I. PREFACE

This Complete Health Insurance Portability and Accountability Act of 1996 (HIPAA) Compliance Manual was originally created in February 2003, and revised in October 2012 and September 2013, for Collins Medical Associates 2, P.C. (the "Practice") to meet the current federally required standards and CT State law requirements.

This Manual provides policies and procedures required for the Practice under the "Standards for Privacy of Individually Identifiable Health Information" (the "Privacy Regulations") portion of the HIPAA regulations, the "Security and Electronic Signature Standards" regulations ("Security Regulations"), and the recent changes to HIPAA as a result of the Health Information Technology for Economic and Clinical Health ("HITECH") Act, enacted on February 17, 2009 as part of the Stimulus Bill. The latest revisions to the Manual are required by the January 17, 2013 Omnibus Final Rule ("Omnibus Rule"), which made significant changes to the privacy and security requirements under HIPAA and HITECH. In addition there is a separate HIPAA Security Procedures Manual that contains *procedures to be implemented and followed by members and contractors* of the Practice.

This HIPAA Compliance Manual has been tailored to the *specific* needs of the Practice, based on a practice-wide evaluation of risk areas and information processes. It should be updated annually to reflect changes in Practice needs, concerns, and policies, and changes in law.

To keep up to date on HIPAA developments, the Privacy Officer should regularly check the government's HIPAA website at http://www.cms.hhs.gov/HIPAAGenInfo.

II. ADMINISTRATION

A. Introduction

This HIPAA Compliance Manual contains our Practice policies, procedures, and standards of conduct designed to ensure our compliance with applicable federal and state laws and regulations. Failure to abide by the rules, policies and procedures established by this Manual or behavior in violation of any HIPAA law, regulation or rule may result in disciplinary action. Willful failure by any employee of the Practice to comply with the policies and procedures contained in this Manual, will result in employment dismissal. Contact our HIPAA Compliance Personnel if you have any questions about our Practice commitment to effective compliance routines.

B. Compliance Mission Statement

This Practice strives at all times to maintain the highest degree of integrity in its interactions with patients and the delivery of quality health care. The Practice and its employees will at all times strive to maintain compliance with all laws, rules, regulations and requirements affecting the practice of medicine and the handling of patient information. The protection of the privacy of an individual's health information is of grave concern to this Practice. Protecting the security of an individual's Electronic Protected Health Information ("e-PHI") is a critical concern to this Practice, and to the trust our patients offer in our treatment of their medical issues.

C. Expectation of Privacy

As outlined in the HIPAA Security Policies, the Practice periodically reviews logins, and audits its systems for securing e-PHI and Protected Health Information (PHI). No employee should have any expectation for privacy regarding any material that is stored, sent or retrieved from or in any workstation. Thus, only information that furthers the mission of the Practice should be downloaded from the Internet. Likewise, there should never be any retrieval of or transmission of any e-PHI, except as specifically authorized by Practice policies.

D. Compliance Personnel

1. Privacy and Security Officers

a. Privacy Officer

Our Practice has appointed Angelo Carrabba M.D. as the Privacy Officer and Privacy Contact to oversee the privacy of patient information. The Practice's Site Coordinators at each location will handle complaint intake and routine questions regarding HIPAA. This information should be communicated to Carol Puerta, Assistant Privacy Officer, while Dr. Carrabba will still have ultimate authority.

This Privacy Officer will serve until the Practice's Board of Directors replaces him/her or until such time as he resigns from the position. The job description for the Privacy Officer is attached as Exhibit A to this Manual. The job description for the Privacy Contact is to field and respond to patient complaints and requests for information.

b. Security Officer.

Our Practice has appointed Susan Link as our Security Officer to oversee the security of the Practice's information and technology systems.

This Security Officer will serve until the Practice's Board of Directors replaces him/her or until such time as he/she resigns from the position. The job description for the Security Officer is attached as Exhibit B to this Manual.

E. Training and Education

The Practice will conduct periodic training, on an ongoing basis as needed and whenever there are material changes to this Manual, with the twin goals that: (1) all employees will receive training on *how to perform their jobs in compliance* with HIPAA; and (2) each employee will *understand that HIPAA compliance is a condition of continued employment.*

1. Positions Affected

While all Practice employees are required to meet the twin goals addressed above, the following employees are deemed to be subject to a heightened level of scrutiny by virtue of being directly involved in the areas of the Practice which are subject to HIPAA laws, rules and regulations ("Affected Employee(s)").

a. Physicians

b. Physician Extenders (i.e., Registered Nurses, Limited Practice Nurses, Medical Assistants, Nurse Practitioners, Physician Assistants, and/or anyone responsible for medical record documentation)

c. Technicians, Scribes, or anyone else responsible for documenting the medical record

d. Practice Administrator/Office Manager/Business Manager

e. Billing/Collections and Accounts Receivable Personnel

f. Front Desk (Check-in, Check-Out)

2. Mandatory Attendance

All Affected Employees are required to complete any training that is deemed appropriate to their duties by the Privacy Officer.

Employees who wish to attend a HIPAA compliance education/training program not otherwise specified by the Privacy Officer, may submit such request together with a description of the program to Compliance Personnel for consideration.

Attendance at HIPAA compliance education/training by all Affected Employees shall be documented on the "Record of HIPAA Training" form attached as Exhibit C to this Manual, which shall be maintained in the central business office Affected Employee's personnel file or HIPAA training files.

All educational and training materials received by an Affected Employee at approved programs shall be the property of the Practice and shall be maintained in a designated location for periodic review by Practice employees.

3. Expense Reimbursement

Affected Employees shall be reimbursed by the Practice for all reasonable and necessary expenses incurred in meeting their HIPAA compliance education and training requirements at approved programs. All expenses shall be recorded and submitted on an Expense Reimbursement Request form provided by the Office Manager. (See Expense Reimbursement Request form attached as Exhibit D to this Manual.)

F. Communication and Reporting

1. Dissemination of Materials

All information obtained by the Practice including manuals, changes in regulations and the like shall be communicated through HIPAA Updates distributed quarterly and training will be facilitated as needed to all Affected Employees.

Employees, who receive information which they believe to be relevant to the HIPAA compliance efforts of the Practice, are required to provide such information to Compliance Personnel. Except as otherwise noted, Compliance Personnel shall be responsible for disseminating relevant materials to Affected Employees.

Practice employees shall also maintain all relevant materials in a designated location for periodic review, as a shared resource.

2. Questions and Concerns

All employees, as a condition of their employment, are expected to read this HIPAA Compliance Manual and understand its principles. The Practice recognizes, however, that HIPAA regulations are complicated and may need further clarification beyond the materials contained in this Manual. Therefore, all employees with questions regarding this Manual or compliance in general are strongly encouraged to seek answers to and/or clarification of any such question or law/regulation/policy from Compliance Personnel. A request for answers to questions or clarification may be verbal or may be submitted in writing to Compliance Personnel: (1) in person or (2) confidentially, as described in Section 4 below.

3. Reporting of Violations or Suspected Violations

In order to help mitigate potential harmful effects and meet the Practice's reporting requirements under HIPAA, any employee who is aware of any actual or suspected violation of

any Practice compliance policy ("Violation" or "Violations"), including any actual or suspected violation by a third-party Business Associate, must immediately report such Violations to Compliance Personnel for investigation. Violations may include: an actual or suspected violation of federal or state legislation, regulations, or requirements pertaining to the security, integrity, or confidentiality of Individually Identifiable Health Information ("IIHI"). The process for reporting suspect conduct can be found in Exhibit E. See also Section V.D. of this Manual regarding the process for reporting a potential breach of unsecured PHI.

If Compliance Personnel are not immediately available or the reporting employee is concerned that Compliance Personnel are or have been involved in the Violation(s), the employee shall report the Violation(s) to any member of the Practice's Board of Directors.

The members of the Board of Directors are elected annually. Please consult the HR Representative for a list of the members of the Board of Directors.

4. Confidentiality

It is the Practice policy that no retaliatory action will be taken against an employee who makes a report, if that report is made based upon a good faith belief that a Violation has occurred, is occurring, or is likely to occur in the near future.

In addition, whenever possible the Practice will make all reasonable efforts to keep confidential the identity of the reporting employee. Employees who wish to make an anonymous report of Violations may submit it in writing and leave it in the Office Manager's office. The Incident Report Form attached as Exhibit F may be used for such purposes.

5. Investigation and Remedial Action

To the extent that Compliance Personnel deem necessary, they shall consult with legal counsel with respect to any reported Violation to ascertain the most appropriate means of investigating

and responding to such report. Compliance Personnel and/or legal counsel, as appropriate shall conduct investigations in a timely manner.

Based upon the findings of such investigation Compliance Personnel, with legal counsel, as appropriate, will take such remedial action to ensure (1) that the Violation ceases immediately, (2) that the Violation will be prevented from occurring in the future, and (3) that any notifications are made, as required by law, in a timely fashion.

6. Disciplinary Action

Any employee who is found to have committed an actual Violation or Violations shall be subject to immediate disciplinary action. The level of such disciplinary action shall be determined by the Office Manager after consulting with the Compliance Personnel, and shall be based upon a number of factors including, but not limited to, the following:

- the nature of the Violation or Violations;
- the employee's level of intent in committing such Violation or Violations (e.g., negligence, willful); and
- special circumstances surrounding or contributing to the Violation or Violations.

The disciplinary action(s) that may be taken against an employee who is found to have committed a Violation are spelled out in the Personnel Policy Manual and generally include:

- admonishment;
- written reprimand (which shall be included in the employee's personnel file);
- suspension; and
- employment termination.

In addition to the disciplinary action(s) set forth above, and on the advice of legal counsel, the Practice may turn an employee who has committed a Violation over to the appropriate authority for criminal prosecution, as appropriate or as required by law.

G. Auditing and Monitoring

To ensure ongoing HIPAA compliance, Compliance Personnel shall conduct regular auditing of Practice functions and operations subject to HIPAA laws and regulations. Those Practice functions/operations include, but are not limited to, the following:

- Protection of patient information
- Security measures for information systems

Audits may include a complete evaluation of Practice procedures, a detailed examination of randomly selected transactions, and a report of the findings for the HIPAA Compliance records.

In addition, Compliance Personnel, in conjunction with the site coordinators will regularly monitor the performance of all Affected Employees to ensure compliance with all applicable compliance standards and policies.

If, based upon an audit, the Practice is found to be non-compliant with any HIPAA law or regulation, Compliance Personnel, in conjunction with the legal counsel, as appropriate, shall take prompt remedial action.

H. Responding to Inquiries

If any employee of the Practice receives an oral or written inquiry regarding the Practice's compliance with any HIPAA law or regulation or private payor requirement, from any

source, whether governmental or private, the employee shall immediately notify Compliance Personnel prior to responding in any way to the inquiry. Compliance Personnel shall:

1. Identify the person or entity making the inquiry;
2. Verify their authority for the inquiry; and
3. Ascertain the nature of the inquiry.

Compliance Personnel shall then immediately notify legal counsel to assist in responding to the inquiry.

I. Certification of Review of Manual

Staff is required to execute the HIPAA Staff Certification form attached as Exhibit G to this Manual.

III. INTRODUCTION TO HIPAA

A. Overview

What is the Health Insurance Portability and Accountability Act of 1996, otherwise known as "HIPAA?" How does it affect our medical Practice?

HIPAA was originally created to provide a mechanism for workers to continue health benefits when they changed jobs. Hence, the word "portability" in the title of the Act. However, as Congress delved into the world of health care, it became apparent that the health care industry was fraught with redundancies and inefficiencies. Congress determined that significant amounts of money could be saved if the industry became more uniform in its business operations. This led to the second major component of the HIPAA legislation: Administrative Simplification. With the addition of this important element, HIPAA has grown to mean ***much more*** for health care providers than originally anticipated.

With the importance of both the Internet and the possibility of real electronic communications of patient information, there is a heightened awareness of the issues regarding patient privacy. These concerns involve privacy in general, and the possibility that health information that specifically identifies a person may inadvertently become available to others, despite the individual patients' expectation of privacy of that information. Congress anticipated the increased use of the Internet in the health care industry and the related potential privacy and security concerns. HIPAA specifically charged the Department of Health and Human Services ("HHS") with developing specific regulations to create standardized procedures aimed at reducing costs and address both the security and privacy issues.

HHS has responded by promulgating a series of regulations pursuant to HIPAA. There are three main sets of HIPAA regulations affecting medical practices:

1. Standards for Electronic Transactions

The "Electronic Transactions Regulations" were made final on October 16, 2000. Although not the focus of this Manual, HIPAA requires compliance with these regulations.

The Electronic Transactions Regulations adopt standards for the exchange of information between parties to carry out financial or administrative activities for eight specific electronic transactions:

- Health care claims encounter information;
- Eligibility for a health plan;
- Referral certification and authorization;
- Health care claim status;
- Enrollment and dis-enrollment in a health plan;
- Health care payment and remittance advice;
- Health care premium payments; and,
- Coordination of benefits.

Most of these regulations are technical in nature and will be accomplished through software. The Practice's Compliance Personnel has confirmed with the Practice's vendors that our systems are HIPAA compliant.

These technical regulations also specify the code sets required for all health care electronic transactions, including CPT-4 for procedures, ICD-9-CM[1] for diagnoses, and HCPCS

[1] ICD-10-CM diagnosis codes will be used beginning October 1, 2013.

for equipment and supplies. For drugs, use of either the HCPCS "J-Codes" or NDC or other codes are permitted. The Practice already uses these code sets now, so this should not represent anything more than a codification of existing policies and procedures.

2. Security and Electronic Signature Standards

Today's technology has enabled electronic medical records and all the personal data contained within those records to be seamlessly transmitted in a virtually instantaneous and paperless transmission with a mere keystroke. In seconds, highly personal health information is captured by insurance companies, remote office terminals, research facilities and countless other individuals and entities. In some cases, however, that information may be subject to inadvertent disclosure or unauthorized use that infringes on a patient's privacy rights. With this in mind, the HIPAA Security Regulations were created to impose standard procedural safeguards to guard the integrity of how both electronic health and electronic medical information is handled.

While the Security Regulations seek to protect "e-PHI" from prying eyes, patient privacy is not the sole purpose for enacting the regulations. The Security Regulations are also intended to diminish the patient fear that intimate, traceable information will be subject to unauthorized use or embarrassing disclosure, by implementing administrative, physical, and technical safeguards covering how that information will be handled.

While packaged as a discrete set of regulations, the Security Regulations are intended to work *in concert* with the HIPAA Privacy Regulations to ensure complete confidentiality of patient health information. To be clear, however, while the Privacy Regulations set forth standards for ***all health information,*** which identifies a particular patient, the Security Regulations set forth the procedures to be put in place to protect only ***electronically*** *stored or*

transmitted health information from unauthorized interception, access, disclosure or use. Therefore, while the Privacy Regulations cover the entire universe of health information containing identity-laced data, the Security Regulations cover only a subset of that health information, that which is stored ***electronically***.

The Security Regulations generally require covered entities to:

- *ensure* the confidentiality, integrity, and availability of electronic protected health information ("e-PHI") that the entity creates, receives, maintains and transmits;
- *protect against* any reasonably anticipated threats or hazards to the security or the integrity of that (electronic) data;
- *protect against* any reasonably anticipated uses or disclosures of that (electronic) information which are not permitted by the Privacy Regulations; and
- *ensure* that the Practice and its workforce understand and comply with these regulations.

Like the Privacy Regulations, the Security Regulations are *flexible* and they incorporate a sliding scale of expected compliance. Thus, a small practice will not be held to the same standard as a mega-group or clinic. The Security Regulations are also "technology neutral," in that they are designed to incorporate future technology advances without necessitating a re-writing of the rules.

The Security Regulations lay out three (3) general categories of safeguards: Administrative, Physical and Technical. These safeguards are further broken down into standards. These standards are the general statements of requirements and are further broken down into (required and addressable) actual implementation specifications, which are essentially the guidelines to help implement the standards. For a matrix of all the implementation specifications (both required and addressable), see Exhibit CC.

There are two types of implementation specifications: "*required*" and "*addressable.*" The *required specifications* are actions that each covered practice **must** do in terms of handling

e-PHI. In other words, if the Practice does not implement the required implementation specification, then it cannot implement the standard, and therefore it cannot be deemed to be in compliance with the Security Regulations.

Addressable specifications are ones that each practice must *evaluate and consider* implementing, though it need only do so if it is appropriate for the Practice at that time (and when periodically reconsidered). If it is not appropriate to implement the standard, then the Practice need only document the reason it is not appropriate to the Practice at that time and under its current situation what (if anything) the Practice did instead to accomplish the intent of the standard. See Exhibit DD for the form that must be completed when implementing an alternative to an addressable specification.

3. Standards for Privacy of Individually Identifiable Health Information

The "Privacy Regulations" were made effective on April 14, 2001 after an extended review and comments period. Health care providers, group health plans, and other businesses had until April 14, 2003 to come into compliance with the significant array of new requirements.

Unlike other major pieces of federal legislation affecting medical providers, such as the Fraud and Abuse and Stark statutes, it is interesting to note that HIPAA and the regulations derived from HIPAA apply to all payers including, **but not limited to**, federally funded programs such as Medicare and Medicaid.

Also, HIPAA rules apply to virtually all "*covered entities,*" regardless of whether federal funds are involved, which include health care providers that transmit health information in electronic form, private and federally funded insurers, and health care clearinghouses. The regulations also apply directly to other entities dubbed "Business Associates," that receive PHI

from covered entities to help the covered entities perform certain jobs (such as billing, legal, actuarial, accounting, consulting, management, administrative accreditation, data aggregation, financial services). Basically, this means that health care providers must have a (HIPAA) plan or protocol to protect individually identifiable health information, and a mechanism for being sure that your business contacts who come into contact with that information, as well as any subcontractors with whom they share information, will also protect the information that you passed on or made available to them.

The HIPAA Privacy Regulations require that a "covered entity" adopt and implement *formal policies and procedures* to protect individually identifiable health information and manage the personnel who come in contact with the information. Thus, any effective policy both informs employees and contractors of their responsibilities to protect patient related personal and proprietary information, *and educates and enforces those guidelines.*

The HIPAA rules regulate all PHI regardless of how that information is stored or transmitted, and the rules *apply to all covered entities regardless of their actual size.*

The Privacy Regulations state that to be most effective, a HIPAA Compliance Plan should contain certain minimum elements. Thus, while actual HIPAA compliance may vary among similar types of organizations, any covered entity should nonetheless address the basic components outlined in the various regulations. As your Practice grows in size, fuller adaptation of each of these elements is encouraged and recommended.

Criminal and civil penalties apply for violating HIPAA regulations. Civil penalties range from a low fine of not more than $100 per person, per violation to a high fine of $1,500,000 annual maximum per violator for identical violations. Criminal penalties range from the low end of $50,000 and/or imprisonment up to one (1) year to the high end of a $250,000 fine and/or

imprisonment for up to ten (10) years. Both entities and potentially key personnel at the entity involved may be subject to criminal penalties.

You should know that the HIPAA Regulations ***preempt*** all state regulations, unless the state regulation provides *more* stringent protection of the PHI, or the Secretary (later) determines that the state law may supersede. The regulations are enforced by the Office for Civil Rights of the Department of Health and Human Services. Under the HITECH Act, state attorney generals are permitted to enforce HIPAA violations if the violation has not been corrected within thirty (30) days and the violation threatens or adversely affects one or more of the state's residents.

B. HITECH/OMNIBUS FINAL RULE

Recently, Business Associates were directly affected by legislation. On February 17, 2009, Congress enacted the American Recovery and Reinvestment Act of 2009 ("ARRA") (Pub.L. 111-5). ARRA (among other Acts) was basically an economic stimulus package intended to rev up the U.S. economy. Included in ARRA is the HITECH Act, which provided sweeping changes to the HIPAA Regulations. The most important change was to apply the Privacy and Security provisions of HIPAA directly to Business Associates. Business Associates are now required to comply with the Security and Privacy Regulations under HIPAA and are further subject to civil and criminal penalties for violations of HIPAA.

On August 24, 2009, the Federal Register published the Department of Health and Human Services' interim final rule regarding breach notification requirements. This rule was published in accordance with the mandates of the HITECH Act, passed as part of ARRA. Under these regulations, health care providers, health care plans, and other covered entities are also required to notify individuals when their health information is breached.

On January 17, 2013, the Department of Health and Human Services published a final rule implementing a number of provisions of HITECH. This rule, known as the Omnibus Final Rule, also made changes to the HIPAA privacy and security rules, strengthening the protections for PHI established under HIPAA's original regulations. Key provisions of the Omnibus Rule include: The creation of a new breach standard; restrictions on marketing and the sale of PHI; patients' rights to limit certain disclosures; patients' rights to request electronic copies of their medical records; extension of many HIPAA requirements to business associates; required changes to a provider's Notice of Privacy Practices; and required changes to the terms of Business Associate Agreements.

C. Key Terms

Business Associate. A "Business Associate" is a person or entity who acts on behalf of a covered entity (but not as an employee), to assist in any function involving the actual or potential disclosure of IIHI. Thus, for example, any person or entity doing business with a covered entity where IIHI could be exchanged or disclosed would be deemed to be a Business Associate. Thus, independent contractors (physicians, physician extenders, contract managers, billing services, transcription services etc.), as well as accountants, lawyers, software vendors, contractors for ancillary services, and the like, are all included. In addition, any subcontractor that creates, receives, maintains or transmits IIHI on behalf of a business associates is considered a business associate as well.

Breach. A "Breach" is the acquisition, access, use, or disclosure of PHI in a manner not permitted by HIPAA, which compromises the security or privacy of such information.

Covered Entity. A "Covered Entity" is any person or organization, including health plans, health care clearinghouses or health care providers including physicians, practices, hospitals, or other businesses who transmit (or have a business associate who comes into or transmits on their behalf), any IIHI in an electronic format in connection with transactions covered by HIPAA.

Electronic health records ("EHR"). An electronic health record is an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

Health care provider. Health care provider is used in the common meaning to include physicians and their medical practices, hospitals, SNFs, CORFs, home health agencies, hospices and those who provide medical, dental, nursing or allied health services. Only health care providers that transmit health information in electronic form in connection with certain transactions are covered entities. However, once you are a covered entity, the Privacy Regulations will apply ***both*** to electronic and non-electronic information.

Health Information. Health information includes any information created or received by a health care provider relating to: (1) the past, present or future health condition of an individual; (2) the provision of health care to an individual; and/or (3) past, present or future payment for provision of health care. Health information includes anything recorded or transmitted orally or recorded in any other form or medium (such as electronic, tape, etc).

Individually Identifiable Health Information (IIHI). IIHI is any information that: (1) *is created or received* by a health care provider, health plan, employer, or health care clearinghouse; *and* (2) relates to the past, present, or future physical or mental health or condition

of an individual, the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (3) either actually or reasonably could identify the individual. IIHI generally identifies or potentially would identify a specific patient. IIHI includes demographic information, patient name, actual or electronic addresses, phone and fax numbers, and unique identifiable numbers and characteristics (e.g., social security numbers and the like.)

Protected Health Information (PHI). Any IIHI that can be associated to an individual that is transmitted or maintained in electronic or other medium is deemed to be PHI. Thus, any of the following items could potentially be PHI:

- Patient charts and other records containing IIHI
- Benefit Management Information
- Claims or encounter forms
- Claim status information
- Coordination of benefits forms or information
- Eligibility for a health plan
- Enrollment or dis-enrollment processing in a health plan
- Explanations of Benefits
- Reports of injury
- Health claims attachments
- Health Data Analysis (if specific to an individual and not the Practice generally)
- Payment or remittance forms or advice
- Practice Management
- Payment of claims, premiums, etc.
- Referral forms certification of medical necessity and authorization of payment of benefits
- Utilization Review
- Other transactions as may be prescribed by regulation

Unsecured PHI. "Unsecured PHI" is PHI that is not secured through the use of a technology standard that renders it unusable, unreadable, or indecipherable to unauthorized

individuals through the use of encryption or destruction, which are the technologies or methodologies specified by the Secretary of HHS in the guidance issued under the ARRA.

IV. PRACTICE HIPAA PRIVACY POLICIES

A. Notice of Privacy Practices

The HIPAA Privacy Regulations require health care providers to furnish patients with a written notice of the Practice's policies and procedures regarding the use and disclosure of protected health information. This Notice of Privacy Practices is the starting point under HIPAA. Our Notice of Privacy Practices is attached as Exhibit H to this Manual. It describes how the Practice will be handling confidential patient information in accordance with the HIPAA regulations and has been updated to include the HITECH and Omnibus Rule changes. Please review it carefully so that you can explain it to patients if asked.

The Notice is posted on the wall of our waiting area and is also posted on our website. Front desk personnel should provide each patient (new or established), at the time of the first office visit, with a laminated copy of the Notice for review and return to the front desk prior to being seen by the doctor. The Practice will also keep on hand paper copies of the Notice for patients who ask for a take-home copy. A current copy of the Notice need only be provided once to the patient.

If the Notice is ever materially changed in terms of the description of permitted disclosures, patient rights, the Practice's legal duties, or other privacy practices, then the Notice must be redistributed once to each patient at that time. The most recent redistribution occurred in 2013, when the Notice was changed to reflect the requirements of HITECH and the Omnibus Rule.

B. Written Acknowledgment

When the patient receives the laminated Notice, front desk personnel should provide the patient with the Written Acknowledgement form included as Exhibit I to this Manual, and ask the patient to sign. This form merely signifies that the patient has received a copy of the Notice. We are required by HIPAA to seek the patient's signature on this form. Once signed, it should be placed in the patient's chart. A notation should also be made on the patient's computer record, so that we need not go to the chart to determine when the patient received a copy of our Notice.

If the patient refuses to sign the Written Acknowledgement, he or she may still be seen by the doctor. Simply use the Good Faith Documentation form attached as Exhibit J to this Manual to establish that we made a good faith effort to obtain the patient's signature. Then file it in the patient's chart, and enter on the computer the date that the Notice was provided (even if no signature was obtained.)

If the patient is a minor (under 18) or incompetent (doesn't have mental capacity to act for himself or herself), the patient will not have legal authority to sign the HIPAA Written Acknowledgement form. (See discussion below of Minors and Incompetent Patients). In this situation, it is the parent or legal guardian who should be presented with the Notice and asked to sign the form. Identification of the patient or legal representative will be confirmed per our Identify Theft Prevention Guidelines.

Special problems present if the minor or incompetent patient is not accompanied by the parent or legal guardian. Babysitters, friends, relatives, nurses aides, etc. do not have authority to sign for minor or incompetent patients. In this situation, it is fine to treat the patient, but (a) give the babysitter, relative, nurses aide, etc., a copy of the Notice and a copy of the HIPAA Written

Acknowledgement form, and ask them to have the parent or legal guardian sign the form and return it to the Practice, or (b) mail a copy of these materials to the parent or guardian with instructions to sign and return the form to the Practice. Complete the HIPAA Good Faith Documentation form, indicating that these steps have been taken. Place the HIPAA Good Faith Effort Documentation form in the patient's chart, and make a notation on the patient's computer record. When the signed HIPAA Written Acknowledgement form is finally received, place it in the chart and note this on the computer.

If the Practice does not subsequently receive back from the parent or guardian the signed Acknowledgement, repeat the process on subsequent visits until either the parent/guardian refuses to sign or an acknowledgement is obtained. Note all such efforts in the chart on the (original) HIPAA Good Faith Documentation form.

C. Staff Access to Information

HIPAA provides that staff member job functions should be reviewed to determine the level of PHI access that the staff member strictly needs to do their job. Staff members should only have the minimum access necessary, and no more.

In our office, essentially all staff members need access to the patient chart and/or patient computer records at various times. We have determined, in conjunction with our advisors, that it is not practical, given our small staff, and the configuration of our software, to segregate information access by staff identity. However, all staff is required to exercise judgment when accessing patient information. If you don't need to see it, don't look at it!

D. Releasing Information

When disclosing PHI to others outside the Practice, think of a "HIPAA Hotel." It's like the "Roach Motel" – easy to check into, hard to check out of.

In other words, PHI can enter the Practice (the "HIPAA Hotel") very easily. When a patient calls for an appointment, we have received PHI (patient name, reason for visit, etc.). But HIPAA says that the information may not leave the "Hotel" unless a specific HIPAA provision permits this. So before you release information to a lab, physician, hospital, or anyone else, ask yourself if HIPAA permits this type of disclosure.

Fortunately, HIPAA contains three major "information exit" exceptions that should cover 99% of the information that we release from our Practice.

First is the "Treatment" exception. We may release PHI to any other "Covered Entity" such as a medical practice, lab, hospital, diagnostics entity, etc. for that entity's treatment of the patient. You may disclose PHI to school nurses within the "treatment" exception.

Next is the "Payment" exception. We may release PHI to obtain payment for our own services, or to help another Covered Entity or health care provider obtain payment for their services, such as in COB situation. "Payment" includes verification of coverage, pre-certifications, referrals, claims processing and the like.

Third is "Operations." This covers such items as general practice administration, utilization review, quality assurance, credentialing, privileging, etc.

"TPO" (Treatment, Payment, Operations) seems to cover almost everything. But not quite. What about reporting child abuse situations to government authorities? That's not treatment, it's not payment, and it's not operations. So you need to look for another HIPAA

exception that fits. Fortunately, HIPAA allows a number of other exceptions, including reports to governmental authorities that are required by law, such as child abuse, as follows:

- Emergency Situations. We may disclose PHI to an organization assisting in a disaster relief effort or in an emergency situation so that the patient's family can be notified about the patient's condition, status and location.

- Research. Under certain circumstances, we may use and disclose PHI for research purposes regarding medications, efficiency of treatment protocols and the like. All research projects are subject to an approval process, which evaluates a proposed research project and its use of medical information. Before we use or disclose medical information for research, the project will have been approved through this research approval process. We must obtain an authorization from the patient before using or disclosing his or her individually identifiable health information for research unless the authorization requirement has been waived by an IRB or Privacy Board.

- Required By Law. We must disclose PHI when required to do so by federal, state or local law. In Connecticut for instance, child abuse must be reported to the authorities.

- To Avert a Serious Threat to Health or Safety. We may use and disclose PHI when necessary to prevent a serious threat either to the patient's health and safety or the health and safety of the public or another person. Any disclosure, however, must only be to someone able to help prevent the threat.

- Organ and Tissue Donation. If the patient is an organ donor, we may release medical information to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, as necessary to facilitate organ or tissue donation and transplantation.

- Workers' Compensation. We may release medical information about the patient as required by workers' compensation rules. These programs provide benefits for work-related injuries or illness.

- Public Health Risks. Law or public policy may require us to disclose medical information about the patient for public health activities. These activities include the following:

    - to prevent or control disease, injury or disability;
    - to report births and deaths;
    - to report child abuse or neglect;
    - to report reactions to medications or problems with products;
    - to notify people of recalls of products they may be using;
    - to notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition;

- to notify the appropriate government authority if we believe a patient has been the victim of abuse, neglect or domestic violence;
- to notify a school of proof of immunization, provided the school is required by law to obtain this information and we have authorization from a parent, guardian or the student if he/she is an adult or emancipated minor.

- Investigation and Government Activities. We may disclose medical information to a local, state or federal agency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections, and licensure. These activities are necessary for the payor, the government and other regulatory agencies to monitor the health care system, government programs, and compliance with civil rights laws.

- Lawsuits and Disputes. If the patient is involved in a lawsuit or a dispute, we may disclose medical information about him/her in response to a court or administrative order. We may also disclose medical information about the patient in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute. (See discussion of subpoenas below.)

- Law Enforcement. We may release medical information if asked to do so by a law enforcement official:

  - In response to a court order, subpoena, warrant, summons or similar process;
  - To identify or locate a suspect, fugitive, material witness, or missing person;
  - About the victim of a crime if, under certain limited circumstances, we are unable to obtain the person's agreement;
  - About a death we believe may be the result of criminal conduct;
  - About criminal conduct at the Practice; and
  - In emergency circumstances to report a crime; the location of the crime or victims; or the identity, description or location of the person who committed the crime.

- Coroners, Medical Examiners and Funeral Directors. We may release medical information to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death. We may also release medical information about patients of the Practice to funeral directors as necessary to carry out their duties.

- Inmates. If the patient is an inmate of a correctional institution or under the custody of a law enforcement official, we may release medical information about him or her to the correctional institution or law enforcement official. This release would be necessary (1) for the institution to provide the patient with health care; (2) to protect his/her health and safety or the health and safety of others; or (3) for the safety and security of the correctional institution.

- Serious Imminent Threat. We may release PHI if necessary to avert or lessen a serious and imminent threat to a person or the public.

if you are not sure about a given disclosure, ask our Privacy Officer.

E. Authorizations

HIPAA specifies that if no exception is available for a given disclosure, you must obtain a written authorization from the patient to release the information. "Authorizations" are basically patient consent forms that contain certain specific provisions required by HIPAA. The Practice's HIPAA compliant Authorization Form is attached to this Manual as Exhibit K.

Thus, if you cannot find an applicable HIPAA exception for the planned disclosure, you have only two options: (a) have the patient execute an Authorization form (which can direct disclosure to a third party), or (b) hand the requested information directly to the patient, and tell the patient to give the information to the person who has requested it. This last alternative is a very convenient "escape hatch"; when in doubt, there is generally not a problem to give the patient's information directly back to the patient. What the patient then does with his or her own PHI is their business.

Typical situations where authorizations are needed are:

- Release of medical records to qualify for life insurance coverage;
- Release of school physical results to the school, for purposes of qualifying for team sports, etc. (easiest course is just to give the patient the information and instruct to send to school);
- Clinical trial participation (release of information to pharmaceutical company is not for treatment; it's for research, which is not a HIPAA exception);

- Completion of Family Medical Leave Act forms for employers (release of information to employer is not "treatment " – easiest course again is to give the patient the information, and instruct them to give the information to the employer);
- Psychotherapy notes in the chart (psychotherapy notes are notes by a mental health professional regarding the contents of counseling conversations and do not include such items as medication information, results of clinical tests, summary of diagnosis or symptoms or prognosis or progress to date.);
- Marketing communications, unless they are face-to face communications by the Practice to an individual or a promotional gift of nominal value given by the Practice to an individual.
- Sale of PHI, subject to certain exceptions such as research, treatment, payment and healthcare operations, and sale of a covered entity.

Authorizations will also be needed under Connecticut law for the following materials, if contained in the patient's chart:

- drug and alcohol abuse treatment records;
- HIV-related information;
- Mental health records of any kind;

For these items, see discussion of Connecticut law below.

When you fill out the Authorization Form, note the required "expiration date" or "expiration event." You can specify any date or event that you want that relates to the individual or the purpose of the disclosure. For instance, for authorization to provide the patient's employer with reports for Family and Medical Leave Act purposes, you could specify the expiration date as

"termination of employment." For research disclosures only, you are allowed to specify "none" as the expiration.

Sometimes you may receive an Authorization form signed by the patient that is on "somebody else's form." For instance, frequently life insurance companies have their medical technicians obtain the patient's signature on a form at the time when all the other paperwork is filled out and the patient gives a blood sample. The life insurance company then sends the form to you, asking for the medical records. Can you accept this form, or do you need to have the patient execute the Practice's own authorization form?

You may accept an outside party's Authorization form provided it has all the elements required by HIPAA, This should be confirmed by the site coordinator or physician prior to releasing the information. These are:

- A specific description of information to be used or disclosed;
- The identification of specific individuals who may use or disclose the information;
- The identification of specific individuals who may receive and use the disclosed information;
- A description of each purpose of the requested use or disclosure;
- The expiration date of the use or disclosure;
- A statement of the patient's right to revoke the Authorization at any time in writing along with procedure for revocation;
- A statement that the provider may not withhold treatment if the patient refuses to sign the authorization (except as noted below for research, school physicals and other situations where treatment would not normally be provided unless the patient authorized disclosure of his or her PHI);
- A statement that the PHI used or disclosed may be subject to re-disclosure by the party receiving the information and may no longer be protected;
- Patient's signature and date.

If the form you are sent does not have these elements, have the patient execute the Practice's Authorization Form.

Note: With respect to the second-to-last bullet above, there are exceptions to the rule that a provider may generally not condition treatment upon the patient's execution of the authorization. The exceptions are:

- Provision of research-related treatment;
- Provision of health care that is solely for the purpose of creating PHI for disclosure to a third party, where the disclosure will require an authorization (for instance, a school physical).

In these situations, the provider is permitted to condition treatment upon execution of the authorization, since without the authorization there is no point in providing treatment. In this situation the authorization should state that the provider may withhold treatment if the patient refuses to sign.

Please be sure to give the patient a copy of the authorization, when it is signed, for their records. This is required by HIPAA.

F. Minors and Incompetent Patients

As noted, minors and incompetent patients generally cannot sign the Written Acknowledgment form for themselves. Typically, they do not have the legal authority to do this. Only the person(s) who have the ability to give informed consent for the minor or incompetent patient, under State law, can exercise these rights.

Normally, in the case of a minor, it is the parent who has such right to give informed consent for the child. Therefore it is the parent who signs the Written Acknowledgment or the

Authorization or other forms and who exercises the child's HIPAA rights as a patient. But there are exceptions. Under Connecticut law, a minor may give informed consent to his or her own treatment if any of the following apply:

- The minor desires medical services to determine the presence of or to treat venereal disease;
- The minor wants to be examined, tested, or treated for HIV and the physician has determined that notification of the parents or guardian of the minor will result in treatment being denied or the physician determines that the minor will not seek, pursue, or continue treatment if the parents or guardian are notified and the minor requests that his parents or guardian not be notified;
- The minor is seeking an abortion, subject to certain obligations of the physician to explain various options re: pregnancy to the patient and obtain her signature on a form documenting that such discussions have been provided;
- The minor needs emergency treatment and parental consent is withheld or unavailable, with such treatment provided "pending receipt of parental consent;"
- The minor is seeking outpatient mental health treatment (excluding certain drugs) from a psychiatrist, psychologist, certified social worker, or licensed family therapist, subject to certain restrictions.

In these situations, since the minor can give informed consent, he or she has the right to act on his/her own behalf, as far as HIPAA is concerned. This makes sense; if the minor can consent to his or her own treatment, surely he/she should have the right to his or her information under HIPAA.

Note: under Connecticut law, a minor who has been married or borne a child may give consent to medical services for his or her own child.

G. Divorced Parents

Sometimes medical practices are in the middle of a dispute between divorcing or divorced parents. There is a dispute over whether Johnny should continue treatment with the Practice, or whether the Practice should be providing information to the other parent.

The question to ask yourself is this: "Who has the right to give informed consent for the minor child?" It is the parent with legal custody. "Legal custody" means the legal right to make major decisions for the child, such as education, religious affiliation, and medical matters. Legal custody is established in a divorce decree or other court order. So if a dispute arises, ask which parent has legal custody, and demand to see the court order establishing it.

H. Friends and Family

"Friends and family" pose a special challenge. These are the people who come with the patient to the doctor's office, or who pick up the phone when you call the patient's home.

Under HIPAA, friends and family, even spouses, are not entitled to the patient's information. Only the patient himself or herself has an absolute right to this information. The exception is parents of minor children or other legal guardians, who are generally to be treated for HIPAA purposes as if they were the patient, as noted above.

Having said this, HIPAA does permit some sharing of information with friends and family. HIPAA specifies that the Practice may, without written Authorization, disclose to a "family member, other relative, or a close personal friend of the [patient], or any other person

identified by the [patient], the PHI directly relevant to such person's involvement with the [patient]'s care or payment related to the [patient's care]." However, there are some "strings attached." To disclose to these people (referred to in this Manual as "friends and family"), one of the following must apply:

- The Practice obtained the patient's oral or written agreement to disclosing information to the person in question;
- The Practice provided the patient with the opportunity to object to the disclosure, and the patient did not object;
- The Practice could "reasonably infer from the circumstances, based on the exercise of professional judgment, that the [patient] does not object to the disclosure," such as when the friend or family member accompanies the patient into the exam room, or when a child arrives at the doctor's office in the care of a babysitter (presumably the parent wants the babysitter to receive all resulting diagnoses and care instructions), or where a patient arrives from the nursing home in the care of a nurse's aide;
- It is an emergency situation or the patient is incapacitated, so that there is no chance to provide the patient with the opportunity to agree or object;
- The friend or family member has been sent to pick up filled prescriptions, medical supplies, x-rays, or other PHI, in which case the Practice is permitted to make a reasonable inference as to the patient's best interest, in accordance with common medical practice.

If a patient wishes to identify a family member or other person with whom their medical information may be shared, use the Patient Communication form attached as Exhibit L to this Manual, which gives the patient the opportunity to designate individuals to whom it is okay to make a disclosure of PHI. This form should be kept inside the patient's chart and updated as designated acceptable PHI recipients are added or dropped. It is not necessary that the patient sign this form to add or drop individuals from the list, since oral agreement suffices. Also, the friends and family who are named on this form do not represent the only individuals authorized to receive the patient's PHI. As noted, there may be situations where the Practice is entitled to infer that the patient does not object to the release of information, such as in the case when the

friend or family member accompanies the patient into the exam room, or a child arrives at the doctor's office in the care of a babysitter.

Simple appointment reminders can generally be left with family members even if the family member is not explicitly designated as a PHI recipient on the Patient Communication form. However, check the Patient Communication sheet to see if the patient has requested an alternative means of communication, and if so, honor it. In any event, do not indicate to the family member the reason for the patient's doctor visit.

I. Incidental or Inadvertent Disclosures

Taken literally, HIPAA's prohibition against the disclosure of PHI would probably bring most medical practices to a standstill. For instance, the mere announcement of a patient's name in the waiting room is a disclosure of PHI – the patient's name. The same applies to sign-in sheets, overheard conversations with the check-in or check-out clerk regarding follow up appointments, or other common situations where one patient inadvertently learns information about another patient.

In changes to the HIPAA regulations and other announcements, the Bush Administration indicated that it understands that some inadvertent disclosures are inevitable in medical practices. For example, sign-in sheets are acceptable, as is calling out patient names in the waiting room. Practices are not required to install soundproof walls, as some had feared.

Overheard conversations and other such inadvertent disclosures are called "incidental disclosures." Under HIPAA, incidental disclosures are not violations, provided that the Practice has taken reasonable steps to "safeguard" PHI and avoid incidental disclosures to the extent possible.

In conjunction with the development of this Compliance Manual, the office's physical layout, computer systems, and administrative procedures were reviewed for their adherence to HIPAA's requirement of "reasonable safeguards." These systems will continue to be monitored and adjusted to minimize incidental disclosures of PHI. Staff are expected to do their part by observing any safeguards that are put in place, and by using common sense: keep your voice down, exercise caution when disclosing information, and don't leave PHI lying around where patients or other unauthorized persons may see it.

J. Faxes, Answering Machines, Messages, Email

As noted, HIPAA requires "reasonable safeguards" to avoid the disclosure of PHI. Although some inadvertent disclosures will be excused as "incidental," the Practice has established the following procedures to minimize the likelihood of HIPAA violations:

- Do not fax information to patients; mail it. This will minimize the chances of a fax going to the wrong fax number.
- Faxes to hospitals, other physicians, labs, and other routine recipients are acceptable. However, double check the fax number before sending, and always use a cover sheet indicating that PHI may be attached and that if the fax has gone to the wrong person, it should be returned or destroyed.
- Leaving messages on answering machines for appointment reminders is acceptable. Do not indicate the reason for the visit. Do not leave messages regarding lab or diagnostic results (even negative results) or any kind of medical information on the answering machine. Just ask that the call be returned. Do not leave a message of any kind on the answering machine if the answering machine tape does not furnish some reasonable indication that you have reached the correct number.
- Leaving messages with family members at home is also okay for appointment reminders. Indicate only that an appointment is scheduled, not what the visit is for. Do not leave any other kind of information, unless your records show that the person on the phone is a "friend or family" designated by the patient to be a permitted recipient of PHI.
- Leaving messages at work is very sensitive. Avoid calling the work number, but if necessary ask for a return call and nothing more.

- Appointment reminders by post-card is acceptable, so long as the appointment is of a routine nature.
- Do not include PHI in unencrypted email.
- Do not use email to communicate with patients unless the Privacy Officer has developed a specific written policy.

K. Reasonable Restrictions and Alternative Communications

Under HIPAA, patients can request modification of our Privacy Policies. As an extreme example, a patient could request that his or her medical chart be kept in a separate safe under lock and key, or to enter the office by a back door, so that he or she is not seen in the waiting area. We are not required to agree to such requests (reasonable or not), with a few exceptions discussed below. All such requests for restrictions, other than those noted below, should be forwarded to the Privacy Officer. No staff member other than the Privacy Officer should decide whether to accept a restriction.

The exceptions noted above relate to the patient's specification of "reasonable requests" to receive communications of PHI by "alternative means or at alternative locations." In other words, the patient can say "don't call me at work" or "don't leave a message on my answering machine" or "send your bills to a P.O. Box." We are required to accommodate such requests as long as the patient provides an alternative means of being contacted and provides an acceptable means, if appropriate, for payment for services to be made.

Any restrictions on use of PHI should be documented using the attached Exhibit M "Request to Restrict Use of Medical Information" form and should be brought to the immediate attention of the Privacy Officer for review and decision. Any request for "alternative communications" should be documented on the attached Exhibit L "Patient Communication"

form. Generally, if all the patient wants is to be contacted at one location versus another, it is fine to agree to this, unless the Privacy Officer has specified otherwise.

All restrictions that the Practice agrees to, and all reasonable requests for alternative communication, should be noted in the chart and on the computer system to ensure adherence to the agreed arrangements going forward. Please be advised that under HITECH, the Practice may not refuse a patient's request to not use or disclose that patient's PHI in instances where the disclosure is to a health plan for payment or health care operations (not treatment) and the PHI pertains solely to a service where the patient paid out of pocket and in full.

L. Connecticut Law: Drug and Alcohol, Mental Health, HIV, Copying Charges

Federal laws generally pre-empt or control any inconsistent state laws. However, HIPAA specifically provides that state law is the dominant rule if it specifies a "more stringent " privacy standard. "More stringent" means that state law:

- Specifies a more restrictive standard in terms of releasing patient information to third parties; or
- Provides the patient with a greater right of access to their own information.

Connecticut has a hodge-podge of different rules regarding the handling and release of patient information. The most widely applicable rules of concern to Connecticut medical practices involve the following:

- General doctor-patient privilege (protects medical information from subpoena and use in lawsuits (CGSA § 52 - 146o);
- HIV-related information (CGSA § 19a - 583, 584, 585);

- Mental health treatment by a psychiatrist or psychologist or therapist (CGSA 52 - 146c through 146f, 146i, 146p, 146q, 146s);

- Medical chart copying charges (this effects patient access to the medical record) (CGSA § 20 - 7c);

- Drug and alcohol abuse records are not protected by Connecticut law, but then are protected under federal law: the Drug Abuse Prevention, Treatment and Rehabilitation Act (21 U.S.C. 1175 and 42 CFR Part 2).

* * *

1. Doctor-Patient Privilege. See discussion below under Section N (Subpoenas).

2. HIV. Medical practices in possession of HIV-related information may disclose the information without the patient's written consent to:

- a federal, state or local health officer, when such disclosure is mandated or authorized by law;
- a health care provider, when such knowledge is necessary to provide treatment or is already recorded in a medical record that the provider has access to;
- a medical examiner to assist in determining the cause of death;
- health facility accreditation/oversight committees conducting monitoring, evaluation or reviews;
- a health care provider who in the course of his occupational duties has had significant exposure to HIV, provided that a number of criteria are met;
- employees of hospitals operated by the Department of Mental Health and Addiction Services if the infection control committee of the hospital determines the patient's behavior posses a significant risk of transmission to another patient of the hospital and there are no other reasonable alternatives to prevent the risk of transmission;
- employees of facilities operated by the Department of Correction to provide services related to HIV infection or if the medical director and chief administrator determine an inmate's behavior possess significant risk of transmission to another inmate and no reasonable alternative exists to prevent the transmission;
- any person allowed access by a court order;
- life and health insurers, government payers, health care centers (and their affiliates), reinsurers, and contractors, except agents and brokers, in connection with underwriting and claim activity for life, health and disability benefits; and
- any health care provider specifically designated by the protected individual to receive such information received by a life or health insurer or health care center pursuant to an application for life, health or disability insurance.

Connecticut law also prohibits any person to whom confidential HIV-related information is disclosed from further disclosing such information except when complying with the state law dealing with informing and warning known partners of possible exposure to HIV (Sec 19a-584) and the state law requirements for disclosure of HIV-related information (Sec. 19a-585).

A physician may warn or inform a known partner of a protected individual if both the partner and the protected individual are under the physician's care or the physician may disclose the HIV-related information to a public health officer for the purpose of warning a known partner when:

- the physician reasonably believes there is a significant risk of transmission to the partner
- the physician has counseled the protected individual regarding the need to notify the partner and the physician reasonably believes the protected individual will not inform the partner
- the physician has informed the protected individual of the physician's intent to notify the partner or public health officer

When making such a disclosure the physician must also make referrals for appropriate medical advice and counseling for coping with the emotional consequences of learning the information and for changing behavior to prevent transmission or contraction of HIV. The physician shall not disclosure the identity of the protected individual when notifying a partner and the notification should be made in person, except where circumstances reasonably prevent doing so.

The physician has no obligation to warn, inform, identify or locate any partner and has no obligation to disclose information to a public health officer for the purpose of warning or informing a partner.

Unless the HIV disclosure falls within one the itemized exceptions above, you need the patient's written consent to release the HIV-related information. If so, use our standard HIPAA authorization form attached to this Manual as Exhibit K but attach the following statement to Exhibit K required by Connecticut law:

> This information has been disclosed to you from records whose confidentiality is protected by state law. State law prohibits you from making any further disclosure of it without specific written consent of the person to whom it pertains, or as otherwise permitted by said law. A general authorization for the release of medical or other information is NOT sufficient for this purpose.

3. Mental Health and Counseling Records. Under Connecticut law, all records and communications from psychiatrists, psychologists, therapists, social workers, and professional counselors, may generally not be disclosed without the patient's written consent, even for treatment, payment, or operations purposes. Use the attached HIPAA Authorization form for any such disclosures to ensure compliance with Connecticut law and HIPAA. For psychiatrist records only, be sure to attach to the Authorization form the following language (provided in an attachment to Exhibit K):

"The confidentiality of this record is required under Chapter 899 of the Connecticut general statutes. This material shall not be transmitted to anyone without written consent or other authorization as provided in the aforementioned statutes."

4. Copying Charges. HIPAA allows providers to levy a "reasonable cost based fee" when a patient demands a copy of their record. However, Connecticut law specifies that the fee charged by a practice to the patient for copies may not exceed 65 cents per page plus the cost of first class postage if applicable. Other applicable limits are:

- No charges allowed for copying of Medicare or Medicaid records
- No charge if record is requested for purpose of supporting a claim or appeal under Social Security Act, such as claims for state disability benefits;
- The Practice's provider contracts with commercial insurers may require that we do not charge for copies requested by the insurer. This may also apply to copies requested by the patient. Check the relevant provider contract.

This list of permitted copying charges is attached as Exhibit W.

5. Drug and Alcohol Abuse. Drug and alcohol abuse records are protected by the federal Drug Abuse Prevention, Treatment and Rehabilitation Act (21 U.S.C. 1175 and 42 CFR Part 2), if the treatment was in any way provided or funded, directly or indirectly, by federal agencies. This federal law prohibits release of such drug or alcohol abuse information without the patient's consent, except in emergencies or upon court order. Practices in possession of such information should secure the patient's consent on a HIPAA-compliant authorization. Use the attached HIPAA Authorization form for any such disclosures to ensure compliance with Connecticut law and HIPAA. For drug and Alcohol abuse records be sure to attach the Authorization form (provided in an attachment to Exhibit K):

M. Subpoenas

From time to time we may be presented with a subpoena for patient medical records. HIPAA imposes new, federal restrictions on responding to such subpoenas. However, Connecticut law is more stringent than HIPAA in that it generally does not permit disclosure of medical or counseling records in response to a subpoena without the patient's written consent, or pursuant to a direct order of the court. Send the letter attached as Exhibit N to the attorney requesting the subpoena with a HIPAA Authorization form for execution by the patient.

If the subpoenaed records contain HIV related information or psychiatrist notes, be sure to attach the appropriate extra language that is discussed above in Section M and is attached to Exhibit K Authorization form.

N. Minimum Necessary

Under HIPAA, generally only the "minimum necessary" PHI is to be disclosed based on the intended purpose of the disclosure. Exceptions to this rule are:

- Disclosures to a health care provider for treatment;
- Disclosures directly to the patient;
- Disclosures pursuant to a signed Authorization;
- Disclosures required by law, such as child abuse reports.

In these situations, you need not sort through the information requested to limit the PHI disclosure to the minimum necessary. For instance, if the patient wants his or her own information, or if he she previously signed an Authorization stating that all information requested by a certain life insurance company, for example, should be disclosed. Unless one of the exceptions listed above applies, staff should take care not to disclose more information than is needed. Do not send the entire medical record unless it has been established that this is the minimum necessary disclosure needed to accomplish the purpose of the disclosure.

There is no definition of minimum necessary, yet guidance from HHS is due. In the meantime, HITECH limits the minimum necessary information to PHI in the "limited data set." HIPAA defines a "limited data set" as information that excludes identifiers such as names, postal address (other than city, state, and zip code), telephone and fax numbers, e-mail address, social security numbers, and medical record numbers.

What if the requester claims that the entire medical record is the minimum necessary needed? Can you take him or her at his word, and supply everything? No. Under HITECH the Practice must make the determination. Consult with our Compliance Personnel for assistance with requests of the entire patient medical record.

Most disclosures that we make in the routine course of business are to other doctors for treatment purposes. As noted, these disclosures are not subject to the minimum necessary rule. Nor are disclosures to the patient or pursuant to signed Authorization. In all other situations, stop and ask yourself the question, what information is really necessary to fulfill the intended purpose? Then disclose only that minimum necessary information.

HIPAA also requires that when we request PHI from another covered entity, that we limit our request to the minimum necessary information needed. However, the exceptions outlined above apply (e.g., requests for PHI for treatment purposes, etc.)

O. Logging and Accounting for Disclosures

HIPAA specifies that medical practices must keep track of certain disclosures of patient information. This is to enable the Practice to satisfy the patient's right, under HIPAA and HITECH, to an accounting of all such disclosures that have been made about him or her in the past. This includes disclosures by the Practice and its business associates of health information in both paper and electronic form. Specifically, the patient can demand that the practice itemize a list of disclosures made in the past six (6) years.[2]

[2] Once final regulations are issued regarding accountings, the Practice will only be required to account for disclosures for a period of three (3) years.

See Exhibit II for instructions regarding creating HIPAA Disclosures document in the Allscripts Enterprise EMR system.

Most disclosures of medical information by our Practice will not be subject to this log/accounting requirement. Specifically, the following disclosures need not be logged or accounted for:

- Treatment, payment, or operations;
- Disclosures made directly to the patient himself or herself;
- Disclosures made pursuant to a patient authorization, such as for research studies, life insurance applications, school physicals, etc.
- Disclosures to friends and family who are involved with the patient's care or with payment for the services provided to the patient;
- So-called "incidental" disclosures, meaning information that is inadvertently disclosed in the course of routine operations, such as when a patient hears another patient's name called out in the waiting area, or overhears a conversation between the receptionist and another patient, or glimpses of information about another patient on computer screens;
- To correctional facilities about inmates, or to other law enforcement officials about patients in their custody.

All other disclosures by medical practices are subject to log/accounting requirements. These disclosures include:

- Disclosures to business associates (unless the disclosure falls within the treatment, payment, or operations exception), such as providing copies of the patient's record to a malpractice attorney to defend the doctor;
- Reports to public health authorities, such as birth, death, communicable disease, child abuse or neglect;
- Disclosures to health oversight agencies, such as for licensing or disciplinary issues, or audits or investigations to determine compliance with Medicare or other government regulations;
- Disclosures made pursuant to court order or subpoena;
- Disclosures to law enforcement officials as permitted by HIPAA, such as disclosures made to locate a fugitive or missing person;
- Disclosures to coroners, medical examiners, or funeral directors;

Note: Disclosure of information from which individual identifying material has been removed, such as name, address, social security number, etc. is not subject to accounting.

For each disclosure that is subject to the log/accounting requirement, the practice must maintain the following information:

- Date of disclosure;
- Name of the entity or person who received the protected health information, and, if known, the address of such entity or person;
- A brief description of the protected health information disclosed; and
- A brief statement of the purpose of the disclosure, so that the patient can tell on what basis the Practice was authorized to release the information consistent with HIPAA.

Use the Log of HIPAA Disclosures form attached as Exhibit O to this Manual to track disclosures about a patient. Insert the disclosure log in the patient's chart, so that it can easily be updated whenever a "loggable" disclosure is made. Use Exhibit X to handle a patient request for accounting of past disclosures.

Moreover, the HITECH Act and the Proposed Final Rule regarding accounting of disclosures (issued May 31, 2011) require medical practices that use or maintain information in an electronic designated record set to provide a patient with an accounting of any disclosures of/access to this e-PHI, if so requested by the patient. This accounting requirement applies to all disclosures made three (3) years prior to the date of the request, and applies to disclosures and access made for treatment, payment or healthcare operations. The effective date for an accounting of disclosures was January 1, 2013 for any electronic designated record set system acquired after January 1, 2009, and January 1, 2014 for any electronic designated record set system acquired on or before January 1, 2009.

The access report must include the following:

- Date of access;
- Time of access;
- Name of person if available, otherwise name of entity, accessing the electronic designated record set;
- Description of the information accessed;
- Description of the action taken by the user.

The access report must be provided in a format that is understandable to the reader.

Note: The Practice may not charge the patient for a HIPAA accounting, unless the patient requests more than one such accounting in a 12-month period. If more than one such accounting is requested, the practice can impose a "reasonable, cost based fee" if the patient is informed in advance of the fee so that the patient can withdraw or modify the request. See discussion above of permitted copying charges.

P. Patient Access to Chart

Except for psychotherapy notes, patients generally have the right to inspect and obtain a copy of their medical chart. Have the patient fill out the "Request for Access to Medical Information" form attached as Exhibit P to this Manual. Generally, the Practice has 30 days to comply with a request for access, or 60 days if the information requested is not on-site.

We must honor the patient's request to have the information delivered in a particular format, if this can be easily done.[3] We may be entitled to demand a copying charge; see discussion above regarding copying charges.

[3] For EHRs, the patient information requested must be provided in electronic format , if so requested. Costs for providing an electronic copy may not exceed the labor costs in responding to the request.

If the patient merely wants to look at the file, not copy it, arrange a mutually convenient time and place for this to be done.

The patient's request for his or her PHI may be denied in very limited circumstances only. Access may be denied if:

- The file contains information obtained from a source other than a health care provider under a promise of confidentiality, and the access would reveal the source;
- The information requested has been compiled in a research trial that is still underway, and the patient previously agreed in writing that access would not be allowed until the trial was completed;
- A licensed health care professional has made a judgment that access would likely endanger the life or physical safety of the patient or someone else;
- The file makes reference to another person, and the licensed health professional makes a judgment that access would likely result in substantial harm to that other person;
- The information is requested by the patient's personal representative and the licensed health professional makes a judgment that access would likely result in substantial harm to the patient or another person.

If access is denied, the patient has a right to review the decision to deny access, unless it is for either of the first two reasons noted above. This review must be done by a licensed health care professional who was not involved in the original decision to deny access. If denial is appropriate, use the "Denial of Access to Medical Record" Letter found in Exhibit Q.

Q. Patient Amendment of Chart.

The patient has a right to request an amendment to their medical record (so long as we maintain it) if he or she believes it is incorrect or incomplete. To request an amendment, the patient should complete the form "Request to Amend Medical Information" attached to this Manual as Exhibit R. The amendment must be dated and signed by the patient.

We may deny the patient's request for an amendment if it is not in writing or does not include a reason to support the request. In addition, we may deny a request to amend information that:

- Was not created by us, unless the person or entity that created the information is no longer available to make the amendment;
- Is not part of the medical information kept by or for the Practice;
- Is not part of the information which the patient would be permitted to inspect and copy; or
- Is accurate and complete.

The Practice must respond to the request to amend within 60 days. Any denial should be made in writing using the "Denial of Amendment of Medical Record" letter found in Exhibit S.

R. Business Associates

The Practice is required to enter into Business Associate Agreements with our Business Associates. See the definition of Business Associate above in the "Key Terms" part of this Manual and the List of Potential Business Associates appended to this Manual as Exhibit T. Use the template Business Associate Agreement appended to this Manual as Exhibit U, or, if the Business Associate insists on using their own form, make sure it obligates the Business Associate to the contract provisions noted in the Checklist of Required Business Associate Contract Terms appended to this Manual as Exhibit V.

S. Marketing

HIPAA prohibits the use or disclosure of PHI for marketing purposes, unless the patient signs an Authorization agreeing to let us use or disclose their information for this

purpose. However, the following activities have effectively been exempted from the category of "marketing":

- Communications to the patient regarding services that we offer;
- Communications to the patient regarding treatment, such as appointment reminders;
- Communications to recommend alternative therapies, health care providers, or settings of care;
- Face-to-face communications with the patient regarding a product or service;
- Promotional gifts of nominal value provided by the Practice.

The HITECH Act contains strict restrictions on the use of PHI for marketing purposes. Our Practice may not receive direct or indirect payment (not including payment for treatment) in exchange for marketing the communications identified above unless:

- payment is for a communication regarding a drug currently prescribed for the recipient of the communication and the payment is a "reasonable amount"; and
- a valid authorization is obtained from the patient.

T. De-Identification and Re-Identification.

If information is de-identified or disassociated from a specific individual, then it is no longer PHI, and therefore not subject to the Privacy Regulations. Information that is subsequently re-identified again becomes subject to the rule.

There are two methods of de-identifying PHI. First, a covered entity may rely on a person or entity with the appropriate knowledge and experience. This person will know generally

accepted statistical and scientific principles and methods for rendering information not individually identifiable.

Second, the covered entity may remove from the data to be disclosed, each of the identifiers[4] enumerated in a lengthy list, for both the individual and relatives, employers, or household members of the individual.

U. Prohibition on Sale of PHI

The HITECH Act prohibits the Practice from directly or indirectly receiving compensation (cash or an equivalent) in exchange for a patient's PHI unless the individual provides a valid authorization. Eight exceptions to the prohibition exist:

- Public health activities;
- Research;
- Treatment;
- Sale, transfer, merger of the Practice;
- Payment by the Practice for services performed by a Business Associate;
- Copying charges;
- Required by law; and
- Other exchanges approved by HHS.

V. Coordination with Hospitals, Surgicenters, and Nursing Homes and Other Entities

Hospitals, surgicenters and nursing homes are all "covered entities" under HIPAA, and are therefore required to have their own HIPAA Compliance Manuals. Generally,

[4] Identifiers generally include a name, phone and fax numbers, actual and electronic addresses including zip codes, Social Security and other unique identifying numbers (including device identifiers), biometric identifiers (fingerprints, full face images) and/or any other unique identifying number, characteristic, or code. Regarding zip code, geocode identifying information such as the first three zip code digits would generally not be considered identifying if the zone in which the person resides has at least 20,000 inhabitants.

our doctors should be covered by these entities' HIPAA Compliance Manuals when they see or treat patients at these locations. (Double check with these entities to make sure that the Notice of Privacy Policies used by these other entities covers our doctors when they are at these facilities.) Thus, our doctors should not need to carry with them to these facilities the Notice of Privacy Policies or other HIPAA materials. However, if a patient who is first seen in the hospital or nursing home comes to the office, then at that time you should provide the Notice and other HIPAA documentation as you would with any other patient.

W. Decedents

The Practice may disclose the PHI of a deceased patient to the patient's family members, relatives or close friends, or to other individuals designated by the deceased patient, who were involved either in the deceased patient's care or payment for that care. The Practice may disclose only PHI that is relevant to the family member, relative or friend's involvement in the deceased patient's care. PHI cannot be disclosed if the Practice is aware that the deceased person expressed a prior preference for it not to be disclosed to the person in question.

V. HIPAA SECURITY POLICIES

HIPAA generally requires providers and their Business Associates to put in place "reasonable [administrative, technical, and physical] safeguards" to protect against intentional or unintentional disclosures of PHI. Thus, computers in open areas where patients, employees, etc. might gain access should be moved to more private and secure locations. A checklist of issues regarding the security of PHI can be found in Exhibit BB. Specific implementation steps can be found in the Practice's separate HIPAA Security Procedures Manual.

Other computer security measures should be taken as well. These measures are specifically addressed in the following policies.

A. Administrative Safeguards

The Practice has implemented administrative policies and procedures to prevent, detect, contain, and correct security violations. These policies and procedures are described in the following sections.

1. Security Management Process

a. *Risk Analysis*

The Practice periodically conducts accurate and thorough assessments of the potential risks and vulnerabilities of the confidentiality, integrity, and availability of e-PHI held in its computer systems including both on-site attacks and internet attacks. When the Security Officer believes any risks exist, the Security Officer addresses each risk and complete a risk mitigation report.

The Practice has implemented security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the HIPAA Security Regulations as detailed in this and related documents. Such security measures include network security policies, firewalls, and server operating system updates. Only authorized personnel may access certain levels of the computer system. Unauthorized or malicious access may be subject to legal action or employment sanctions as set forth herein.

b. *Risk Management*

As part of its risk management procedure, the Practice tracks authorized and unauthorized access to any part of the computer system.

c. *Sanction Policy*

The Practice will apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures, as detailed in the Practice's Personnel Policy Manual. Contact the Security Officer to review a copy of these sanctions. Unauthorized access by workforce members may result in removal from the premises, termination of employment and legal action.

d. *Information System Activity Review, Login Monitoring*

The Practice has implemented the procedures to regularly review records of information system activity. The Security Officer, in his/her sole discretion, periodically reviews any or all files contained on the Practice computers.. In addition the Security Officer regularly monitors usage of the Practice computers by regularly observing employee conduct for inappropriate access.

2. Assigned Security Responsibility

Our Practice has appointed the Security Officer to oversee the security of the Practice's information and technology systems. The Security Officer will serve until the Practice's Board of Directors replaces him/her or until such time as he/she resigns from the position. While there is a specific job description for the Security Officer, generally he/she is charged with the following responsibilities:

- Oversee and monitor the implementation of the Security components of the HIPAA Compliance Plan;
- Prepare and present regular reports to the Board of Directors and the Practice, as a whole, on Practice compliance;
- Develop and implement a training program focusing on the security components of the HIPAA Compliance Program, and ensure that training materials are appropriate for all Practice employees;
- Ensure that independent contractors who furnish information services to the Practice are aware of the requirements of the Practice's HIPAA Compliance Plan;
- Coordinate security compliance efforts within the Practice and establish methods such as periodic audits, both to improve the Practice's efficiency and quality of services and to reduce the Practice's vulnerability to security abuse;
- Revise the HIPAA Compliance Program periodically, in light of changes in the needs of the Practice or changes in the law of Government and private payer health plans;
- Develop mechanisms to receive and investigate reports of non-compliance and monitor subsequent corrective action and/or compliance;
- Develop policies and programs that encourage employees to report non-compliance without fear of retaliation.

This position is expected to be modified over time, as our Practice situation changes.

3. Workforce Security

a. *Authorization, Supervision, Clearance Procedure*

The Security Officer determines which workforce members appropriately have access to e-PHI. All employees who are allowed access to e-PHI are assigned a specific level of access, so that some people may be permitted greater access to more e-PHI than other individuals. Likewise, the Security Officer may assign passwords for various individuals. Those passwords are to be used only by the individual to whom they are assigned and only during office hours. No person may share either a login or a password with any other person. Passwords and logins should be committed to memory and not written down in any discoverable location.

Workforce members who do not need access to e-PHI, or otherwise, cannot obtain such access, as they are intended not to have such access, so information should not be shared with them.

b. *Termination Procedures*

When an individual's employment or other arrangement with the Practice ends for any reason, that employee's access to e-PHI and the facility is terminated by removing his or her user ID from the Practice computers and seeking return of any other means of physical access (keys, ID numbers, etc.). In addition the employee is required to turn in PDAs, access codes, portable computers and other Practice property, tangible or intangible.

4. Information Access Management/Isolating Healthcare Clearinghouse Function

The Practice currently does not perform any healthcare clearinghouse functions. However, in the future, if the Practice does perform clearinghouse functions, a procedure will be developed to ensure data security, reliability and integrity. In addition, the

Practice requires any clearinghouse it works with to be HIPAA compliant and has entered into business associate and/or confidentiality agreements as necessary.

5. Security Awareness and Training

a. Security Reminders

The Practice will conduct periodic security awareness training on an ongoing basis with the twin goals that:

(1) All employees will receive training on *how to perform their jobs in compliance* with the security policies of the Practice and any applicable regulations; and

(2) Each employee will understand that HIPAA security compliance is a condition of continued employment.

All employees are required to attend at least one HIPAA security awareness/training program per year. These programs are likely to be in-house sponsored programs. Nonetheless, the Office Manager may, in conjunction with the HIPAA Security Officer, maintain a list of other "Practice approved" security awareness/training programs.

All educational and training materials received by an employee at approved programs shall be the property of the Practice and shall be maintained in a designated location for periodic review by Practice employees.

In addition, employees shall be reimbursed by the Practice for all reasonable and necessary expenses incurred in meeting their HIPAA security awareness/training requirements at approved programs. All expenses shall be recorded and submitted on the Expense Reimbursement Request form provided in Exhibit D.

b. *Protection from Malicious Software*

The Practice's computers have anti-virus scanning software installed. Updates to that software are periodically purchased and installed when available. No employee may at any time download any non-Practice related material from the internet, or otherwise. All employees are required to review the E-mail And Other Telephonic Communications Policy in Exhibit Y. See also Exhibit Z for Our Policy on Software Piracy/Office Technology.

6. Security Incident Procedures, Response and Reporting

The Security Officer notes any security issues he/she is aware of in the Practice's incident log, and addresses them on a case-by-case basis. Each employee will be contacted directly and individually if a problem arises. The steps for responding to potential security violations are: (1) isolate the problem; (2) report the incident; (3) log the incident; and (4) correct the issue (if possible).

7. Contingency, Data Backup, Disaster Recovery, Emergency Mode Operations, Testing and Revisions

The Practice periodically backs up its computer systems, and the back-up is taken each night to a safe, off-site location. If an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) damage the Practice operational systems, hardware, or software that contain e-PHI, the Security Officer (or designated representative) shall take the back-up copy along with any other necessary data to a reliable computer and operate the system from that location. In that case, the Practice would restore the system to its last

operational state. The Security Officer (or designated representative) operates the system from that location until the disaster situation is remedied.

This procedure is tested whenever new software programs are installed to ensure data can be fully and effectively backed up, restored, and operational as soon as possible.

In addition, the Practice has established a Disaster Recovery Plan that covers simple hardware failures, as well as more critical system failures due to a catastrophic event. The Disaster Recovery Plan establishes procedures for both controllable and uncontrollable events. "Controllable" events are disasters that can be subdued by human work such as building fires, power failures, pipe leaks/bursts, etc. In a controllable event, the Practice retains the ability to either immediately repair the system or rebuild using data stored at an off-site back up. The Practice has also established procedures for uncontrollable events such as earthquakes, hurricanes, wild fires, etc. For more information, see the Practice Disaster Recovery Plan in Exhibit AA.

8. Evaluation

The Security Officer (or designated representative) performs a quarterly technical and non-technical evaluation of the procedures in this document, or any time there are significant environmental or operational changes affecting the security of e-PHI. The Practice's policy is to review all facets of data security, integrity, reliability and system functionality during such quarterly review.

9. Business Associate Contracts and Other Arrangements

The Practice has contracts in place with its business associates who create, receive, maintain, or transmit e-PHI on our behalf. If any employee needs to send or receive e-

PHI, he or she should confirm that there is a Business Associates contract in place with that recipient/sender, if one is so required.

B. Physical Safeguards

The Practice has implemented physical safeguard-related policies and procedures to prevent, detect, contain, and correct security violations. These policies and procedures are described in the following sections.

1. Facility Access Controls

Computers are kept in secure, private locations and the building is secure from unauthorized access. This is done through a key lock.

Access to e-PHI is limited. All users are assigned a unique user ID. Employees are not to share their user ID with anyone, at any time. This includes not using anyone's ID to access passwords, logins and so on.

2. Workstation Use

Workstations are to be used exclusively for Practice operations. You may not send e-mail or use instant messaging without the prior approval of the Security Officer. Consult our policies regarding E-mail and Internet use for additional information. In addition, the Practice has implemented security rights and policies within the computer infrastructure to protect against malicious attempts on the system.

3. Workstation Security

Workstation access is restricted to authorized users only. Only those personnel who require access to those systems are authorized to use them. In addition, all

monitors are positioned so that they are turned *away* from unauthorized users, including patients. All workstations are located in secure areas. If you have access to a workstation, you must use a password protected screen saver that is activated when your station becomes idle or if you leave your station unattended. The screensaver should activate after no less than three (3) minutes of non-use. The lock out should occur after not more than sixty (60) minutes of non-use.

4. Device and Media Controls

The Security Officer (or designated representative) oversees the movement, receipt and removal of all hardware and electronic media on an as-needed basis. The Security Officer also oversees the final disposition of any hardware or electronic media, and erases disks and other media as needed upon disposal or in preparation for re-use. Records are maintained for the movements of hardware and electronic media and any person responsible therefore. In addition, the Security Officer (or designated representative) creates a retrievable, exact copy of e-PHI, when needed, before movement of equipment.

C. Technical Safeguards

Our Practice has implemented technical safeguard-related policies and procedures in the following areas to prevent, detect, contain, and correct security violations, as described in the following sections.

1. Access Control

Each employee is assigned a unique name and/or number for identifying and tracking user identities. You must keep your user ID secure and you must not share it with

anyone. Each employee shall have his or her own user ID. User ID's shall be unique to the individual, not to the job function.

In addition, the Practice has set up password protected screen savers to activate when your workstation is idle for extended periods or when you leave your workstation unattended. If your workstation remains idle for sixty (60) minutes or more you will be automatically logged off the system and will need to login again upon your return. As extra protection, if you will be walking away from your system, user should lock computer by pressing Ctrl, Alt, Delete keys simultaneously and selecting Lock Computer.

2. Audit Controls

Our Practice has implemented procedural mechanisms that record and examine activity in information systems that contain or use e-PHI. These mechanisms include failed login reports and account activity reports.

3. Integrity

The Practice has implemented procedures to protect e-PHI from improper alteration or destruction, to corroborate that e-PHI has not been altered or destroyed in an unauthorized manner, and to verify that a person or entity seeking access to e-PHI is the one claimed.

4. Person or Entity Authentication

As outlined above, the Practice has installed measures to verify that anyone trying to access e-PHI is the person that he/she claims to be. Thus, it is of utmost importance that you do not share you access codes with anyone.

5. Transmission Security

You must not transmit e-PHI (via e-mail or otherwise) unless you are directed to do so by your supervisor.

D. Breach

Under the HITECH Act and the Omnibus Rule, our Practice is required to notify affected patients in writing if we believe that a breach, by our Practice or one of our Business Associates, of unsecured PHI compromises the security or privacy of the PHI. Unsecured PHI is PHI that has not been rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of encryption or destruction. To understand what a breach is, it might be helpful to identify what is not a breach. Specifically, the rule carves out three exceptions to the definition of breach:

(1) an unintentional use of PHI by a workforce member or a person acting under the authority of our Practice or our Business Associate acting in good faith and within the scope of his or her authority, and the PHI is not further improperly used and disclosed;

(2) an inadvertent disclosure of PHI by an authorized person to another authorized person (both persons are at our Practice or at the same Business Associate), and the PHI is not further improperly used and disclosed; and

(3) a disclosure of PHI to an unauthorized person where there is a good faith belief that the disclosed PHI could not be retained.

In a nutshell, these exceptions apply to any unintentional or inadvertent acquisition, access, or use of PHI by a workforce member (i.e., someone acting under your authority or that of

a Business Associate), which cannot result in any further prohibited use or disclosure or where the unauthorized person to whom the disclosure of PHI was made would not reasonably be able to retain the disclosed information. If any of these exceptions apply, no breach has occurred and we are not required to notify any patients.

If one of the above exceptions does not apply, any non-permitted acquisition, access, use or disclosure of PHI is presumed to be a breach unless the Practice or our business associate is able to demonstrate that there is a low probability the PHI has been compromised. This determination must be based on a risk assessment that includes at least the following factors:

- The nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

As previously mentioned, all employees have a duty to immediately report any actual or suspected violations of HIPAA of which they become aware. A determination of whether a breach has occurred will be made based on the facts and circumstances of the situation. Our Compliance Personnel will undertake a risk assessment to determine if a breach has occurred. You may be asked to assist in this assessment if you were involved in the breach. A complete checklist of questions to perform the Risk Assessment can be found in Exhibit EE.

If the Compliance Personnel determines that a breach has occurred (no exceptions apply), those affected patients will be notified in writing within sixty (60) days of the date the breach was discovered. A standard Breach Notification Letter is included as Exhibit FF. Due to the sensitive nature of any breach, and so that our Practice may deal with breaches internally without

undue stress to all of our patients, no employee may discuss a potential or actual breach with any other employees, patients, the media, or outside persons, unless directed to do so by Compliance Personnel. Our Breach Notification Policy can be found in Exhibit GG.

Once a year our Practice is required to report to HHS any breaches that occurred at our Practice in the prior year. Employees may be asked by Compliance Personnel to log any breaches discovered by the Practice. See Exhibit HH for our Breach Notification Log.