7.00 HIPAA FORMS INDEX

This index includes information on how to properly complete the forms. If you need more information regarding when to use a particular form, please see the HIPAA Forms Index in the Forms section of your HIPAA Manual.

Many of the forms contain form fields. These are blank fields that may be filled in electronically in order to save you time. Some of the forms will not contain any form fields, and should be printed blank for completion by patients and/or staff members. If you would like to save your entries in the form fields, first save a copy of the file on your computer.

The forms as they are presented in this file cannot be changed beyond completion of form fields. If you would like to make content or layout changes to a form, you may request a file of the forms in Microsoft Word® format. Simply call (800) 777-2337 or email hprochaska@mac.com and request that we email you a compressed file of the forms in Microsoft Word®.

Form # Title

7.10 Confidentiality Statement

Print and distribute this form to each employee for completion.

7.11 Employee Notice of Privacy Practices

Print and distribute this form to employees for completion.

7.12 Vendor Confidentiality Statement

The practice name is called for on the first line of this form. Simply hit the tab key once and enter the practice name.

7.12a Visitor Confidentiality Statement

Print and distribute this form to visitors who will have access to PHI.

7.20 Notice of Privacy Practices

Two formats are provided, a two-page version and a condensed, one-page copy. Each form contains fields for the practice name, the publication and effective dates (they may be the same date), and a line for Privacy Manager contact information.

7.22 Business Associate Agreement

The opening paragraph contains three form fields, the first will contain the name of your practice (Covered Entity), the second the name of your Business Associate, and the third the date of the agreement. Fill in the three form fields, and then move to page five of the document to enter the address of the practice and the Business Associate address. Once printed, a representative of the practice and a representative of the Business Associate must sign the form.

7.22a Business Associate Agreement - Attachment A

Complete this form with the services provided by the Business Associate (i.e., billing services, debt collection, transcription, courier services, document storage, chart copying or microfilming, chart auditing, etc.) and attach to the Business Associate Agreement.

7.30 Patient Authorization for Personal Representative

Enter the Name of the Practice. There is also a line for you to enter the Patient's Name. (The last four digits of the social security number and date of birth should be entered by hand so that this information is not stored in the electronic document). Last, you will want to enter the address where you would like patients to mail their requests to revoke or terminate the authorization.

7.31 Limited Patient Authorization for Disclosure of PHI

Enter the patient's name and complete the practice information in the next section (Entity Requested to Release Information). The patient will complete the remainder of the form.

7.34 Patient Authorization for Disclosure of Protected Health Information via Alternative Means

Enter the name of the practice in the footer. The patient's name may be completed, but the patient should complete the remainder.

7.40 Patient Privacy Complaint Form

Print and distribute this form to a patient upon request.

7.60 Request for Access to PHI

You may tab into the "copy fee" form field to enter the fee that will be charged for copying services. If your practice does not charge a fee, you may enter $0. The patient will complete the remainder of the form.

7.70 Patient Request for Restriction of PHI

You may enter the practice name in the first form field and it will automatically duplicate in the second field. Then print and distribute the form to the patient requesting it for completion.

7.71 Acceptance/Denial of Requested Restriction

Tab into the first field to enter the current date, and tab again to enter the patient's name. The second date field should be completed with the date that the patient request was received by your practice.

7.72 Termination of Patient Restriction

This form may be used by the practice to advise a patient that the restriction of his/her protected health information will be terminated.

7.80 Patient Request for Amendment of PHI

Print and distribute this form to a patient who wishes to amend his/her PHI.

7.81 Acceptance/Denial of Requested Amendment

Tab into the first form field to enter the current date, the second to enter the patient's name, and the third form field to enter the date that the request was made by the patient. There is a check box to indicate acceptance or denial of the request.

7.90 Disclosure Accountability Request

Print and distribute this form to a patient that wishes to request a listing of disclosures of his/her PHI over a specified period of time.

7.91 Privacy Breach Risk Assessment Form (and Guide)

As the form will be completed over time as your investigation unfolds, please print a copy of the form for manual completion. A separate guide is provided with this form to provide explanation of each item requested.

7.92 Sample Privacy Breach Notification Letter

This sample letter may be modified in any word processing program to fit the unique circumstances of the breach.

For assistance, please contact Eagle Associates at (800) 777-2337.

Confidentiality Statement **Form 7.10**

Through your employment activities and duties, you may learn of or have access to employee protected health information and protected health information of patients. Protected health information, for employees and patients, is defined as any information that identifies an individual (patient) and describes their health status, sex, age, ethnicity, or other demographic characteristics, in any format (i.e., electronic, written, or oral). Protected health information is to be maintained in a confidential manner. All protected health information is protected by law and by the privacy policies of this practice. The intent of the laws and policies is to ensure that protected health information remains confidential, and that it is used only to provide for employee or patient care and services. Your duties, obligations and responsibilities with regard to confidentiality are described below in the form of an agreement with this practice. You are required to abide by these duties, obligations and responsibilities. Any violation will subject you to discipline, which may include termination of employment and legal liability from the patient and this practice.

Confidentiality Agreement - I, the undersigned employee, agree to the following:

1. I will use protected health information only as needed to perform my legitimate duties as an employee of this practice. This means, among other things, that:

    - I will only access protected health information necessary for the performance of my duties;
    - I will not in any way divulge, copy, release, sell, loan, review, alter or destroy any confidential information, except as properly authorized by my employer; and
    - I will not misuse or act carelessly with protected health information.

2. I will safeguard and will not disclose information that could provide access to protected health information by persons outside of this practice.

3. I will report activities by any person or entity that I suspect may compromise the confidentiality of protected health information. (Reports made in good faith about suspect activities will be held in confidence to the extent permitted by law, including the name of the individual reporting the activities.)

4. I understand that my obligations for maintaining confidentiality of protected health information maintained by this practice will continue after termination of my employment.

5. I understand that I have no right or ownership interest in any protected health information referred to in this agreement. My employer may at any time revoke my access to confidential information. At all times during my employment, I will safeguard and retain the confidentiality of all protected health information.

6. I will be responsible for any misuse or wrongful disclosure of confidential information and for my failure to safeguard my means of access to confidential information. I understand that my failure to comply with this agreement may result in legal liability and/or my loss of employment.

_____

Employee Name

_____ _____

Employee Signature Date

Employee Notice of Privacy Practices

Form 7.11

This notice describes how employee protected health information (PHI) about you may be used and disclosed, along with how you can get access to this information. Please review it carefully.

Employee protected health information (PHI) has the same definition as patient PHI. In the case of your employment with this organization, employee PHI is information provided to the organization as needed to provide healthcare benefits. Our organization is required to follow specific rules on how we use and/or disclose your employee PHI. This Notice describes how we follow those rules to use and disclose your employee PHI to provide healthcare benefits to you for treatment, payment, to manage our healthcare operations, and for other purposes that are permitted or required by law. It also describes your rights regarding your employee PHI.

We are required to abide by the terms of this Notice of Privacy Practices. We reserve the right to change the terms of our notice, at any time. The new notice will be effective for all protected health information that we maintain at that time. A copy of a revised Notice of Privacy Practices may be obtained by contacting the Privacy Officer. Please contact the Privacy Officer if you have any questions about this notice.

Your Rights Under the Privacy Rule - The following is a statement of your rights, under the Privacy Rule, in reference to your employee PHI. Please feel free to discuss any questions with your supervisor or the Privacy Officer.

1. You have the right to receive a copy of this Notice of Privacy Practices - We are required to follow the terms of this notice. We reserve the right to change the terms of our notice, at any time. If needed, new versions of this notice will be effective for all protected health information that we maintain at that time. Upon your request, we will provide you with a revised Notice.

2. You have the right to inspect and obtain a copy of your employee PHI - This means you may inspect and obtain a copy of employee PHI about you. A written request must be made to the Privacy Officer to inspect your employee PHI.

3. You have the right to authorize other disclosure - This means you have the right to authorize disclosure other than for the purposes of providing healthcare benefits to you for treatment, payment, to manage our healthcare operations and for other purposes that are permitted or required by law. You may revoke an authorization, at any time, in writing, except to the extent that the organization has taken an action in reliance on the use or disclosure indicated in the authorization.

4. You may have the right to request an amendment your employee PHI - This means you may request an amendment of employee PHI about you for as long as we maintain this information. In certain cases, we may deny your request for an amendment. If we deny your request, we will provide you with a copy of any such denial.

5. You have the right to request a disclosure accountability - This means that you may request a listing of your employee PHI disclosures we have made to entities or persons outside of our organization. It excludes disclosures we may have made directly to you, disclosures for the purposes of providing healthcare benefits to you for treatment, payment, to manage our healthcare operations and for other purposes that are permitted or required by law, or for authorizations requested by you.

How We May Use or Disclose Protected Health Information - This organization may use and disclose your employee PHI to provide healthcare benefits for you, for treatment and payment of healthcare benefits, to manage our healthcare operations, and for other purposes that are permitted or required by law.

Questions or Complaints – Any questions or complaints regarding the organization's use or disclosure of your employee PHI can be made in writing to the Privacy Officer.

Acknowledgement of Receipt I acknowledge receipt of the organization's "Employee Notice of Privacy Practices."

_____

Print Name

_____ _____

Signature Date

Vendor Confidentiality Statement

Form 7.12

_____

Practice Name

Through your activities and service provided to our office, you and/or your staff may have access to protected health information. Protected health information is defined as any information that identifies an individual (patient) and describes their health status, sex, age, ethnicity, or other demographic characteristics in any format (i.e., electronic, written, or oral). The protected health information of our patients is to be maintained in a confidential manner. All protected health information is protected by federal law and by the privacy policies of this practice. The intent of the laws and policies is to assure that protected health information remains confidential, and that it is used only to provide for patient care and services. Your duties, obligations and responsibilities with regard to confidentiality are described below in the form of an agreement with this practice. We require you and your staff to agree to and abide by the terms of this agreement. Any violation may subject you and your staff to discipline, which may include termination of our vendor agreement and legal liability from the patient and this practice.

Confidentiality Agreement - I, the undersigned agent for our company, agree to the following on behalf of our company and staff that may have access to your office as a result of the service we provide:

1. Our company and staff will safeguard and will not disclose information that could provide access to protected health information by persons outside of our company.
2. Our company and/or staff will report activities by any person or entity that we suspect may compromise the confidentiality of protected health information. (Reports made in good faith about suspect activities will be held in confidence to the extent permitted by law, including the name of the individual reporting the activities.)
3. Our company and staff acknowledge that we will be responsible for any misuse or wrongful disclosure of confidential information and for any failure, on our part, to safeguard our means of access to confidential information. Our company and staff understand that failure to comply with this agreement may also result in termination of our vendor agreement and legal liability.

_____

company name

_____

name of authorized agent (please print)

_____ _____

authorized agent's signature date

If you have questions regarding this statement or agreement, please contact our Privacy Manager.

Visitor Confidentiality Statement

Form 7.12a

Through your activities and association with our office, you may have access to protected health information (PHI) and electronic protected health information (EPHI). PHI is defined as any information that identifies an individual (patient) and describes their health status, sex, age, ethnicity, or other demographic characteristics in any format (i.e., electronic, written, or oral). EPHI is the same information but in an electronic format. The information of our patients is to be maintained in a confidential manner. All PHI and EPHI is protected by federal law and by the privacy policies of this practice. The intent of the laws and policies is to assure that PHI and EPHI remain confidential, and that it is used only to provide for patient care and services. Your duties, obligations and responsibilities with regard to confidentiality are described below in the form of an agreement with this practice. As a visitor who has authorized access to our PHI and EPHI we require you agree to and abide by the terms of this agreement. Any violation may subject you to discipline, which may include termination of our association and legal liability from the patient and this practice.

Confidentiality Agreement – I agree to the following requirements for safeguarding of the practice's PHI and EPHI:

1. I will safeguard and will not disclose information that could provide access to protected health information by persons outside of the practice.
2. I will report activities by any person or entity that I suspect may compromise the confidentiality of PHI or EPHI. (Reports made in good faith about suspect activities will be held in confidence to the extent permitted by law, including the name of the individual reporting the activities).
3. I will be responsible for any misuse or wrongful disclosure of confidential information and for any failure, on my part, to safeguard my means of access to confidential information. I understand that failure to comply with this agreement may also result in termination of my association with the practice and legal liability.

_____

name of individual

_____ _____

signature date

This notice describes how medical information about you may be used and disclosed, and how you can gain access to this information. Please review it carefully.

Protected health information (PHI), about you, is maintained as a written and/or electronic record of your contacts or visits for healthcare services with our practice. Specifically, PHI is information about you, including demographic information (i.e., name, address, phone, etc.), that may identify you and relates to your past, present or future physical or mental health condition and related healthcare services.

Our practice is required to follow specific rules on maintaining the confidentiality of your PHI, using your information, and disclosing or sharing this information with other healthcare professionals involved in your care and treatment. This Notice describes your rights to access and control your PHI. It also describes how we follow applicable rules and use and disclose your PHI to provide your treatment, obtain payment for services you receive, manage our healthcare operations and for other purposes that are permitted or required by law.

Your Rights Under The Privacy Rule

Following is a statement of your rights, under the Privacy Rule, in reference to your PHI. Please feel free to discuss any questions with our staff.

You have the right to receive, and we are required to provide you with, a copy of this Notice of Privacy Practices - We are required to follow the terms of this notice. We reserve the right to change the terms of our notice, at any time. Upon your request, we will provide you with a revised Notice of Privacy Practices if you call our office and request that a revised copy be sent to you in the mail or ask for one at the time of your next appointment. The Notice will also be posted in a conspicuous location within the practice, and if such is maintained by the practice, on it's web site.

You have the right to authorize other use and disclosure - This means you have the right to authorize any use or disclosure of PHI that is not specified within this notice. For example, we would need your written authorization to use or disclose your PHI for marketing purposes, for most uses or disclosures of psychotherapy notes, or if we intended to sell your PHI. You may revoke an authorization, at any time, in writing, except to the extent that your healthcare provider, or our practice has taken an action in reliance on the use or disclosure indicated in the authorization.

You have the right to request an alternative means of confidential communication – This means you have the right to ask us to contact you about medical matters using an alternative method (i.e., email, telephone), and to a destination (i.e., cell phone number, alternative address, etc.) designated by you. You must inform us in writing, using a form provided by our practice, how you wish to be contacted if other than the address/phone number that we have on file. We will follow all reasonable requests.

You have the right to inspect and copy your PHI - This means you may inspect, and obtain a copy of your complete health record. If your health record is maintained electronically, you will also have the right to request a copy in electronic format. We have the right to charge a reasonable fee for paper or electronic copies as established by professional, state, or federal guidelines.

You have the right to request a restriction of your PHI - This means you may ask us, in writing, not to use or disclose any part of your protected health information for the purposes of treatment, payment or healthcare operations. If we agree to the requested restriction, we will abide by it, except in emergency circumstances when the information is needed for your treatment. In certain cases, we may deny your request for a restriction. You will have the right to request, in writing, that we restrict communication to your health plan regarding a specific treatment or service that you, or someone on your behalf, has paid for in full, out-of-pocket. We are not permitted to deny this specific type of requested restriction.

You may have the right to request an amendment to your protected health information - This means you may request an amendment of your PHI for as long as we maintain this information. In certain cases, we may deny your request.

You have the right to request a disclosure accountability - This means that you may request a listing of disclosures that we have made, of your PHI, to entities or persons outside of our office.

You have the right to receive a privacy breach notice - You have the right to receive written notification if the practice discovers a breach of your unsecured PHI, and determines through a risk assessment that notification is required.

If you have questions regarding your privacy rights, please feel free to contact our Privacy Manager. Contact information is provided on the following page under Privacy Complaints.

How We May Use or Disclose Protected Health Information

Following are examples of uses and disclosures of your protected health information that we are permitted to make. These examples are not meant to be exhaustive, but to describe possible types of uses and disclosures.

Treatment - We may use and disclose your PHI to provide, coordinate, or manage your healthcare and any related services. This includes the coordination or management of your healthcare with a third party that is involved in your care and treatment. For example, we would disclose your PHI, as necessary, to a pharmacy that would fill your prescriptions. We will also disclose PHI to other Healthcare Providers who may be involved in your care and treatment.

Special Notices - We may use or disclose your PHI, as necessary, to contact you to remind you of your appointment. We may contact you by phone or other means to provide results from exams or tests and to provide information that describes or recommends treatment alternatives regarding your care. Also, we may contact you to provide information about health-related benefits and services offered by our office, for fund-raising activities, or with respect to a group health plan, to disclose information to the health plan sponsor. You will have the right to opt out of such special notices, and each such notice will include instructions for opting out.

Payment - Your PHI will be used, as needed, to obtain payment for your healthcare services. This may include certain activities that your health insurance plan may undertake before it approves or pays for the healthcare services we recommend for you such as, making a determination of eligibility or coverage for insurance benefits.

Healthcare Operations - We may use or disclose, as needed, your PHI in order to support the business activities of our practice. This includes, but is not limited to business planning and development, quality assessment and improvement, medical review, legal services, auditing functions and patient safety activities.

Health Information Organization - The practice may elect to use a health information organization, or other such organization to facilitate the electronic exchange of information for the purposes of treatment, payment, or healthcare operations.

To Others Involved in Your Healthcare - Unless you object, we may disclose to a member of your family, a relative, a close friend or any other person, that you identify, your PHI that directly relates to that person's involvement in your healthcare. If you are unable to agree or object to such a disclosure, we may disclose such information as necessary if we determine that it is in your best interest based on our professional judgment. We may use or disclose PHI to notify or assist in notifying a family member, personal representative or any other person that is responsible for your care, of your general condition or death. If you are not present or able to agree or object to the use or disclosure of the PHI, then your healthcare provider may, using professional judgment, determine whether the disclosure is in your best interest. In this case, only the PHI that is necessary will be disclosed.

Other Permitted and Required Uses and Disclosures - We are also permitted to use or disclose your PHI without your written authorization for the following purposes: as required by law; for public health activities; health oversight activities; in cases of abuse or neglect; to comply with Food and Drug Administration requirements; research purposes; legal proceedings; law enforcement purposes; coroners; funeral directors; organ donation; criminal activity; military activity; national security; worker's compensation; when an inmate in a correctional facility; and if requested by the Department of Health and Human Services in order to investigate or determine our compliance with the requirements of the Privacy Rule.

Privacy Complaints

You have the right to complain to us, or directly to the Secretary of the Department of Health and Human Services if you believe your privacy rights have been violated by us. You may file a complaint with us by notifying the Privacy Manager at:

_____

We will not retaliate against you for filing a complaint.

Effective Date _____ Publication Date _____

Notice of Privacy Practices

This notice describes how medical information about you may be used and disclosed, and how you can gain access to this information. Please review it carefully.

Protected health information (PHI), about you, is maintained as a written and/or electronic record of your contacts or visits for healthcare services with our practice. Specifically, PHI is information about you, including demographic information (i.e., name, address, phone, etc.), that may identify you and relates to your past, present or future physical or mental health condition and related healthcare services.

Our practice is required to follow specific rules on maintaining the confidentiality of your PHI, using your information, and disclosing or sharing this information with other healthcare professionals involved in your care and treatment. This Notice describes your rights to access and control your PHI. It also describes how we follow applicable rules and use and disclose your PHI to provide your treatment, obtain payment for services you receive, manage our healthcare operations and for other purposes that are permitted or required by law.

Your Rights Under The Privacy Rule

Following is a statement of your rights, under the Privacy Rule, in reference to your PHI. Please feel free to discuss any questions with our staff.

You have the right to receive, and we are required to provide you with, a copy of this Notice of Privacy Practices - We are required to follow the terms of this notice. We reserve the right to change the terms of our notice, at any time. Upon your request, we will provide you with a revised Notice of Privacy Practices if you call our office and request that a revised copy be sent to you in the mail or ask for one at the time of your next appointment. The Notice will also be posted in a conspicuous location within the practice, and if such is maintained by the practice, on it's web site.

You have the right to authorize other use and disclosure - This means you have the right to authorize any use or disclosure of PHI that is not specified within this notice. For example, we would need your written authorization to use or disclose your PHI for marketing purposes, for most uses or disclosures of psychotherapy notes, or if we intended to sell your PHI. You may revoke an authorization, at any time, in writing, except to the extent that your healthcare provider, or our practice has taken an action in reliance on the use or disclosure indicated in the authorization.

You have the right to request an alternative means of confidential communication – This means you have the right to ask us to contact you about medical matters using an alternative method (i.e., email, telephone), and to a destination (i.e., cell phone number, alternative address, etc.) designated by you. You must inform us in writing, using a form provided by our practice, how you wish to be contacted if other than the address/phone number that we have on file. We will follow all reasonable requests.

You have the right to inspect and copy your PHI - This means you may inspect, and obtain a copy of your complete health record. If your health record is maintained electronically, you will also have the right to request a copy in electronic format. We have the right to charge a reasonable fee for paper or electronic copies as established by professional, state, or federal guidelines.

You have the right to request a restriction of your PHI - This means you may ask us, in writing, not to use or disclose any part of your protected health information for the purposes of treatment, payment or healthcare operations. If we agree to the requested restriction, we will abide by it, except in emergency circumstances when the information is needed for your treatment. In certain cases, we may deny your request for a restriction. You will have the right to request, in writing, that we restrict communication to your health plan regarding a specific treatment or service that you, or someone on your behalf, has paid for in full, out-of-pocket. We are not permitted to deny this specific type of requested restriction.

You may have the right to request an amendment to your protected health information - This means you may request an amendment of your PHI for as long as we maintain this information. In certain cases, we may deny your request for an amendment.

You have the right to request a disclosure accountability - This means that you may request a listing of disclosures that we have made, of your PHI, to entities or persons outside of our office.

You have the right to receive a privacy breach notice - You have the right to receive written notification if the practice discovers a breach of your unsecured PHI, and determines through a risk assessment that notification is required.

If you have questions regarding your privacy rights, please feel free to contact our Privacy Manager. Contact information is provided at right, under Privacy Complaints.

How We May Use or Disclose Protected Health Information

Following are examples of uses and disclosures of your protected health information that we are permitted to make. These examples are not meant to be exhaustive, but to describe possible types of uses and disclosures.

Treatment - We may use and disclose your PHI to provide, coordinate, or manage your healthcare and any related services. This includes the coordination or management of your healthcare with a third party that is involved in your care and treatment. For example, we would disclose your PHI, as necessary, to a pharmacy that would fill your prescriptions. We will also disclose PHI to other Healthcare Providers who may be involved in your care and treatment.

Special Notices - We may use or disclose your PHI, as necessary, to contact you to remind you of your appointment. We may contact you by phone or other means to provide results from exams or tests and to provide information that describes or recommends treatment alternatives regarding your care. Also, we may contact you to provide information about health-related benefits and services offered by our office, for fund-raising activities, or with respect to a group health plan, to disclose information to the health plan sponsor. You will have the right to opt out of such special notices, and each such notice will include instructions for opting out.

Payment - Your PHI will be used, as needed, to obtain payment for your healthcare services. This may include certain activities that your health insurance plan may undertake before it approves or pays for the healthcare services we recommend for you such as, making a determination of eligibility or coverage for insurance benefits.

Healthcare Operations - We may use or disclose, as needed, your PHI in order to support the business activities of our practice. This includes, but is not limited to business planning and development, quality assessment and improvement, medical review, legal services, auditing functions and patient safety activities.

Health Information Organization - The practice may elect to use a health information organization, or other such organization to facilitate the electronic exchange of information for the purposes of treatment, payment, or healthcare operations.

To Others Involved in Your Healthcare - Unless you object, we may disclose to a member of your family, a relative, a close friend or any other person, that you identify, your PHI that directly relates to that person's involvement in your healthcare. If you are unable to agree or object to such a disclosure, we may disclose such information as necessary if we determine that it is in your best interest based on our professional judgment. We may use or disclose PHI to notify or assist in notifying a family member, personal representative or any other person that is responsible for your care, of your general condition or death. If you are not present or able to agree or object to the use or disclosure of the PHI, then your healthcare provider may, using professional judgment, determine whether the disclosure is in your best interest. In this case, only the PHI that is necessary will be disclosed.

Other Permitted and Required Uses and Disclosures - We are also permitted to use or disclose your PHI without your written authorization for the following purposes: as required by law; for public health activities; health oversight activities; in cases of abuse or neglect; to comply with Food and Drug Administration requirements; research purposes; legal proceedings; law enforcement purposes; coroners; funeral directors; organ donation; criminal activity; military activity; national security; worker's compensation; when an inmate in a correctional facility; and if requested by the Department of Health and Human Services in order to investigate or determine our compliance with the requirements of the Privacy Rule.

Privacy Complaints

You have the right to complain to us, or directly to the Secretary of the Department of Health and Human Services if you believe your privacy rights have been violated by us. You may file a complaint with us by notifying the Privacy Manager at:

_____

We will not retaliate against you for filing a complaint.

Effective Date _____ Publication Date _____

Business Associate Agreement for Privacy and Security **Form 7.22**

This Business Associates Agreement ("Agreement") is entered into between

_____ (hereafter "Covered Entity") and

_____ (hereafter "Business Associate") and

shall be effective as of _____ ("Effective Date").

The purpose of this Agreement is to comply with HIPAA's Privacy, Security and Enforcement (Final) Rules, as published by the Secretary of the U. S. Department of Health and Human Services (DHHS). This Agreement defines the parties' rights and responsibilities under HIPAA for the exchange of PHI (Protected Health Information) and EPHI (Electronic Protected Health Information) as defined in this Agreement and establishes that the Business Associate desires to provide satisfactory assurances required by the Privacy Standards.

This Agreement sets forth the terms and conditions that govern the use and disclosure of Protected Health Information which is provided to the Business Associate by the Covered Entity.

1. Business Associate Services

The Business Associate provides services for the Covered Entity that involve the use and disclosure of Protected Health Information. The specific services provided by the Business Associate are described in Attachment A of this Agreement.

2. Definitions

PHI – Protected Health Information (PHI) is defined, under the Privacy Standards, as any information that identifies an individual and describes their health status, sex, age, ethnicity, or other demographic characteristics, whether or not that information is stored or transmitted electronically. PHI includes oral, written, and electronic information.

EPHI – Electronic Protected health Information (EPHI) is defined as PHI that is stored or transmitted electronically.

Security Incident – A security incident is defined as an attempted or successful unauthorized access, use, disclosure, modification or destruction of EPHI.

3. Description of Permitted Uses and Disclosures

In order for Business Associate to provide its services to Covered Entity in accordance with this Agreement, Covered Entity intends to disclose Protected Health Information to Business Associate and expects Business Associate to use the Protected Health Information to perform its services under this Agreement such as:

(a) Use of the Protected Health Information in its possession for its proper management and administration and to fulfill any present or future legal responsibilities of Business Associate provided that such uses are permitted under state and federal confidentiality laws; and

(b) Disclosure of the Protected Health Information in its possession to third parties for the purposes of proper management and administration or to fulfill any present or future legal

responsibilities of Business Associate provided that (i) such uses are permitted under state and federal confidentiality laws or; (ii) Business Associate has received third party written assurances regarding its confidential handling of such Protected Health Information as required by Privacy Standards, and

(c) Aggregation of the Protected Health Information with the protected health information of other covered entities that Business Associate has in its possession through its capacity to provide its services to other covered entities, provided that the purpose of such aggregation is to provide covered entities with data analyses relating to their healthcare operations. Under no circumstances may Business Associate disclose Protected Health Information of Covered Entity to another covered entity absent the explicit authorization of Covered Entity, and

(d) De-identification of Protected Health Information provided that the de-identification conforms to the requirements of Privacy Standards and further provided that Covered Entity is sent the documentation required by Privacy Standards that shall be in the form of a written assurance from Business Associate. Pursuant to Privacy Standards, de-identified information does not constitute Protected Health Information and is not subject to the terms of this Agreement.

4. Responsibilities of Business Associates

The Business Associate agrees to comply with all applicable requirements of HIPAA's Privacy and Security Rules, HITECH Act and 2013 Omnibus Rule.

With regard to its use and disclosure of Protected Health Information, the Business Associate agrees to do the following:

(a) Use and/or disclose the Protected Health Information only as permitted or required by this Agreement or as otherwise required by law;

(b) Report to the designated privacy officer of the Covered Entity, by fax or electronic mail, any use or disclosure or security incident with PHI (electronic or other format) that is not permitted or required by the Privacy Rule or this agreement. Notification by the business associate to the covered entity must be made as soon as possible but not more than 60 calendar days from the discovery of a breach by the business associate."

Information regarding a breach shall include (if available):

- A brief description of what happened, including the date of the breach (if known) and the date of discovery of the breach;

- A description of the types of unsecured PHI that were involved in the breach (i.e., full name, social security number, date of birth, home address, account number, diagnosis, disability code, and other types of PHI). Note – only the <u>types</u> of PHI will be listed, not the actual individual's information;

- Any steps an individual should take to protect themselves from potential harm resulting from the breach (i.e., recommendations for an individual to contact credit bureaus, and how to make contact if credit card information was involved);

- A brief description of what the Business Associate is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches, including the imposition of employee sanctions, if appropriate; and

- Business Associate contact information for the practice's Compliance Officer to ask questions or learn additional information.

- Required breach notifications will be sent to affected individuals by the Covered Entity.

(c) Use commercially reasonable efforts to maintain the security of PHI and to prevent unauthorized use and/or disclosure of such information, including the implementation of administrative, physical and technical safeguards to protect EPHI, and must require subcontractors to implement reasonable and appropriate safeguards to protect EPHI;

(d) Require all of its employees, representatives, subcontractors or agents that receive or use or have access to PHI under this Agreement to agree in writing to adhere to the same terms and conditions on the use and/or disclosure of PHI that apply herein, including the obligation to return or destroy the Protected Health Information as provided under (h) of this section.

(e) Make available all records, books, agreements, policies and procedures relating to the use and/or disclosure of PHI to the Secretary of DHHS for purposes of determining the Covered Entity's compliance with the Privacy and Security Standards, subject to attorney-client and other applicable legal privileges.

(f) Upon written request, make available during normal business hours at Business Associate's offices all records, books, agreements, policies and procedures relating to the use and/or disclosure of PHI to the Covered Entity within ten (10) days, for purposes of enabling the Covered Entity to determine the Business Associate's compliance with the terms of this Agreement;

(g) Upon written request, provide PHI in accordance with the individual's right to access, inspect, and copy their health information. This means the Covered Entity's patients shall continue to have the right to inspect and/or obtain copies of their PHI maintained by the Business Associate.

(h) Within forty five (45) days of receiving a written request from the Covered Entity, provide to the Covered Entity such information, as is requested by the Covered Entity, to permit the Covered Entity to respond to a request by the subject individual for amendment and accounting purposes of the disclosures of the individual's PHI;

(i) Return to the Covered Entity or destroy, as requested by the Covered Entity, within fifteen (15) days of the termination of this Agreement, the PHI in Business Associate's possession and retain no copies or back-up tapes. If this isn't possible, then the Business Associate must agree to limit disclosures of protected information beyond the termination of the contract.

5. Responsibilities of Covered Entity

With regard to the use and/or disclosure of PHI by the Business Associate, the Covered Entity hereby agrees:

(a) To inform the Business Associate of any changes in the form of notice of privacy practices that the Covered Entity provides to individuals and provide the Business Associate a copy of the notice currently in use; and

(b) To notify the Business Associate, in writing and in a timely manner, of any restrictions on the use and/or disclosure of Protected Health Information agreed to by the Covered Entity.

6. Mutual Representation and Warranty

Each party represents and warrants to the other party that all of its employees, agents, representatives and members of its work force, whose services may be used to fulfill obligations under this Agreement, are or shall be appropriately informed of the terms of this Agreement and are under legal obligation to fully comply with all provisions of this Agreement.

7. Term and Termination

(a) This Agreement shall become effective on the Effective Date and shall continue in effect until all obligations of the parties have been met, unless terminated as provided herein or by mutual agreement of the parties.

(b) As provided for under the Privacy and Security Standards, the Covered Entity may immediately terminate this Agreement and any related agreement if it determines that the Business Associate has breached a material provision of this Agreement, including, without limitation, the confidentiality and privacy provisions of the contract. Alternatively, the Covered Entity may choose to: (i) provide the Business Associate with ten (10) days written notice of the existence of an alleged material breach; and (ii) afford the Business Associate an opportunity to cure said alleged material breach upon mutually agreeable terms. Failure to cure the alleged material breach in the manner set forth in this paragraph is grounds for the immediate termination of the Agreement. If termination is not feasible, the Covered Entity shall report the breach to the Secretary of DHHS. This Agreement will automatically terminate without any further action of the parties upon the termination or expiration of the Service Agreement.

(c) This Agreement shall have an automatic renewal on the anniversary of the Effective Date with both parties having the option to terminate the Agreement without reason by providing the other party with a written notice of such termination at least thirty (30) days prior to the anniversary of the Effective Date.

The respective rights and obligations of Business Associate and Covered Entity under the provisions of sections 4(i) and 8 shall survive the termination of this Agreement indefinitely.

8. Modification and Amendment

This Agreement may not be modified or amended, except in writing as agreed to by each party.

9. Third Part Beneficiaries

Nothing express or implied in this Agreement is intended to confer, nor anything herein shall confer, upon any person or entity, other than the Covered Entity and Business Associate, any rights, remedies, obligations, or liabilities whatsoever.

10. Notices

Any notices to be given hereunder shall be made via U.S. mail or express courier, or hand delivery to the other party's address given below as follows:

If to Business Associate:

If to Covered Entity:

IN WITNESS WHEREOF, the parties hereby set their hands and seals on the day and date first written above:

_____	_____
Covered Entity	Business Associate
By: _____	By: _____
Authorized Representative	Authorized Representative

Business Associate Agreement - Attachment A

Form 7.22a

The Business Associate provides services for the Covered Entity that involve the use and disclosure of Protected Health Information. The specific services provided by the Business Associate are described as:

Patient Instructions for Form 7.30 - Patient Authorization for a Personal Representative

Your authorization for a Personal Representative will give our office the authority to provide access and other rights to your health information for the person you have designated to be your Personal Representative. If you wish to designate a Personal Representative, Form 7.30 must be completed and signed by you, and will be maintained as part of your medical record.

Your Personal Representative will have all of the rights to your health information that you have under the Privacy Rule. This means that your Personal Representative will have the right to access and review your health information, the right to appoint more Personal Representatives, the right to request restrictions and amendments to your health information, and the right to obtain an accounting of disclosures we have made regarding your health information.

A Personal Representative does **not** have the authority to make healthcare decisions on your behalf.

The following outline will help to explain what information we will need on the form and its purpose. Please address any questions with our staff.

Name of Practice - List the name of our practice if it is not already on the form.

Patient Name - Print your name.

Social Security Number and Date of Birth - This information is needed for identity verification and will be maintained in a confidential manner at all times.

Purpose of Request - You must print the name of the person that you want to be your Personal Representative, along with his/her phone number and address so that we may contact him/her if necessary.

Description of Information to be Disclosed - A Personal Representative has the right to access and be informed of all of your health information. Should you wish to limit the information to which he/she will have access, we will instead provide you with a "Limited Patient Authorization" form for your use.

Expiration or Termination - This authorization will remain in effect until you or your Personal Representative, or someone with legal authority, chooses to request termination of the authorization.

Right to Revoke or Terminate - You may revoke or terminate this authorization at any time by contacting our Privacy Manager. Requests for revocation or termination must be made in writing.

Redisclosure Statement - We cannot be responsible for what your Personal Representative does with your health information that we would provide under this authorization. The redisclosure statement simply informs you of this situation.

Signature and Date - We will need your signature and date of the signature to make the authorization effective.

Copies - We will provide you with a copy of this signed authorization upon request.

Patient Authorization for Personal Representative

Form 7.30

Please print all information, then sign and date form at bottom.

Name of Practice: _____

Patient Name: _____

Social Security Number: _____ **Date of Birth:** _____

Purpose of request: I authorize the practice to disclose or provide my protected health information to the following individual who is authorized to act as my personal representative for the purposes of receiving all protected health information about myself. As my designated personal representative, he/she may exercise my right to inspect, copy, and request amendments to my protected health information. He/she may also consent or authorize the use or disclosure of my protected health information:

_____

Name of Personal Representative Phone

_____

Address

_____

City, State, Zip

- **Description of information to be disclosed:** I authorize the practice to disclose all of my protected health information to my designated personal representative.
- **Expirations or termination of authorization:** This authorization will remain in effect until terminated by you, your personal representative or another individual(s) of legal entity authorized to do so by court order or law.
- **Right to revoke or terminate:** As stated in our Notice of Privacy Practices, you have the right to revoke or terminate this authorization by submitting a written request to our Privacy Manager. This can be done in-person or by mailing a request to:

  _____

  _____

  _____

  Attn: Privacy Manager.

Redisclosure: We have no control over the person(s) you have listed as your personal representative. Therefore, your protected health information disclosed under this authorization, will no longer be protected by the requirements of the Privacy Rule and will no longer be the responsibility of this practice.

_____ _____

patient signature date

Copies of signed authorizations are available upon request.

Patient Instructions for Form 7.31

Limited Patient Authorization for Disclosure of Protected Health Information

The Limited Patient Authorization will give our office the authority to provide the person or entity you designate on the form with access to your protected health information (PHI). The Limited Patient Authorization is limited to accessing only the information that you designate and does not give any other rights to the person you have named on the form. Use of this form will enable us to provide your health information to a person or entity that may be involved in your healthcare.

The following outline will describe the information we will need on the form and its purpose. Please address any questions you have with our staff.

Patient Name - Print your name.

Social Security Number and Date of Birth - This information is needed for identity verification and will be maintained in a confidential manner at all times.

Entity Requested to Release information - This simply identifies who is to provide the information.

Purpose of Request- To disclose your protected health information to an individual.

Who will be authorized to receive information – Enter the name, address and phone number of the individual or entity that you are designating to receive the disclosure.

Description of Information to be disclosed - The type and amount of health information that we disclose is determined by you. We can disclose or provide access to all of your health information, or it can be limited to a specific item.

Purpose of Disclosure - Regulations require that we identify the purpose for disclosing limited information. You also have the right to keep the purpose to yourself by selecting "Patient Request."

Expiration or Termination - This authorization will expire at the end of the calendar year in which it was signed unless you specify an earlier termination. The authorization must be renewed each year as a means of protecting your information by verifying your wish to continue the authorization for disclosure.

Right to Revoke or Terminate - You may revoke or terminate the authorization at any time by submitting written notice to our Privacy Manager.

Non-Conditioning Statement - This simply states that our practice does not place conditions for treatment on the use of the authorization.

Redisclosure Statement - We cannot be responsible for what the receiving entity does with your health information that we provide under this authorization. The redisclosure statement simply informs you of this situation.

Signature and Date - We will need your signature and date of the signature to make the authorization effective.

Copies - We will provide you with a copy of this signed authorization upon request.

Limited Patient Authorization for Disclosure of Protected Health Information

Form 7.31

Please print all information. Form must be signed and dated each year.

Patient Name: _____

SSN (last four digits): _____ **Date of Birth:** _____

Entity Requested to Release Information:

Purpose of request (who will be authorized to receive information) - I authorize the entity identified above to disclose or provide protected health information, about me to the individual(s) listed below.

Who will be authorized to receive information (list the individual/entity who is to receive your PHI)**:**

Individual/Entity Name: _____

Address: _____

Phone: _____

Description of information to be disclosed - I authorize the practice to disclose the following protected health information about me to the entity, person, or persons identified above:

☐ Entire patient record; **or**, check **only** those items of the record to be disclosed:

- ☐ office notes
- ☐ lab results, pathology reports
- ☐ x-rays;
- ☐ financial history report (previous 3 years only).
- ☐ nursing home, home health, hospice, and other physician records
- ☐ record of HIV and communicable disease testing
- ☐ record of mental health or substance abuse treatment
- ☐ Only send the following: _____

Purpose of disclosure (please record the purpose of the disclosure or check patient request):

☐ Patient Request ☐ Other (please specify): _____

- This authorization will expire at the end of the calendar year of your last signature below, unless you specify an earlier termination. You must renew or submit a new authorization after the expiration date to continue the authorization. Please list the date of expiration if earlier than the end of the calendar year: _____
- You have the right to terminate this authorization at any time by submitting a written request to our Privacy Manager. Termination of this authorization will be effective upon written notice, except where a disclosure has already been made based on prior authorization.
- The practice places no condition to sign this authorization on the delivery of healthcare or treatment.
- We have no control over the person(s) you have listed to receive your protected health information. Therefore, your protected health information disclosed under this authorization may no longer be protected by the requirements of the Privacy Rule, and will no longer be the responsibility of the practice.

_____ _____

patient or representative signature date

_____ _____

patient or representative signature date

_____ _____

patient or representative signature date

_____ _____

patient or representative signature date

You have the right to receive a copy of signed authorizations upon request.

Patient Authorization for Disclosure of Protected Health Information via Alternative Means

Form 7.34

Please print all information, then sign and date authorization form at bottom.

Patient Name: _____ **Date of Birth:** _____

Purpose of Authorization – It is the policy of this practice to provide communication with patients, as stated in our Notice of Privacy Practices, "*by phone or other means designated by you to provide results from exams and tests and to provide information that describes or recommends alternatives regarding your care*." The practice requires the following authorization for release of protected health information via alternative means (other than to the primary home phone number that you have provided).

I authorize the practice to disclose or provide protected health information (as described below) directly to me at the email address, fax number, phone number, cell phone number or alternative address that I have indicated below. I understand that it is my responsibility to notify the practice of any change in this manner of communication and that any disclosure made to the designated address or number, indicated by me, is subject to the redisclosure statement within this authorization.

☐ cell phone: ☐ email address: ☐ US Mail: ☐ fax number: ☐ phone:

_____

Description of information to be disclosed - I authorize the practice to disclose the following protected health information about me *(please provide a written description of the information to be disclosed, such as results of exams, laboratory tests, procedures, and other healthcare services)*:

_____

_____

Purpose of disclosure – I am authorizing the alternative means of communication for disclosure of my protected health information to ensure the confidentiality of communications from the practice.

Expirations or termination of authorization – This authorization will renew automatically, unless I specify an earlier termination. If I specify an expiration date, I understand that I must submit a new authorization to continue the authorization after that date.

(Please list desired expiration date):_____

Right to revoke or terminate: As stated in the practice's Notice of Privacy Practices, I have the right to revoke or terminate this authorization at any time. This can be done in-person or by mailing a written request to the practice, Attn: Privacy Manager.

Non-Conditioning statement: The practice places no condition to sign this authorization on its' delivery of healthcare or treatment.

Redisclosure Statement – I understand that the practice has no control regarding persons who may have access to the mailing address, email address, telephone, cell or fax number I have designated to receive my protected health information. Therefore, I understand that my protected health information disclosed under this authorization will no longer be the responsibility of this practice.

_____ _____

patient signature date

Copies of signed authorizations are available upon request.

Patient Privacy Complaint Form

Form 7.40

This form is provided so that we may address your concerns with the privacy policies and procedures of our practice. We will mail a response to your complaint within five (5) working days. Please print and complete the following information (attach additional pages as necessary):

Date: _____

Patient Name: _____

Mailing Address (where a response should be sent)**:**

_____

_____

_____

Privacy Compliant – please specify your concerns with our privacy policies/procedures:

_____

_____

_____

_____

Response: A response was provided on _____

_____

_____

_____

_____

_____

Request for Access to Protected Health Information

Form 7.60

Under the Privacy Rule, a patient or his/her personal representative may request access to the patient's protected health information for the purposes of inspection and/or obtaining a copy of the protected health information. There are conditions under which a healthcare provider may deny access to protected health information. Under such conditions, there is no opportunity or requirement to have the denial of access reviewed. These conditions include:

1. Psychotherapy notes;
2. Information intended for use in a civil, criminal, or administrative actions;
3. When an individual (patient) is an inmate in a correctional facility or the healthcare provider is acting under the direction of correctional facility, where providing access to information would endanger other inmates or correctional employees;
4. When an individual (patient) has consented to the withholding of information as a subject in a research program that is still in progress;
5. When the Privacy Rule denies access; and
6. When the healthcare provider obtained the protected health information under a promise of confidentiality, and access to the information would reveal the source of the information.

There are three conditions under which a healthcare provider may deny access to protected health information but, if they do, must provide the individual (patient) or his/her personal representative an opportunity to have the denial reviewed. These conditions include:

1. When the healthcare provider has determined that access to the protected health information is likely to endanger the life or physical safety of the individual (patient) or another person;
2. When the information identifies another person, and the healthcare provider believes that access will cause harm to the other person; and
3. When the information is requested by a personal representative of an individual (patient) and, in the judgment of the healthcare provider, providing access to the information might subject the individual (patient) to domestic violence, abuse, or neglect by the personal representative.

Access (inspection and/or obtaining copies) to protected health information is provided on a scheduled basis. Our receptionist can provide the schedule information for you at the time of your request. Additionally, we will charge a reasonable fee for any copies of protected health information. Our copy fee is $_____. Please note that, due to privacy and risk management guidelines, original documents of protected health information may only be inspected in the presence of one of our staff members and original materials may not be removed from the facility.

_____

patient name

_____ _____

patient signature date

Please specify the format in which you would like the PHI provided to you. We will accommodate your request, if possible.

- ❑ paper copy
- ❑ electronic copy – preferred format: _____

Patient Request for Restriction of Protected Health Information

Form 7.70

I, the undersigned, am requesting a restriction on the use and/or disclosure of my protected health information. I understand that _____ is not obligated to agree to the restriction and may, therefore, deny my request (unless the request is for the purposes of payment from an insurance carrier or for healthcare operations, and payment for services has been made out-of-pocket in full by the patient). I also understand that a copy of this request and any subsequent agreement, disagreement, or termination will be maintained as part of my medical records as required by the Privacy Rule.

_____ also has the right to terminate this restriction, if they agree to it, at any time. If terminated, an agreed to restriction will not apply to any protected health information obtained after the date of a termination. A copy of any termination will be maintained in my medical record as required by the Privacy rule. Requested restrictions for the purposes of payment from an insurance carrier or for healthcare operations, and for which payment for services has been made out-of-pocket in full by the patient may not be terminated.

This request will identify what protected health information I want to restrict, which persons and/or entities I want to be restricted from receiving the protected health information.

Protected Health Information to be Restricted (please list the information you want restricted)

_____

_____

_____

_____

_____

_____

Entities Restricted from Receiving the Protected Health Information (please identify those who should not receive the information)

_____

_____

_____

____ Requested restriction is for purposes of payment from an insurance carrier or for healthcare operations, and for which I have made payment out-of-pocket in full to the practice.

_____

patient name

_____ _____

patient signature date

Acceptance/Denial of Requested Restriction

Form 7.71

Date: _____

To: _____
Re: Requested restriction to protected health information dated _____

Acceptance of Requested Restriction

_____ Your request to restrict protected health information in your medical record has been accepted. This form serves as our notice to you of the acceptance. Please note that a copy of the restriction will be maintained in your medical record as required by the Privacy Rule.

We reserve the right to terminate the restriction at any time. We will notify you in writing if we choose to terminate the restriction. You may choose to submit a written disagreement to any such termination. Please note that a copy of any termination and/or disagreement will be maintained in your medical record as required by the Privacy Rule.

Denial of Requested Restriction

____ Your request to restrict protected health information in your medical record has been denied. This form serves as our notice to you of the denial. We have attached a copy of the reason for denial to this notice. Please note that a copy of your request and the denial will be maintained, along with the original information in your medical record as required by the Privacy Rule.

You have the right to submit a written disagreement to our denial of your requested restriction. If you wish to submit a written disagreement, it should be sent to our practice and addressed to the attention of our Privacy Manager.

Questions

Please contact our Privacy Manager if you have any questions regarding the acceptance or denial of your requested restriction to protected health information.

Termination of Patient Restriction

Form 7.72

Date: _____

To: _____

Reference: Restriction to protected health information dated _____

On _____, your request to restrict protected health information in your medical record was accepted. Termination of that restriction will take effect 10 days from the date of this notice.

As stated in our original acceptance of your requested restriction, we reserve the right to terminate the restriction at any time. Our original acceptance stated that we would notify you in writing if we decided to terminate the restriction. This notice will serve as our notification to you of our decision to terminate the restriction.

You may choose to submit a written disagreement to this termination. If you wish to submit a written disagreement, it should be sent to our practice and addressed to the attention of our Privacy Manager. Please note that a copy of this termination and any disagreement will be maintained in your medical record as required by the Privacy Rule.

We will continue the terms of the original restriction on any protected health information obtained during the effective dates of the restriction. The terms of the restriction shall not apply to any protected health information obtained prior to the date of acceptance for the restriction or after the effective date of this termination.

Questions

Please contact our Privacy Manager if you have any questions regarding the acceptance or denial of your requested restriction to protected health information.

Patient Request for Amendment of Protected Health Information

Form 7.80

I, the undersigned, am requesting an amendment to my protected health information maintained by _____. I understand that this request may be accepted or denied. I also understand that if my request is accepted the following actions may occur:

- I will be informed of the amendment's acceptance;
- Any applicable original information will still remain in my record with the requested amendment or amended information;
- I may authorize a notification of the amendment to be sent to persons or entities identified by me; and
- A copy of the amended information may be sent to entities that could be predicted to use the original information in a detrimental manner.

If my request is denied, the following actions may occur:

- I will be provided with a written denial explaining the reason for the denial;
- I can submit a disagreement to the denial stating my reasons for disagreeing; and
- I may receive a response (rebuttal) to my disagreement.

I understand that a copy of this request, a copy of an acceptance or denial, a copy of any disagreement, and any rebuttal will become a permanent part of my medical record along with the original information I sought to amend.

_____

patient name

_____ _____

patient signature date

Requested Amendment

I request the following amendment to information in my medical record:

_____

_____

_____

_____

_____

_____

_____

_____

Please continue on the back of this form if necessary.

Acceptance/Denial of Requested Amendment

Form 7.81

Date: _____

To: _____

Reference: Requested amendment to protected health information dated _____

Acceptance of Requested Amendment

☐ Your request to amend protected health information in your medical record has been accepted. This form serves as our notice to you of the acceptance. We will make the amendment to your medical record as you requested. Please note that the original information must still be maintained along with the amended information in your medical record as required by the Privacy Rule.

We will provide a copy of the amendment to persons or entities that you identify on the attached authorization form. We will also provide a copy of the amendment to persons or entities that we have identified in order to prevent them from using the original information, which in certain instances could be detrimental to your care, etc.

Denial of Requested Amendment

☐ Your request to amend protected health information in your medical record has been denied. This form serves as our notice to you of the denial. We have attached a copy of the reason for denial to this notice. Please note that a copy of your request and the denial will be maintained, along with the original information, in your medical record as required by the Privacy Rule.

You have the right to submit a written disagreement to our denial of your requested amendment. If you wish to submit a written disagreement, it should be sent to our practice and addressed to the attention of our Privacy Manager.

After review of your disagreement, we will provide you with a written rebuttal if we decide to continue with the denial. As with the request and initial denial, a copy of any disagreement and rebuttal (if applicable) will be maintained in your medical record as required by the Privacy Rule.

Questions

Please contact our Privacy Manager if you have any questions regarding the acceptance or denial of your requested amendment to protected health information.

Disclosure Accountability Request

Form 7.90

I, the undersigned, am requesting a list of disclosures of my protected health information since the date of _____. I understand that it may require as long as 60 days to provide the listing of disclosures. Additionally, I understand that I may be charged a reasonable fee for any additional disclosure accountability requests made within the twelve months. Any fee for disclosure accountability requests (2nd or more within the same twelve month period) would require payment prior to the listing being made available for my use.

I understand that the Privacy Rule does not allow my healthcare provider to release information such as:

1. Psychotherapy notes;
2. Information intended for use in a civil, criminal, or administrative actions; and
3. Information that cannot be disclosed under the Clinical Laboratory Improvement Amendment.

_____

patient name

_____ _____

patient signature date

PRIVACY BREACH RISK ASSESSMENT GUIDE

NOTE THAT YOU HAVE 60 DAYS TO PROVIDE BREACH NOTIFICATIONS - Use this guide, along with Form 7.91 in assessing a privacy breach. In the process of completing Form 7.91 with the use of this guide, you will determine whether a privacy breach of unsecured protected health information has indeed occurred and whether patient/Health and Human Services notification will be required.

Create a Record - Develop a paper or electronic file in which you can maintain a copy of the Privacy Breach Risk Assessment Form and all subsequent documentation.

☐ **1. Document the Incident** – Complete Form 7.91 with the information that is called for. If it is determined that a breach of unsecured information has occurred that requires notification, the information contained on Form 7.91 will be needed for your notice to Health and Human Services. Some of the information will also be communicated to the patient(s) involved in the breach.

a. Date(s) of Disclovery (the date on which you discovered or were informed of the incident).

b. Date(s) of Breach (the date on which the incident occurred - if it can be determined).

c. The employee(s) involved in the incident.

d. Select the category of protected health information (i.e., demographic, clinical, financial) involved in the breach and a description of the type of patient information involved. Please do not list the actual information, only a *description* of the *type* of information (i.e., patient names, addresses, phone numbers, dates of birth, social security numbers, etc.) Note that in a written notification to the patient, you will have to list each type of information that has been disclosed.

e. Select the type of breach (i.e., theft, unauthorized disclosure, etc.) and provide a description of what occurred. This is a narrative that describes how the breach (may have) occurred.

f. Location of breached information. If known, select the location of the information at the time of the breach.

g. Select the security safeguards that were in place prior to the breach. This item may help you to determine logical security measures that will prevent a recurrence of the incident.

☐ **2. Risk Assessment** – Any impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity can demonstrate that there is a low probability that the PHI has been compromised. You must evaluate each impermissible use or disclosure according to the following four factors in order to assess this probability.

Factor 1 – Consider *the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.*
Considering the types of PHI involved, what is the probability that the PHI could be used by an unauthorized recipient in a manner adverse to the individual or otherwise used to further the unauthorized recipient's own interests? For example, if patient names, addresses and social security numbers was impermissibly disclosed, the PHI is obviously identifiable, and a risk assessment likely would determine that there is more than a low probability that the information has been compromised, dependent on an assessment of the other factors.

The likelihood that the PHI released could be re-identified based on the context and the ability to link the information with other valuable information must also be considered. For example, if only a list of treatment dates and diagnoses was disclosed, the entity would need to consider whether any of the individuals could be identified based on the specificity of the diagnosis, the size of the community served by the covered entity, or whether the unauthorized recipient has the ability to combine the information with other information to re-identify the affected individuals.

Factor 2 – *Consider the unauthorized person who used the PHI or to whom the disclosure was made.*
Was the recipient of the PHI a covered entity, or entity otherwise obligated to protect the privacy and security of the information (another practice, a hospital, Federal agency, etc.)?

Does the unauthorized person who received the PHI have the ability to re-identify the information? For example, if dates of healthcare service and diagnoses of an employee was impermissibly disclosed to his/her employer, the employer may be able to determine that the information pertains to a specific employee based on other information available to the employer, such as dates of absence from work. In this case, there may be more than a low probability that the PHI has been compromised.

Factor 3 – *Consider whether the PHI was actually acquired or viewed.*
For example, if a covered entity mailed PHI to the wrong individual who opened the envelope and called the entity to say that she received the information in error, then, in this case, the unauthorized recipient viewed and acquired the information because she opened and read the information to the extent that she recognized it was mailed to her in error.

Factor 4 – *Consider the extent to which the risk to the PHI has been mitigated.*
Were you able to take immediate steps to mitigate the disclosure (i.e., obtaining the recipient's assurances that the information would not be further used or disclosed, and would be destroyed)? Depending on the professional reliability of the recipient (a known legal or accounting firm versus an unknown individual), the covered entity may or may not be able to rely on the recipient's assurances.

☐ **Final Risk Determination** - Evaluate the overall probability that the PHI has been compromised by considering all of the factors in combination. If an evaluation fails to demonstrate that there is a low probability that the PHI has been compromised, breach notification is required (continue with item 4 below).

If you determine that there is only a low probability that the PHI was compromised, there is no need to send a notice to the patient(s) or to submit notice to HHS. However, you must maintain documentation of the incident (Form 7.91) for a minimum of six years.

☐ **3. Create a notification letter** – You must provide the affected individual(s) with written notification within 60 days of the date of discovery. You may use the Sample Privacy Breach Notification Letter that follows Form 7.91. The notification is required to include the following information:

a. A brief description of what happened, including the date of the breach (if known) and the date of discovery of the breach;

b. A description of the types of unsecured information that was involved in the breach (i.e., individual's full name, social security number, date of birth, home address, account number, diagnosis, disability code, and other types of PHI). Note – only the types of information will be listed, not the actual information;

c. Any steps an individual should take to protect themselves from potential harm resulting from the breach (i.e., recommendations for an individual to contact credit bureaus and how to make contact if credit card information was involved);

d. A brief description of what the practice is doing to investigate the breach, to limit harm to individuals, and to protect against any further breaches including the imposition of employee sanctions, if appropriate; and

e. Contact procedures (i.e., the practice's Compliance or Privacy Officer contact information) for individuals to ask questions or learn additional information, which will include a toll-free number, an email address, website, or postal address.

☐ **4. Send notification to affected individuals** – You must mail written notification to the affected individuals, their appointed personal representatives, or known living relatives. Email notification may be provided if the patient has agreed to receive an electronic notice. Likewise, the notice may be provided via telephone only if the patient has specifically requested telephone communication. Note that the Security Rule requires that an email containing such information would need to be secure (i.e., encrypted).

☐ **5. Provide required notification to HHS** – Follow the policies in section 3.35 of the HIPAA Manual to provide notice to the Secretary of Health and Human Services. Notice will be provided within 60 days of the date of discovery if the breach involved 500 or more patients. Notice will be submitted at the end of the calendar year in which the breach occurred if it involved fewer than 500 individuals.

☐ **6. Provide substitute notices and notification to media, if required** – Policies in sections 3.33d – 3.34b of the HIPAA Manual should be followed for special circumstances as needed.

Contact Eagle Associates at (800) 777-2337 for additional assistance in handling privacy breach incidents.

Privacy Breach Risk Assessment Form

Form 7.91

Covered Entity Name: _____

Contact Name: _____

Contact Phone: _____ Contact Email: _____

Potential Breach

Date(s) of Discovery: _____ Date(s) of Breach: _____

Employee(s) Involved in Incident: _____

_____

Type of Breach:

- ☐ Theft
- ☐ Loss
- ☐ Improper Disposal
- ☐ Other: _____
- ☐ Unauthorized Access/Disclosure
- ☐ Hacking/IT Incident
- ☐ Unknown

Number of Patients Affected by the Breach: _____
(provide an approximate number if the exact number is unknown)

Description of the Breach: Please include the location of the breach, a description of how the breach occurred, and any additional information regarding the type of breach, type of media, and types of protected health information involved in the breach.

_____

_____

Location of Breached Information: Please select the location of the information at the time of the breach. If selecting the "Other" category, describe the location of the information.

- ☐ Laptop
- ☐ Desktop Computer
- ☐ Network Server
- ☐ Paper
- ☐ Email
- ☐ Other Portable Electronic Device
- ☐ Electronic Medical Record
- ☐ Other: _____

Safeguards in Place Prior to Breach: Please indicate what protective measures were in place prior to the breach.

- ☐ Firewalls
- ☐ Packet Filtering (router-based)
- ☐ Secure Browser Sessions
- ☐ Physical Security
- ☐ Strong Authentication
- ☐ Encrypted Wireless
- ☐ Logical Access Control

Risk Assessment (Please see the Privacy Breach Risk Assessment Guide for further explanation).

FACTOR 1

Type of Protected Health Information Involved in the Breach: Please select all categories of protected health information that were involved in the breach. If selecting the "Other" category, please describe the information in detail in the description section below.

- ☐ Demographic Information
- ☐ Financial Information
- ☐ Clinical Information
- ☐ Other: _____

Describe the specific type(s) of patient information involved in the incident (if known), such as types of demographic information (i.e., patient names, addresses, dates of birth), financial information (i.e., social security numbers, credit card numbers, etc.), and clinical information (i.e., diagnoses, treatment plans, medical histories, test results, etc.):

_____

_____

What is the likelihood that the information could be re-identified: _____

Considering the type of PHI involved, what is the probability that the PHI could be used by an unauthorized recipient in a manner adverse to the individual, or otherwise used to further the unauthorized recipient's own interests? _____

_____

FACTOR 2

Was the recipient of the PHI a covered entity, or otherwise obligated to protect the privacy and security of the information? _____

Does the unauthorized person have the ability to re-identify the information? _____

FACTOR 3

Was the impermissibly used or disclosed PHI actually viewed or acquired? _____

_____

FACTOR 4

What steps were taken to mitigate risk to the PHI: _____

_____

_____

Considering the steps that were taken to mitigate risk to the PHI, and the recipient of the unauthorized disclosure, what is the probability that the information was compromised?_____

Risk Determination

- ☐ There is a low probability that the impermissibly used or disclosed PHI has been compromised. Maintain a copy of this form, including any additional information to support your determination, for a minimum of six years. No further action is required.
- ☐ There is a significant risk that the impermissibly used or disclosed PHI has been compromised. Complete the remaining steps below.

Notice of Breach and Actions Taken

Date(s) of Patient Notification (must be provided within 60 days of the date of discovery):

Was Substitute Notice Required? _____

Was Media Notice Required?: _____

Notice to the Secretary of Health and Human Services

For breaches involving more than 500 individuals, the practice must notify the Secretary of Health and Human Services within 60 days following discovery of the breach. Was such notice required? _____

For breaches involving fewer than 500 individuals, the practice must electronically submit notice to HHS between January 1 and March 1. See section 3.35 of the HIPAA Manual for more information, including instructions for accessing the electronic form for submission of privacy breach notifications. Indicate the individual responsible for year-end notification to HHS:

Actions Taken in Response to Breach: Please select the actions taken to respond to the breach. If selecting the "Other" category, please describe the actions taken in the section below.

- ☐ Security and/or Privacy Safeguards
- ☐ Mitigation
- ☐ Sanctions
- ☐ Policies and Procedures
- ☐ Other

Describe Other Actions Taken: Please describe in detail any actions taken following the breach in addition to those selected above.

Business Associate (complete this section if breach occurred at, or by a Business Associate)

Name of Business Associate: _____

Address: _____

City: _____ State: _____ Zip Code: _____

Business Associate Contact Name: _____

Business Associate Contact Phone: _____

Business Associate Contact Email: _____

Sample Privacy Breach Notification Letter **Form 7.92**

Dear Patient:

On *(insert the date of discovery)* we discovered an unauthorized disclosure of your patient information. The disclosure occurred on *(insert the date the breach occurred or the approximate date if unknown)*. Your information was accidentally mailed to another patient of the practice. *(Insert a brief description of what occurred such as this example. Keep the description as brief and as simple as possible while stating what happened)*.

The disclosed information included your name, address, phone number and social security number *(provide the patient with a description of the type(s) of information disclosed, as in this example - not the actual data)*.

We recommend *(this example recommends monitoring credit reports, but is dependent upon what type of information was disclosed – there may be no need for monitoring)* that you check with your local credit bureau or credit monitoring agency *(you can recommend the three common agencies – TransUnion, Experian, or Equifax or not recommend any agencies)* for any unauthorized activity with your credit or identity.

We have investigated the incident and taken appropriate corrective actions including disciplinary actions with the employees who were involved in the disclosure. We feel confident that the corrective actions will prevent any recurrence of this type of unauthorized disclosure in the future.

OR *(if your investigation is ongoing)*

We are continuing to investigate the incident and will provide a follow up to notify you of our results. As necessary, we will be implementing appropriate corrective and disciplinary actions to prevent any recurrence of this type of unauthorized disclosure in the future.

We are committed to protecting the information of our patients and apologize for this incident. Please feel free to contact our Privacy Manager at XXX-XXX_XXXX (this should be a toll free call) with any questions or requests for additional information.

Sincerely,

The Practice