The Oncology Institute HIPAA Privacy & Security Plan Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations restrict The Oncology Institute's ("TOI", "Practice") ability to use and disclose protected health information (PHI).

Protected health information (PHI, or Medical Records) means information that is created or received by the Practice and relates to the past, present, or future physical or mental health condition of a Patient/Client ("Patient"); the provision of health care to a patient; or the past, present, or future payment for the provision of health care to a patient; and that identifies the patient or for which there is a reasonable basis to believe the information can be used to identify the patient. Protected health information includes information of persons living or deceased.

The 18 PHI Indemnifiers are:

1. Patient names
2. Geographical elements (such as a street address, city, county, or zip code)
3. Dates related to the health or identity of individuals
4. Telephone numbers
5. Fax numbers
6. Email addresses
7. Social security numbers
8. Medical record numbers
9. Health insurance beneficiary numbers
10. Account numbers
11. License/ID number
12. Vehicle identifiers (license plate, VIN)
13. Device attributes or serial numbers
14. Digital identifiers, such as website URLs
15. IP addresses
16. Biometric elements, including finger, retinal, and voiceprints
17. Full face photographic images
18. Other identifying numbers or codes

It is the Practice's policy to comply fully with HIPAA's requirements. To that end, all staff members who have access to PHI must comply with this HIPAA Privacy and Security Plan. For purposes of this plan and the Practice's use and disclosure procedures, the workforce includes individuals who would be considered part of the workforce under HIPAA such as employees, volunteers, interns, and other persons whose work performance is under the direct control of TOI, whether or not they are paid by TOI. The term "employee" or "staff member" includes all of these types of workers.

All staff members must comply with all applicable HIPAA privacy and information security policies. If after an investigation you are found to have violated the organization's HIPAA privacy and information security policies then you will be subject to disciplinary action up to termination or legal ramifications if the infraction requires it.

I. Privacy Officer

The General Counsel/Compliance Officer will be the HIPAA Privacy Officer for The Oncology Institute. The Privacy Officer will be responsible for the development and implementation of policies and procedures relating to privacy, including but not limited to this Privacy Policy and the Practice's use and disclosure procedures. The Privacy Officer will also serve as the contact person for patients who have questions, concerns, or complaints about the privacy of their PHI. The Privacy Officer can be reached at 562-735-3225 ext 89011.

II. Incident Response Team

The Incident Response Team is comprised of the CEO, COO, Compliance Officer, Site Managers and additional members deemed appropriate on an ad hoc basis in the reasonable judgment of the Privacy Officer. In the event a security incident results in a wrongful disclosure of PHI, the Privacy Officer, in conjunction with the Incident Response Team will take appropriate actions to prevent further inappropriate disclosures. In addition, Human Resources and Medical Records may be consulted as part of the review team to assist in the review and investigation of privacy incidents when required. If the Privacy Officer and Incident Response Team have not resolved the incident, the Privacy Officer shall involve anyone determined to be necessary to assist in the resolution of the incident. If patients need to be notified of any lost/stolen PHI, the Privacy Officer will send PHI Theft/Loss Disclosure Letters to all possible affected individuals.

III. Employee Training

It is the Practice's policy to train all members of its workforce who have access to PHI on its privacy policies and procedures. All staff members receive initial and annual HIPAA training. Whenever a privacy incident has occurred, the Privacy Officer will evaluate the occurrence to determine whether additional staff training is in order. Depending upon the situation, the Privacy Officer may determine that all staff should receive training that is specific to the privacy incident. The Privacy Officer will review any privacy training developed as part of a privacy incident resolution to ensure

the materials adequately address the circumstances regarding the privacy incident and reinforce the Practice's privacy policies and procedures.

IV. Safeguards

The Practice has established technical and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. Technical safeguards include limiting access to information by creating computer firewalls, and using an encrypted EHR. Physical safeguards include locking doors or filing cabinets and periodically changing door access codes. Additionally all staff members can only access PHI by using their own login information. Encryption ensure that only authorized employees will have access to PHI, that they will have access to only the minimum amount of PHI necessary for their job functions, and that they will not further use or disclose PHI in violation of HIPAA's privacy rules.

V. Complaints

The Privacy Officer will be the Practice's contact person for receiving complaints and can be reached via email, or at 562-735-3225 ext 89011.

VI. Sanctions for Violations of Privacy Policy

Sanctions for using or disclosing PHI in violation of this HIPAA Privacy Plan will be imposed in accordance up to and including termination.

VII. Mitigation of Inadvertent Disclosures of Protected Health Information

TOI shall mitigate, to the extent possible, any harmful effects that become known to it because of a use or disclosure of a Patient's PHI in violation of the policies and procedures set forth in this Plan. As a result, if an employee becomes aware of a disclosure of protected health information, either by a staff member of the Practice or an outside consultant/contractor that is not in compliance with this Policy, immediately contact the Privacy Officer so that the appropriate steps to mitigate the harm to the patient can be taken.

VIII. No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy

No employee may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA.

No individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment or eligibility.

IX. Documentation

The Practice's privacy policies and procedures shall be documented and maintained for at least six years. Policies and procedures must be changed as necessary or appropriate to comply with changes in the law, standards, requirements and implementation specifications (including changes and modifications in regulations). Any changes to policies or procedures must be promptly documented. If a change in law impacts the privacy notice, the privacy policy must promptly be revised and made available. Such change is effective only with respect to PHI created or received after the effective date of the notice.

TOI shall document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to an individual's privacy rights. The documentation of any policies and procedures, actions, activities and designations will be maintained in the patient's electronic chart.

SECTION 2: Use and Disclosure of PHI

I. Use and Disclosure Defined

The Practice will use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

• Use. The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any person working for or within the Practice, or by a Business Associate of the Practice.
• Disclosure. For information that is protected health information, disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons not employed by or working within TOI with a business need to know PHI.

II. Access to PHI Is Limited to Certain Employees

All staff who performs Patient functions directly on behalf of the Practice or on behalf of group health plans will have access to PHI as determined by their department and job description. These employees with access may use and disclose PHI as required under HIPAA but the PHI disclosed must be limited to the ***minimum amount necessary*** to perform the job function. Employees with access may not disclose PHI unless an approved compliant authorization is in place or the disclosure otherwise is in compliance with this Plan and the use and disclosure procedures of HIPAA.

Staff members may not access either through our information systems or the patient's medical record the medical and/or demographic information for themselves, family members, friends, staff members or other individuals for personal or other non-work related purposes, even if written or oral patient authorization has been given. If the staff member is a Patient in TOI's plans, the staff member must go through their Provider in order to request their own PHI.

In the very rare circumstance when a staff member's job requires him/her to access and/or copy the medical information of a family member, a staff member, or other personally known individual, then he/she should immediately report the situation to his/her manager who will determine whether to assign a different staff member to complete the task involving the specific Patient.
Your access to your own PHI must be based on the same procedures available to other patients not based on your job-related access to our information systems. For example, if you are waiting for a lab result or want to view a clinic note or operative report, you must either contact your physician for the information or make a written request to the Privacy Officer. You cannot access your own information; you must go through all the appropriate channels as any Patient would have to.

III. Disclosures of PHI Pursuant to an Authorization
PHI may be disclosed for any purpose if an authorization that satisfies all of HIPAA's requirements for a valid authorization is provided by the patient. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

IV. Permissive Disclosures of PHI: for Legal and Public Policy Purposes
PHI may be disclosed in the following situations without a patient's authorization, when specific requirements are satisfied. The Practice's use and disclosure procedures describe specific requirements that must be met before these types of disclosures may be made. Permitted are disclosures:

- In certain circumstances, covered entities may disclose protected health information to appropriate government authorities regarding victims of abuse, neglect, or domestic violence.
- Covered entities may disclose protected health information in a judicial or administrative proceeding if the request for the information is through an order from a court or administrative tribunal.
- Covered entities may disclose protected health information to law enforcement officials for law enforcement purposes under specific circumstances
- For public health activities;
- Covered entities may disclose protected health information to health oversight agencies for purposes of legally authorized health oversight activities, such as audits and investigations necessary for oversight of the health care system and government benefit programs.
- Covered entities may disclose protected health information to funeral directors as needed, and to coroners or medical examiners to identify a deceased person, determine the cause of death, and perform other functions authorized by law.
- For cadaver organ, eye or tissue donation purposes;
- For certain limited research purposes;
- To avert a serious threat to health or safety;

- For specialized government functions an authorization is not required to use or disclose protected health information for certain essential government functions.
- Covered entities may disclose protected health information as authorized by, and to comply with, workers' compensation laws

Any such disclosure must first be approved by the Privacy Officer.

V. Complying With the "Minimum-Necessary" Standard

HIPAA requires that when PHI is used or disclosed, the amount disclosed generally must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure.
All other disclosures must be reviewed on an individual basis with the Privacy Officer to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

VI. Disclosures of PHI to Business Associates

With the approval of the Privacy Officer, and in compliance with HIPAA, employees may disclose PHI to the Practice's business associates and allow the Practice's business associates to create or receive PHI on its behalf. However, prior to doing so, the Practice must first obtain assurances from the business associate that it will appropriately safeguard the information. This is accomplished in the form of a business associate agreement. Before sharing PHI with outside consultants or contractors who meet the definition of a "business associate," employees must contact the Privacy Officer and verify that a business associate contract is in place.
Business Associate is an entity that:

- performs or assists in performing a Practice function or activity involving the use and disclosure of protected health information (including claims processing or administration, data analysis, underwriting, etc.); or
- provides legal, accounting, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.

Examples of Business Associates are:

- A third party administrator that assists the Practice with claims processing.
- A CPA firm whose accounting services to a health care provider involves access to protected health information.
- An attorney whose legal services involve access to protected health information.
- A consultant that performs utilization reviews for the Practice
- A health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of the Practice and forwards the processed transaction to a payer.

- An independent medical transcriptionist that provides transcription services for the Practice.

VII. Disclosures to Family, Friends or Others-Patient Location

There are instances when a patient's friend or family member contacts TOI to ask about the location of a patient or whether the patient has been seen at TOI. Following is guidance provided to assist staff in providing appropriate responses for specific situations that commonly occur. In rare cases of emergency, at the discretion of senior management the minimum of information may be released in order to assist in resolving and emergency situation.

Guidance:

Situation: Friends or family are concerned about the whereabouts of a person. They contact the practice to ask if a person is at TOI or has been seen as a patient recently.

Response: If the person is not currently a TOI patient, the caller may be told that the person is not at the clinic. If the person is currently receiving services at the clinic, clinic staff should take the name of the caller, their purpose for calling the patient and tell them that they will check. Staff should then ask the patient if it is okay to provide information to the caller and what information to provide. If the patient does not want the clinic staff to provide information, staff should tell the caller that they are unable to provide information about the patient due to privacy rights and suggest that the caller contact the patient directly for information.

If the caller is asking for historical information about visits or services provided and the patient has not either provided an authorization to share this information with this person pertaining to their involvement in the patient's treatment or payment, the caller should be informed that due to HIPAA confidentiality requirements, information about patient visits is not provided without patient authorization.

Situation: An individual comes to TOI and tells the reception area that they have arrived to pick up a patient.

Response: If the patient has notified TOI staff that someone is coming to pick them up (by giving the name of the individual), the individual should be directed to the location of the patient. If the patient has not provided information about anyone coming to pick them up, TOI staff should ask for the person's name and tell the person that they will check. Another staff member should be given a note to tell the patient that someone has arrived to pick them up and ask them whether it is okay to tell the person the patient's location.

VIII. Faxing PHI

Each fax should be accompanied by a TOI fax cover sheet. Faxing of highly confidential information is not recommended, and may only occur if relevant authorization for the disclosure of that exact information is already in the patient file.

If the fax was transmitted to the wrong recipient, in all cases follow these steps:
Fax a request to the incorrect fax number explaining that the information has been misdirected, and ask that the materials be returned or destroyed. Report the incident immediately to the Compliance/Privacy Officer at 562-735-3225 ext 89011.. Verify the fax number with the recipient before attempting to fax the information again.

IV. Printing and Copying PHI
When using shared copy machines/printer documents containing PHI should never be left unattended on the devices.

SECTION 3: Patient Individual Rights

I. Access to Protected Health Information and Requests for Amendment
HIPAA gives patients the right to access and obtain copies of their PHI that the Practice or its business associates maintains. HIPAA also provides that patients may request to have their PHI amended. The Practice will provide access to PHI and it will consider requests for amendment that are submitted in writing by patients.

II. Patient Requests For Copies of Records

All requests for copies must be in writing. A signed TOI medical release form must be signed by the patient specifying dates or a date range for which the copies are to be made.

For copies of a deceased patient's records, a signed TOI medical release form must be signed accompanied by a copy of the death certificate and proper identification (to be scanned into the deceased patient's medical record). Copies of a deceased patient's medical record may only be released to the patient's legal representative or next of kin (spouse/domestic partner, child, parent, sibling, etc.)

Copies should be delivered in the method specified on the patient's request form.

If the information cannot be easily produced in the specified format, TOI staff can either provide the patient with a hard paper copy of the information or attempt to work out an alternative format acceptable to the patient.

III. Requests For Amending Records

Patients have a right to request that their medical record be amended if he/she feels it is inaccurate. Patients who wish to have their record amended must submit their request in writing, be a reasonable length, and signed by the requestor.

If the patient wishes to add an addendum to the medical record he/she may do so after the records have been inspected. The addendum may not be more than 250 words and regard an item or statement in the records that he/she believes is incorrect.

Requests will be handled no more than sixty (60) days after receipt.

If the provider is unable to act within the sixty (60) day timeframe, the provider may request a thirty (30) day extension provided that the member is notified in writing of the reason of the delay and the date in which the action will be taken.

Once approved, the provider must draw a line through the disputed entry, initial and date it, and write an addendum or the provider can add a statement that "this is the patient's view of this situation."

The request may be denied if it was created by someone other than the record keeper, is not part of the records, is not subject to patient inspection, or is accurate and complete.

If the request is denied the provider must write a short statement stating the basis for the denial, the patient's right to submit a written statement disagreeing with the denial and how to do so, inform the patient that he/she may keep the record of the request and denial with any future disclosures of information that is attempting to be amended, and how the patient can complain to the physician.

IV. Denying Access.

A patient's request to access his/her information may be denied under the following circumstances:

- The request is not in writing;
- The information requested is not contained in a designated record set maintained by TOI;
- Release of the requested information could possibly endanger the life or physical safety of the patient or another person.

Partial Denial – Access to Medical Records

If only a part of the PHI requested is denied, TOI staff must provide the patient with the rest of the information after excluding the parts that cannot be inspected or copied. A summary of the excluded parts should be provided to the patient.

Notice of Denial – Access to Medical Records

TOI staff must notify the patient of a denial within writing if the denial is for any reason other than procedural, ie, incorrect signature, request not in writing, etc.

a) TOI staff must indicate the grounds for the denial;

b) If the request is denied because the information is not maintained in the designated record set, practice staff must state any known information about where the patient may obtain access to the requested records.

c) If the requested information is only partially denied, practice staff must explain in the Denial Letter what information the patient will and will not be able to access.

VI. Acceptable Methods of Verification of Identity for Release of Personal Health Information (PHI):

When the Requestor is the Patient:
The Practice will take reasonable steps and exercise professional judgment to verify the identity of the individual making a request for access to his/her own PHI.
a. If the request is made in person, verification of identity may be accomplished by asking for photo identification (such as a driver's license). A copy of the I.D. must be attached to the request and placed in the Patients record.
b. If the request is made over the telephone, verification will be accomplished by requesting identifying information such as social security number, birth date, and medical record number and confirming that this information matches what is in the patient's record. Or, verification will occur through a callback process using phone numbers documented in the patient record to validate the caller's identity.
c. If the request is made in writing, verification will be accomplished by requesting a photocopy of photo identification if a photocopy of the ID is not available, the signature on the written request must be compared with the signature in the patient record. In addition, TOI will need to verify the validity of the written request by contacting the patient by telephone

VII. When the requestor is the Patients Legally Authorized Representative

Verification of identity will be accomplished by asking for a valid photo identification (such as driver's license) if the request is made in person. Once identity is established, authority in such situations may be determined by confirming the person is named in the medical record or in the patient's profile as the patient's legally authorized representative. Or, if there is no person listed in the medical record as the patient's legally authorized representative, authority may be established by the person presenting an original of a valid power of attorney for health care or a copy of a court order appointing the person guardian of the patient and a valid photo I.D. A copy of the I.D. and legal notice must be attached to the request and placed in the Patients record. Any such power of attorney must first be given to the Privacy Officer for review and approval.

VIII. Other Methods

The Practice may use any other method of verification that, in the Practice's discretion, is reasonably calculated to verify the identity of the person making the request. Some acceptable means of verification include, but are not limited to:

d. Requesting to see a photo ID
e. Requesting a copy of a power of attorney
f. Confirming personal information with the requestor such as date of birth, policy number or social security number
g. Questioning a child's caretaker to establish the relationship with the child
h. Calling the requestor back through a main organization switchboard rather than a direct number

PHI Breach Reporting:

The purpose of this section is to address the Practice's privacy requirements for reporting, documenting, and investigating a known or suspected action or adverse event resulting from unauthorized use or disclosure of individually identifiable health information.

A privacy breach is an adverse event or action that is unplanned, unusual, and unwanted that happens as a result of non-compliance with the privacy policies and procedures of the Practice. A privacy breach must pertain to the unauthorized use or disclosure of health information, including 'accidental disclosures' such as misdirected e-mails or faxes. The Privacy Officer shall immediately investigate and attempt to resolve all reported suspected privacy breaches.

Staff members are required to verbally report to his/her supervisor any event or circumstance that is believed to be an inappropriate use or disclosure of a patient PHI. If the supervisor is unavailable, the staff member must notify the Privacy Officer within 24 hours of the incident. If the manager determines that further review is required, the manager and staff member will consult with the Privacy Officer to determine whether the suspected incident warrants further investigation. In all cases and Incident Report must be filled out and submitted to the appropriate reviewer.

If the patient is not aware of a privacy incident, the Privacy Officer shall investigate the incident thoroughly before determining whether the patient should be informed. If the patient is aware of a privacy incident, the Privacy Officer shall contact the patient within three (3) business days of receiving notice of the incident. The method of contact is at the discretion of the Privacy Officer.
Staff who fail to report known PHI/security incidents, or fail to report them promptly, may be subject to disciplinary action up to termination.

I. Breach Notification Requirements
Following a breach of unsecured protected health information, covered entities must provide notification of the breach to affected individuals *if necessary* and, in certain circumstances, to the media. In addition, business associates must notify covered entities that a breach has occurred. Determination of breach notification is a question for the Privacy Officer to determine in light of HIPAA and the breach in question. Therefore, all such instances shall be forwarded to the Privacy Officer for determination.

Media Notice:
Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area.

Notice to the Secretary:
In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach.

Notification by a Business Associate:
If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach. A business associate must provide notice to the covered entity without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach as well as any information required to be provided by the covered entity in its notification to affected individuals.

II. Complaint/Concerns Reporting

Concerns about the Practice's privacy practices may arise in a variety of contexts and may be received by many different persons at the Practice. It is important that the Practice responds to concerns and complaints in a timely manner. When a staff member hears or receives a complaint/concern, he/she should ask the complainant whether or not the complainant wishes to file a formal complaint with the Privacy Officer. Even if the person does not wish to file a complaint or provide identifying information, the staff member should proceed with the procedures outlined below.

Filing a Complaint

a. Patient's complaints of alleged privacy rights violations may be forwarded through multiple channels, such as telephone calls, letter via mail/email, in person. If these complaints are received by a staff member the person receiving the complaint will:

• In response to a Telephone Call or In-Person Request to File a Complaint – Mark the patient's chart with a note detailing the complaint.

• In response to a Letter or Email (c – forward the letter/email to the Privacy Officer.

b. Staff Members – Call the Privacy Officer at 562-735-3225 ext 89011.

• Initial review – All complaints will be initially reviewed by the Privacy Officer to determine if the complaint alleges a violation of established policies and procedures or other known regulations regarding the protection of individually identifiable health information. If there is no legitimate allegation, the Privacy Officer will, when possible, contact the Complainant and inform him/her of this finding within 60 days.

c. Outcome of Investigation - The purpose of the investigation is to determine the compliance of the Practice's policies and procedures implementing the privacy standards mandated by HIPAA. The Practice will mitigate, to the extent practicable, any harmful effect that is known of a use or disclosure of PHI in violation of the Practice's policies and procedures or HIPAA's privacy requirements by the Practice or any of its Business Associates. In the event that disciplinary action is recommended, the Privacy Officer or his/her designee will coordinate any action with management.

III. Non-Retaliation

The Practice shall not intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any person who has reported a privacy incident.

SECTION 4: Summary Guidelines for Safeguarding the Privacy of Health Information

These are guidelines centered on how to safeguard health information and ensure confidentiality when using normal business communications, such as conversations, telephone, faxes, mail, and electronic mail. When using and disclosing PHI, you must take reasonable measures to ensure the

information is protected. Below are simple safeguarding tasks that should be used when communicating in a work environment that necessitates access to and use and disclosure of PHI. Remember to limit your communications of PHI to the minimum necessary for the intended purpose. Restrict your communications to those who have a valid "need to know" the information. If you have questions about these safeguards and how to protect PHI communications, please discuss them with your supervisor.

1. Verbal Conversations – in person

- Discuss patients PHI in private. Use an office with a door whenever possible, or leave areas where others can overhear.
- Be aware of those around you and lower your voice when discussing patients health information.
- If possible, point out health information on paper or on-screen non- verbally when discussing patients health information.
- **Physicians shall not discuss a patient's PHI with any person, even patient's family, outside the presence of the patient. However, if the patient has authorized such conversations, and that authorization is placed in the patient's chart, then TOI physicians may engage in PHI discussions with those parties approved in the authorization.**

2. Verbal Conversations – telephone

- Follow the above guidelines for "Oral Conversations"-in person"
- Don't use names instead say; "I have a question about a client".
- Do not use the name "The Oncology Institute", instead use the name of patient's attending MD.
- Never give PHI over the phone when talking to unknown callers, but call back and verify information.
- Never leave PHI on voice messages; instead leave a message requesting a return call to discuss a patient giving only your name and phone number.
- Do not discuss PHI over unencrypted cellular or portable (wireless) phones or in an emergency, as the transmissions can be intercepted.

3. Fax

- Use a cover sheet clearly identifying the intended recipient and include your name and contact information on the cover sheet.
- Include a confidentiality statement on the cover sheet of faxes that contain PHI.
- Do not include or reference PHI on cover sheet.
- Confirm fax number is correct before sending.
- Send fax containing patient health information only when the authorized recipient is there to receive it whenever possible.

- Verify that fax was received by authorized recipient; check the transmission report to ensure correct number was reached and when necessary contact the authorized recipient to confirm receipt.
- Deliver received faxes to recipient as soon as possible. Do not leave faxes unattended at fax machine.

4. Email

- Do not include PHI in Subject-line or in Body of email.
- Transmit PHI only in a password-protected attachment (MS Word and MS Excel provide password protection).
- Include a confidentiality statement on emails that contain any PHI in email attachments.
- Do not send attachment passwords in the same email as the attachment.
- Include your contact information (name and phone number minimum) as part of the email.
- Request that email recipients call to discuss specific patient data.

5. Work Areas

- Do not leave PHI (files, records, Rolodex, reports) exposed, open, or unattended in public areas, conference rooms, mailboxes, wall trays, etc.
- Store all PHI securely in locked file cabinets, desk drawers, offices, or suites when you are not in your work area.

SECTION 5: Retention and Disposal of PHI

Each respective department is responsible for preserving the safety and confidentiality of documents in the organizations possession. Documents (either hard copy or electronic format) should be maintained at the organization's office or off-site (via encrypted EMR) at the discretion of the Administration to provide for their security and preserve their usefulness to the organization.

It is the responsibility of each respective department to ensure that all permitted document destruction shall halt if the organization is being investigated by a government law enforcement agency, and routine destruction shall not resume without the written approval of legal counsel.

Procedure:

1. Retention

1. Documents should be maintained until the end of the identified retention period, and should then be destroyed in an appropriate manner. (see appendix)
2. Sensitive documents such as those containing financial, account, personnel or medical information should be destroyed with no reasonable risk of the information being recovered. Specifically, all paper documents must be shredded, and electronic copies deleted completely.

3. In cases of patient death, records shall only be released to the next of kin provided the following information is first received:
    a. Patient's death certificate
    b. ID of next of kin
    c. Written authorization of surviving next of kin
    d. Medical record department shall add patient authorization for release of PHI to patient charts when received.
4. All PHI shall be retained for a minimum of seven (7) years from the date of most recent discharge, or the death of patient.
5. PHI of minor patients aged under 18 years shall be kept 7 years after the patient's 18th birthday.
6. The obligations provided herein to retain such PHI shall continue even if the practice is sold or dissolves.

APPENDIX: PHI Destruction Schedule

Document Type	Minimum Suggested Retention
Medical Records (Any Format) – Following Patient Discharge - ADULT	7 years
Medical Records (Any Format) – Following Patient Discharge – MINOR ****Records must be maintained at least 1 year following minor's 18th birthday, but in no event less than 7 years****	7 years
X-Rays (Any Format) – Following Patient Discharge - ADULT	7 years
X-Rays (Any Format) – Following Patient Discharge – MINOR ****Records must be maintained at least 1 year following minor's 18th birthday, but in no event less than 7 years****	7 years
Billing Records – Encounter Forms, Claims (Any Format)	6 years
Disclosure Histories (Any Format)	6 years
"Notice of Privacy Practices" (Receipt of Acknowledgment)	6 years
Right to Access, Amend, or Restrict Use or Disclosure of Protected Health Information	6 years

****Request, Response, Agreement, Notice of Denial (in whole or in part), Copy of Notice to Interested Parties, Statements of Disagreement, Termination, etc.****	
Right to Request Confidential Communications (Request, Response)	6 years
Right to Request Accounting of Disclosures ****Request, Response, Copy of Information Disclosed****	6 years
Patient Signed Authorizations to Use/Disclose Protected Health Information	6 years
Verifications of Identity & Authority ****Personal Representation, Public Official, Next of Kin****	6 years
Any Communication, Action, Activity or Designation Required by Policy or Procedure Related to Use/Disclosure of Protected Health Information in Compliance w/HIPAA	6 years
Complaints From Individuals Related to Inappropriate Use/Disclosure of Protected Health Information ****Written Complaint, Written Response, and/or any Mitigating Actions****	6 years
Reports of Suspected Breaches in Privacy, Confidentiality or Security of Protected Health Information ****Incident Reports, Responses, Disciplinary Actions and/or Sanctions****	6 years
Privacy and Security Policies & Procedures ****Maintained from last effective date****	6 years
Notice of Privacy Practices ****Maintained from last effective date****	6 years