drug reps for lunch or any marketing discussion, patients are not to be identified by name.

GOMT

A. Privacy

1. At the end of the day no charts are to remain in the doctors office.
2. All telephone notes or other identifiable information are to be shredded. This includes notes by the receptionist for medication renewal, prescription requests, and notices of patient symptoms or questions that the doctor uses to call the patient.

General Office Policies

A. Privacy

1. The general voice volume should be kept low when speaking or using the telephone so as not to disclose information to patients, drug reps, couriers or others in the office hallways. Employees and the Physician are not to discuss patients, case histories, or other identifiable information where others can overhear. If necessary, use general terms that do not identify the patient.
2. Overhead paging should not mention the name of a patient who is calling. The name of the doctor calling may (if necessary) be announced.
3. E-mails to patients should not contain sensitive or embarrassing information. Direct telephone conversation's with the patient (not a relative) is preferred.
4. Faxing: patients who ask for identifiable information to be sent by fax must ensure the fax is secure. It is not necessary to call to verify security of a fax machine. This office can refuse to fax sensitive information at the discretion of the doctor's.
5. Tara Fritz is the privacy officer for this practice. All privacy issues are to be directed to her.

B. Security

1. Employees will not leave medical records unsecured, unattended or visible to the public.

C. Employee training and Education

1. Employees will review the HIPAA manual and sign a statement when completed
2. Employees will meet regularly in office meetings that will devote time brainstorming on privacy and security issues.
3. This manual and policy listing is a work-in – progress and will be updated regularly. It is not necessary for employees to sign each time a change is made to the polices and procedures manual.

D. Faxing and record transfer policies

1. Faxing information to specialist physicians does not require patient authorization. The office will only fax information to specialist that are documented to be seeing the patient (the doctor has referred the patient, recommended the patient to the specialist, or patient record has a prior consultation letter or reference to that specialist).
2. Requests for faxing information to hospital and other physicians will require patient authorization only on a case-by-case basis determined by the doctor.
3. Requests for copying or faxing patient information to insurance companies MUST contain the beginning date and ending date of requested information. A HIPAA complaint form must be completed by the patient before records are copied and sent.
4. Request for faxing information to insurance companies requires patient authorization
 - a. Unless specified otherwise, records sent to insurance companies must comply with the Minimum Necessary Standards Rule. Final decisions are determined on an individual basis.
 - b. It is preferred that requests for records specify “all records” or specific dates (from—to--)
5. This office will comply with current regulations as it relates to required patient written authorization prior to transferring, faxing, mailing, or turning over any patient health information.
6. The receptionist will ask insurance company representatives to state the dates of service (beginning and ending) for requested information, or whether a summary is acceptable.
7. Transfer of medical information to insurance companies will require a HIPAA complaint authorization signed by the patient.

E. Patient access to their own medical information

1. Patients will have access to their medical information as outlined in the Privacy Notice and Patient’s Rights document. Exceptions are outlined in the Privacy Notice.
2. If a patient finds an entry in their medical records for which she takes issue, the office will provide a form for request for correction/amendment of Protected Health information. Tara Fritz will consider each request and will discuss it with the patient. She will either amend the entry or will explain to the patient why she feels that amendment is not necessary. The request for correction/amendment will be kept in the patient’s chart.
3. Business associates (listed in this manual) must sign a Business Associates contract before receiving identifiable patient information.

F. E-mail Issues

1. When sending e-mail to patients, preferably use home e-mail rather than work e-mail.
2. Patients will be informed that business e-mail is NOT secure or confidential. Employers and others within a company have legal right to the information on business e-mail.
3. On the Patient Information Sheet (Demographics) patients sign once each year, the authorization to allow e-mail to be sent to the patient must be signed before e-mail can be sent.

G. Telephones Issues

1. Physician and employees must give confidential and sensitive information only to the patient or close family members for whom an authorization is signed.
2. Voice mail (especially in businesses) and e-mail are considered NOT completely confidential; employers have a right to information on company voice or e-mail.
3. Employees should use the caller id when possible to ensure the patient is identified before giving verbal patient health information (lab, tests, etc)
4. Employees will not leave sensitive medical information on a patient's answering machine, but may leave the request to call the office instead.
5. Communication of health information with a friend of a patient must be done carefully and only with prior approval (verbal or written) from the patient.
6. If employees (or the doctor) are not sure of the identity of a caller (and the "caller id does not answer this concern) the employee may ask the caller for identifying demographic information about the patient to ensure identity. If the employee is still not convinced of the identity of the caller, the requested information may be denied or the employee may call the patient back on a known or home or work telephone number.
7. This office may call patients to remind them of their visit the next day. This may include reminding them to bring in their medications. This may also be left on an answering machine or voice mail.
8. If an employee is not sure if a patient is calling for information (or for prescription requests etc.) is the person claimed, the employee may decline to provide the information, call in a prescription. One option is to call the patient back using a known telephone number.
9. The consent patients will sign at the first visit must allow them to give permission to leave messages on answering machines with an expiration date or (preferably) until change is made by patient.

H. Additional Disclosure Issues

1. Patients will need to sign summary of Notice of Privacy and disclosure statements in order for the doctor and his and her staff to discuss clinical information or reminders for appointments with spouses, children, parents, siblings or other relatives.
2. Patients will need to sign Summary of Notice of Privacy and accompanying disclosure statements in order for the doctor and his and her staff to leave messages on answering machines
3. Despite disclosure statements and Notices of Privacy, sensitive patient information will not be left with relatives, authorized friends, or answering machines- at the discretion of the doctor and staff.
4. Back to Work Notes: Unless stated by the patient, back to work slip will not divulge the illness, disease or the reason the patient is out of work.
5. Patient Complaints: Patients who wish to lodge a complaint may obtain a copy of the Patient Complaint Form and complete it for submission to the privacy officer. All complaints will be kept in the HIPAA manual along with the officer's response to all complaints in writing. Responses will be sent to the patient within 7 working days.

I have been given Documentation of staff review of HIPAA Privacy and Security Procedures for GOMT

Print Name _____

Signature _____ . Date _____