

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE READ IT CAREFULLY.

NOTICE OF PRIVACY POLICY

Effective April 1, 2003

The following is the privacy policy ("Privacy Policy") of Dr. Thomas Cristello D.C. ("Covered "Entity") as described in the Health Insurance Portability and Accountability Act of 1996 and regulations promulgated thereunder, commonly known as HIPAA. HIPAA requires Covered Entity by law to maintain the privacy of your personal health information and to provide you with notice of Covered Entity's legal duties and privacy policies with respect to your personal health information. We are required by law to abide by the terms of this Privacy Notice.

Your Personal Health Information

We collect personal health information from you through treatment, payment and related healthcare operations, the application and enrollment process, and/or healthcare providers or health plans, or through other means, as applicable. Your personal health information that is protected by law broadly includes any information, oral, written or recorded, that is created or received by certain health care entities, including health care providers, such as physicians and hospitals, as well as, health insurance companies or plans. The law specifically protects health information that contains data, such as your name, address, social security number, and others, that could be used to identify you as the individual patient who is associated with that health information.

Uses or Disclosures of Your Personal Health Information

Generally, we may not use or disclose your personal health information without your permission. Further, once your permission has been obtained, we must use or disclose your personal health information in accordance with the specific terms that permission. The following are the circumstances under which we are permitted by law to use or disclose your personal health information.

Without Your Consent

Without your consent, we may use or disclose your personal health information in order to provide you with services and the treatment you require or request, or to collect payment for those services, and to conduct other related health care operations otherwise permitted or required by law. Also, we are permitted to disclose your personal health information within and among our workforce in order to accomplish these same purposes. However, even with your permission, we are still required to limit such uses or disclosures to the minimal amount of personal health information that is reasonably required to provide those services or complete those activities.

Examples of treatment activities include: (a) the provision, coordination, or management of health care and related services by health care providers; (b) consultation between health care providers relating to a patient; or (c) the referral of a patient for health care from one health care provider to another.

Examples of payment activities include: (a) billing and collection activities and related data processing; (b) actions by a health plan or insurer to obtain premiums or to determine or fulfill its responsibilities for coverage and provision of benefits under its health plan or insurance agreement, determinations of eligibility or coverage, adjudication or subrogation of health benefit claims; (c) medical necessity and appropriateness of care reviews, utilization review activities; and (d) disclosure to consumer reporting agencies of information relating to collection of premiums or reimbursement.

Courtesy of Baker & Hostetler, LLP.

Examples of health care operations include:

(a) development of clinical guidelines; (b) contacting patients with information about treatment alternatives or communications in connection with case management or care coordination; (c) reviewing the qualifications of and training health care professionals; (d) underwriting and premium rating; (e) medical review, legal services, and auditing functions; and (f) general administrative activities such as customer service and data analysis.

As Required By Law

We may use or disclose your personal health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law. *Examples of instances in which we are required to disclose your personal health information include:* (a) public health activities including, preventing or controlling disease or other injury, public health surveillance or investigations, reporting adverse events with respect to food or dietary supplements or product defects or problems to the Food and Drug Administration, medical surveillance of the workplace or to evaluate whether the individual has a work-related illness or injury in order to comply with Federal or state law; (b) disclosures regarding victims of abuse, neglect, or domestic violence including, reporting to social service or protective services agencies; (c) health oversight activities including, audits, civil, administrative, or criminal investigations, inspections, licensure or disciplinary actions, or civil, administrative, or criminal proceedings or actions, or other activities necessary for appropriate oversight of government benefit programs; (d) judicial and administrative proceedings in response to an order of a court or administrative tribunal, a warrant, subpoena, discovery request, or other lawful process; (e) law enforcement purposes for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, or reporting crimes in emergencies, or reporting a death; (f) disclosures about decedents for purposes of cadaveric donation of organs, eyes or tissue; (g) for research purposes under certain conditions; (h) to avert a serious threat to health or safety; (i) military and veterans activities; (j) national security and intelligence activities, protective services of the President and others; (k) medical suitability determinations by entities that are components of the Department of State; (l) correctional institutions and other law enforcement custodial situations; (m) covered entities that are government programs providing public benefits, and for workers' compensation.

All Other Situations, With Your Specific Authorization

Except as otherwise permitted or required, as described above, we may not use or disclose your personal health information without your written authorization. Further, we are required to use or disclose your personal health information consistent with the terms of your authorization. You may revoke your authorization to use or disclose any personal health information at any time, except to the extent that we have taken action in reliance on such authorization, or, if you provided the authorization as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy.

Miscellaneous Activities, Notice

We may contact you to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to you. We may contact you to raise funds for Covered Entity. If we are a group health plan or health insurance issuer or HMO with respect to a group health plan, we may disclose your personal health information to be sponsor of the plan.

Your Rights With Respect to Your Personal Health Information

Under HIPAA, you have certain rights with respect to your personal health information. The following is a brief overview of your rights and our duties with respect to enforcing those rights.

Right To Request Restrictions On Use Or Disclosure

You have the right to request restrictions on certain uses and disclosures of your personal health information about yourself. *You may request restrictions on the following uses or disclosures:* to carry out treatment, payment, or

healthcare operations; (b) disclosures to family members, relatives, or close personal friends of personal health information directly relevant to your care or payment related to your health care, or your location, general condition, or death; (c) instances in which you are not present or your permission cannot practicably be obtained due to your incapacity or an emergency circumstance; (d) permitting other persons to act on your behalf to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of personal health information; or (e) disclosure to a public or private entity authorized by law or by its charter to assist in disaster relief efforts.

While we are not required to agree to any requested restriction, if we agree to a restriction, we are bound not to use or disclose your personal healthcare information in violation of such restriction, except in certain emergency situations. We will not accept a request to restrict uses or disclosures that are otherwise required by law.

Right To Receive Confidential Communications

You have the right to receive confidential communications of your personal health information. We may require written requests. We may condition the provision of confidential communications on you providing us with information as to how payment will be handled and specification of an alternative address or other method of contact. We may require that a request contain a statement that disclosure of all or a part of the information to which the request pertains could endanger you. We may not require you to provide an explanation of the basis for your request as a condition of providing communications to you on a confidential basis. We must permit you to request and must accommodate reasonable requests by you to receive communications of personal health information from us by alternative means or at alternative locations. If we are a health care plan, we must permit you to request and must accommodate reasonable requests by you to receive communications of personal health information from us by alternative means or at alternative locations if you clearly state that the disclosure of all or part of that information could endanger you.

Right To Inspect And Copy Your Personal Health Information

Your designated record set is a group of records we maintain that includes Medical records and billing records about you, or enrollment, payment, claims adjudication, and case or medical management records systems, as applicable. You have the right of access in order to inspect and obtain a copy your personal health information contained in your designated record set, *except for* (a) psychotherapy notes, (b) information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding, and (c) health information maintained by us to the extent to which the provision of access to you would be prohibited by law. We may require written requests. We must provide you with access to your personal health information in the form or format requested by you, if it is readily producible in such form or format, or, if not, in a readable hard copy form or such other form or format. We may provide you with a summary of the personal health information requested, in lieu of providing access to the personal health information or may provide an explanation of the personal health information to which access has been provided, if you agree in advance to such a summary or explanation and agree to the fees imposed for such summary or explanation. We will provide you with access as requested in a timely manner, including arranging with you a convenient time and place to inspect or obtain copies of your personal health information or mailing a copy to you at your request. We will discuss the scope, format, and other aspects of your request for access as necessary to facilitate timely access. If you request a copy of your personal health information or agree to a summary or explanation of such information, we may charge a reasonable cost-based fee for copying, postage, if you request a mailing, and the costs of preparing an explanation or summary as agreed upon in advance. We reserve the right to deny you access to and copies of certain personal health information as permitted or required by law. We will reasonably attempt to accommodate any request for personal health information by, to the extent possible, giving you access to other personal health information after excluding the information as to which we have a ground to deny access. Upon denial of a request for access or request for information, we will provide you with a written denial specifying the legal basis for denial, a statement of your rights, and a description of how you may file a complaint with us. If we do not maintain the information that is the subject of your request for access but we know where the requested information is maintained, we will inform you of where to direct your request for access.

Right To Amend Your Personal Health Information

You have the right to request that we amend your personal health information or a record about you contained in your designated record set, for as long as the designated record set is maintained by us. We have the right to deny your request for amendment, if: (a) we determine that the information or record that is the subject of the request was not created by us, unless you provide a reasonable basis to believe that the originator of the information is no longer available to act on the requested amendment, (b) the information is not part of your designated record set maintained by us, (c) the information is prohibited from inspection by law, or (d) the information is accurate and complete. We may require that you submit written requests and provide a reason to support the requested amendment. If we deny your request, we will provide you with a written denial stating the basis of the denial, your right to submit a written statement disagreeing with the denial, and a description of how you may file a complaint with us or the Secretary of the U.S. Department of Health and Human Services ("DHHS"). This denial will also include a notice that if you do not submit a statement of disagreement, you may request that we include your request for amendment and the denial with any future disclosures of your personal health information that is the subject of the requested amendment. Copies of all requests, denials, and statements of disagreement will be included in your designated record set. If we accept your request for amendment, we will make reasonable efforts to inform and provide the amendment within a reasonable time to persons identified by you as having received personal health information of yours prior to amendment and persons that we know have the personal health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to your detriment. All requests for amendment shall be sent to **Dr. Thomas Cristello D.C., 9 E 19th St. 6th Floor, NY NY 10003**.

Right To Receive An Accounting Of Disclosures Of Your Personal Health Information

Beginning April 14, 2003, you have the right to receive a written accounting of all disclosures of your personal health information that we have made within the six (6) year period immediately preceding the date on which the accounting is requested. You may request an accounting of disclosures for a period of time less than six (6) years from the date of the request. Such disclosures will include the date of each disclosure, the name and, if known, the address of the entity or person who received the information, a brief description of the information disclosed, and a brief statement of the purpose and basis of the disclosure or, in lieu of such statement, a copy of your written authorization or written request for disclosure pertaining to such information. *We are not required to provide accountings of disclosures for the following purposes:* (a) treatment, payment, and healthcare operations, (b) disclosures pursuant to your authorization, (c) disclosures to you, (d) for a facility directory or to persons involved in your care, (e) for national security or intelligence purposes, (f) to correctional institutions, and (g) with respect to disclosures occurring prior to 4/14/03. We reserve our right to temporarily suspend your right to receive an accounting of disclosures to health oversight agencies or law enforcement officials, as required by law. We will provide the first accounting to you in any twelve (12) month period without charge, but will impose a reasonable cost-based fee for responding to each subsequent request for accounting within that same twelve (12) month period. All requests for an accounting shall be sent to **Dr. Thomas Cristello D.C., 9 E 19th St. 6th Floor, NY NY 10003**.

Complaints

You may file a complaint with us and with the Secretary of DHHS if you believe that your privacy rights have been violated. You may submit your complaint in writing by mail or electronically to our privacy officer, **Dr. Thomas Cristello D.C., 9 E 19th St. 6th Floor, NY NY 10003**. A complaint must name the entity that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable requirements of HIPAA or this Privacy Policy. A complaint must be received by us or filed with the Secretary of DHHS within 180 days of when you knew or should have known that the act or omission complained of occurred. You will not be retaliated against for filing any complaint.

Amendments to this Privacy Policy

We reserve the right to revise or amend this Privacy Policy at any time. These revisions or amendments may be made effective for all personal health information we maintain even if created or received prior to the effective date of the

revision or amendment. We will provide you with notice of any revisions or amendments to this Privacy Policy, or changes in the law affecting this Privacy Notice, by mail or electronically within 60 days of the effective date of such revision, amendment, or change.

On-going Access to Privacy Policy

We will provide you with a copy of the most recent version of this Privacy Policy at any time upon your written request sent to **Dr. Thomas Cristello D.C., 9 E 19th St. 6th Floor, NY NY 10003** or at the following website address: N/A. For any other requests or for further information regarding the privacy of your personal health information, and for information regarding the filing of a complaint with us, please contact our privacy officer, at the address, telephone number, or e-mail address listed above.

Abbreviated Notice of Privacy Policy For Dr. Thomas Cristello D.C.
Effective April 1, 2003

We collect your personal health information from you through treatment, payment or other means as applicable. Your personal health information is protected by federal law. Generally we do not use or disclose your information without your permission. Once permission has been obtained, we must disclose your personal health information in accordance with the specific terms of permission. The following is an outline of the circumstances under which we are permitted by law to use or disclose your personal health information. You may request a copy of the detailed privacy policy with a written request sent to: Dr. Thomas Cristello D.C. 9 E 19th St. 6th Floor, NY, NY 10003.

1. With out your consent we may use or disclose your personal health information in order to provide you with services and treatments you may require or request, or to collect payment for services or and to conduct other operations otherwise permitted or required by law. We can also disclose your personal health information within and among our workforce to accomplish the same purposes.
2. As required by law we may use or disclose your personal health information to the extent that such use or disclosure as required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.
3. All other situations, with your specific authorization. Except as otherwise permitted or required, as outlined above, we may not use or disclose your personal health information without your written permission. You may revoke your authorization at any time except is some circumstances.
4. Miscellaneous Activities, NOTICE WE may contact you to provide appointment reminders or information about treatments or other heath-related benefits and services that may be of interest to you.

Your Rights with Respect to your Personal Health Information

1. Right to Request Restrictions on Use or Disclosure
2. Right to Receive Confidential Information
3. Right to Receive Confidential Communications
4. Right to Inspect and Copy Your Personal Health Information
5. Right to Amend Your Personal Health Information
6. Right to Receive and Accounting of Disclosures of Your Personal Health Information
7. Right to file a complaint with us and the Secretary of the DHHS if you believe your privacy rights have been violated. You may submit your complaint in writing by mail to our privacy officer, Dr. Thomas Cristello within 180 days of when you knew or should have known the act of omission complained of occurred. You will not be retaliated against for filing any complaint.

We reserve the right to amend this privacy policy at any time for which we will provide you with notice within 60 days of the effective date of such revision, amendment or change.

Dr. Thomas Cristello D.C.

Accounting of Non-Authorized Use or Disclosure Request Form

I, _____, request that Dr. Thomas Cristello provide me with an accounting of any and all applicable "non-authorized" uses and disclosures of my protected health information (PHI) between _____ (beginning date) and _____ (ending date).

I would like to limit this request for accounting to include disclosures only pertaining to:

I understand that I may be charged for this information if I have previously requested this information within the last 12 months. I have been informed of the approximate cost of \$_____, and agree to be financially responsible for this charge.

Patient signature: _____
Printed name and date of birth: _____
Date: _____

Privacy Officer Action/Comments:

Action must be taken within 60 days of the receipt of the request

- ____ Request approved
- ____ Request denied for the following reason. Health Information was released:
 - ____ For treatment, payment, or health care operations
 - ____ To you
 - ____ With your authorization
 - ____ For National Security Purposes
 - ____ For Law Enforcement purposes
 - ____ As part of a limited data set
 - ____ Prior to April 14, 2003
 - ____ Incident to an otherwise permitted use or disclosure
- ____ Request 30-day extension to respond due to _____

Authorization Form Policy

Effective date of policy April 15, 2003

Protected health information (PHI) will only be released from our practice with a properly executed authorization from the patient or his/her personal representative, except for treatment, payment, or health care operations (TPO) and as otherwise required by law. Examples of some instances in which we are required to disclose your PHI include:

Public health activities; information regarding victims of abuse, neglect, or domestic violence; health oversight activities; judicial and administrative proceedings; law enforcement purposes; organ donations purposes; research purposes under certain circumstances; national security and intelligence; correctional institutions; and
Worker's Compensation.

Dr. Thomas Cristello will only use or disclose PHI, except as noted above, consistent with the terms of the authorization.

A patient may revoke his authorization to use or disclose PHI at any time but actions taken prior to the revocation are excluded. If authorization is a condition of obtaining insurance coverage, and the authorization is revoked, the insurer may contest a claim under the policy.

Authorizations must be properly executed by the patient or his personal representative. It should include, the date signed, specific PHI to be released or used, to whom this use or release relates, and an expiration date for the authorization.

Right to Confidential Communications Policy

Patients may request to receive confidential communications of their protected health information (PHI) from Dr. Thomas Cristello.

A patient may request that communications from the practice be sent to an alternate location or by an alternate means. Dr. Thomas Cristello will accommodate reasonable requests for such confidential communications. The patient is not required to give a reason for this request. If disclosing information through regular channels will endanger the patient, he/she may want to make that known to you.

Dr. Thomas Cristello prefers these requests be in writing.

Privacy Complaint Policy

Effective date of policy: April 15, 2003

Patients have a right to file a formal complaint if they feel we have not adequately protected their privacy. This complaint must be submitted in writing to the privacy officer or may be submitted directly to the U.S. Department of Health and Human Services Secretary. The complaint must be submitted within 180 days of the event of concern.

The privacy officer is responsible for the investigation and resolution of the complaint.

The practice must maintain a record of the complaints and the resolution, if applicable, for six (6) years.

Confidentiality Policy

Effective date of policy: April 15, 2003

All employees, staff, contractors, and agents of our practice will be trained to respect the health care information of the patients of our practice. They will treat all medical, personal, biometric, and financial information as confidential.

All employees, staff, contractors, and agents of our practice will receive confidentiality training and sign confidentiality agreements annually.

Any person who breaches this trust will be disciplined and risks immediate termination.

Medical Record Amendment Policy

Policy effective date: April 15, 2003

Any patient may request that his/her medical record be changed, corrected, or amended. This request must be in writing and must include the reason for the desired change, amendment, or correction.

This practice may accept or deny this request and will inform the patient in writing of the decision within 60 days. One 30-day extension is permitted if the patient is notified of the reason for the delay. If the request is denied, the practice must give a reason for denying the request. The patient may file a written rebuttal to the denial.

Denying a request to amend the medical record may be due to, but not limited to, some of the following reasons: information is not part of the designated record set; information is complete and accurate; under HIPAA the patient is restricted from accessing or amending this information.

Requests will be retained for six (6) years and must be included in future releases of the patient's protected health information (PHI). If the amendment request has been denied, this denial letter must also be included in future PHI disclosures.

Requests for amendment of medical records should be submitted to the privacy officer for action.

Minimum Necessary Disclosure Policy

Effective date of policy: April 15, 2003

All uses, disclosures of, or requests for protected health information (PHI) will be limited to the minimum amount necessary to accomplish the stated purpose. Professional judgment will determine the amount of information to be released. The minimum necessary standard is not intended to impede the provision of quality health care.

Disclosures of PHI between providers for treatment, payment and health care operations, or pursuant to an authorization without complying with this requirement are exempt from the minimum necessary rule.

Notice of Privacy Practices (NPP) Policy

Effective date of policy: April 15, 2003

Every patient will receive a Notice of Privacy Practices (NPP):

- You **MUST** distribute it to your patient as the first officer visit after 4/13/03 and you must get **written documentation** from the patient that he/she received this notice.
- You must post an abbreviated notice prominently in the office.
- You may distribute it via e-mail with a return receipt.
- If you have a Web site, it must be on the Web site.
- You must make a reasonable effort to assure that each patient gets a **Notice of Privacy Practice** on his or her first date of service after 4/13/03 and document this effort in writing.

In the event that the patient does not get a notice while in the office, you should mail the notice to them, **ON THE SAME DAY**, and document why it was not given to the patient at the time of service and that the notice was mailed.

Your notice:

- Must be posted in an abbreviated form prominently in the office.
- May be distributed via e-mail with a return receipt for documentation.
- Must be on your Web site, if you have one.

This office will comply with all aspects as printed in our Notice of Privacy Practices and our privacy notice will be in compliance with all appropriate laws and regulations, federal, state, and local.

Patient Access to the Medical Record Policy

Effective date of policy April 15, 2003

Deleted: :

Patients have the right to inspect and receive copies of their medical records. This practice may charge for the copying of the record, as well as supplies, labor, and postage, and the patient should be notified of this cost in advance. The patient should agree to this financial responsibility in writing, in advance. (See form.)

This practice has the right to deny a patient's request to inspect and copy their medical record. This denial must be in writing and explain why the request has been denied.

There are several circumstances when the denial may not be appealed (*unreviewable denial*).

- Psychotherapy notes.
- Information compiled in reasonable anticipation of or for use in a civil, criminal, or administrative action proceeding.
- Protected health information (PHI) maintained by a practice subject to Clinical Laboratory Improvements Amendments (CLIA) (to the extent access to an individual would be prohibited by law).
- PHI regarding an inmate at a correctional facility.
- In research situations, if the patient was advised prior to the study.
- If the information was obtained from someone other than a health care provider and if access would compromise an individual providing information under a promise of confidentiality.

The patient can appeal the denial and has the right to request review by another licensed health professional designated by the practice and who was not a part of the original decision to deny access (*reviewable denial*).

- If a licensed health care professional determines that the requested access would endanger the life or physical safety of the individual or another person.
- If the record makes reference to another person and the licensed health professional believes the access could cause substantial harm to that person.
- Request has been made by patient's personal representative and the licensed professional believes it could cause harm to that individual or another person.

Patients should make this request on the attached form, which is then submitted to the privacy officer for action.

**Restriction of Use or Disclosure of Protected Health Information (PHI)
Policy**

Effective date of policy: April 15, 2003

A patient has the right to REQUEST that the use and disclosure of his protected health information (PHI) be restricted for treatment, payment, and health care operations (TPO), as well as restricting disclosure to certain people, such as family members.

Deleted:

THIS PRACTICE DOES NOT HAVE TO AGREE TO SUCH REQUESTS.

The restriction request must be in writing, be specific as to what information is covered by the request, whether it covers use, disclosure, or both, and to whom these limitations apply.

If this practice agrees to the request, it will honor the request except when overriding laws or emergencies apply.

The agreement to restrict health information use and/or disclosure of treatment, payment, or health care operations may be terminated at any time, in writing, by the patient, or by the practice for health information created or received after the date of the notice.

Accounting of Non-Authorized Use or Disclosure Request Form

I, _____, request that Dr. Thomas Cristello provide me with an accounting of any and all applicable “non-authorized” uses and disclosures of my protected health information (PHI) between _____ (beginning date) and _____ (ending date).

I would like to limit this request for accounting to include disclosures only pertaining to:

I understand that I may be charged for this information if I have previously requested this information within the last 12 months. I have been informed of the approximate cost of \$_____, and agree to be financially responsible for this charge.

Patient signature: _____
Printed name and date of birth: _____
Date: _____

Privacy Officer Action/Comments:

Action must be taken within 60 days of the receipt of the request

- ____ Request approved
- ____ Request denied for the following reason. Health Information was released:
 - ____ For treatment, payment, or health care operations
 - ____ To you
 - ____ With your authorization
 - ____ For National Security Purposes
 - ____ For Law Enforcement purposes
 - ____ As part of a limited data set
 - ____ Prior to April 14, 2003
 - ____ Incident to an otherwise permitted use or disclosure
- ____ Request 30-day extension to respond due to _____

**HIPAA PRIVACY
AUTHORIZATION FOR USE AND DISCLOSURE OF
PERSONAL HEALTH INFORMATION**

This authorization is prepared pursuant to the requirements of the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191), 42 U.S.C. Section 1320d, et. seq., and regulations promulgated thereunder, as amended from time to time (collectively referred to as "HIPAA").

This authorization affects your rights in the privacy of your personal healthcare information. Please read it carefully before signing.

_____, ("Covered Entity") will not condition treatment payment, enrollment in a health plan, or eligibility for benefits, as applicable, on your providing authorization for the requested use or disclosure. **YOU MAY REFUSE TO SIGN THIS AUTHORIZATION.**

By signing this authorization you acknowledge and agree that Covered Entity may use or disclose _____ [describe information] for the purpose(s) of _____ [describe intended use].

By signing this authorization you agree that Covered Entity or its Business Associates may disclose your personal health care information to _____ [identify intended recipients].

Further, by signing this authorization you acknowledge that you have been provided a copy of and have read and understand Covered Entity's HIPAA Privacy Notice containing a complete description of your rights, and the permitted uses and disclosures, under HIPAA. While Covered Entity has reserved the right to change the terms of its Privacy Notice, copies of the Privacy Notice as amended are available from Covered Entity at any of its offices or by sending a written request with return address to 9 E 19th St. 6th Floor, New York, NY 10003.

In accordance with your rights under, and subject to certain restrictions imposed by, HIPAA, you may inspect or copy your PHI in the designated record set maintained by Covered Entity for as long as the PHI is maintained in the designated record set.

You have the right to revoke this authorization, in writing, at any time, except to the extent that Covered Entity has taken action in reliance on it. A revocation is effective upon receipt by Covered Entity of a written request to revoke and a copy of the executed authorization form to be revoked at the address listed above.

This authorization shall expire upon the earlier occurrence of: (a) revocation of the authorization, (b) a finding by the Secretary of the U.S. Department of Health and Human Services, Office of Civil Rights that this authorization is not in compliance with requirements of HIPAA, (c) complete satisfaction of the purposes for which this authorization was originally obtained, to be determined in the reasonable discretion of Covered Entity, or (d) six years from the date this authorization was executed.

By signing this authorization you acknowledge and agree that any information used or disclosed pursuant to this authorization could be at risk for redisclosure by the recipient and no longer protected under HIPAA.

Covered Entity will provide _____ [name of patient] with a copy of this signed authorization.

Acknowledged and agreed to by:

PATIENT:

By _____
Print Name _____ Date _____

Address: _____

or, ON BEHALF OF PATIENT

By _____
Print Name _____ Date _____
As _____

Address: _____

Dr. Thomas Cristello D.C.

Authorization for Disclosure of Health Information

Patient Name: _____

Date of Birth: _____ Phone: _____

Address: _____

City: _____ State: _____ Zip: _____

- 1. *I authorize the use or disclosure of the above named individual's health information as described below.*
- 2. *The following individual or organization is authorized to make the disclosure:*

Name: _____

Address: _____

City: _____ State: _____ Zip: _____

- 3. The type and amount of information to be used or disclosed is as follows: (include dates where appropriate).

Complete health records Lab results/X-ray reports
 Physical exam Consultation reports
 Immunization record
 Other (please specify: _____)

- 4. I understand that the information in my health record may include information relating to sexually transmitted disease, acquired immunodeficiency syndrome (AIDS) or human immunodeficiency virus (HIV). It may also include information about behavioral or mental health services and treatment for alcohol and drug abuse.

- 5. *This information may be disclosed to and used by the following individual or organization.*

Name: _____

Address: _____

City: _____ State: _____ Zip: _____

For the purpose of: _____

- 6. I understand that I have a right to revoke this authorization at any time. I understand that if I revoke this authorization I must do so in writing and present my written revocation to the health information management department. I understand that the revocation will not apply to my insurance company when the law provides my insurer with the right to contest a claim under my policy. Unless otherwise revoked, this authorization will expire on the following date, event, or condition: _____

- 7. If I fail to specify an expiration date, event or condition, this authorization will expire in sixty days. I understand that authorizing the disclosure of this health information is voluntary. I can refuse to sign this authorization. I need not sign this form in order to assure treatment. I understand that I may inspect or copy the information to be used or disclosed, as provided in CFR 164.524. I understand that any disclosure of information carries with it the potential for an unauthorized redisclosure and the information may not be protected by federal confidentiality rules. If I have questions about disclosure of my health information, I can contact:

Dr. Thomas Cristello,
Privacy Officer for Dr. Thomas Cristello D.C..

Signature of patient or legal representative

Signature of witness

Date: _____

Date: _____

Confidential Communications Request Form

I, _____, request confidential communication of my health information when my health information is disclosed on my behalf.

Please use the following address or manner in disclosing my health information to me.
(Please be as specific as possible.)

____ My initials here affirm that failure to disclose my health information in the non-conforming manner stated above could endanger me.

Patient Signature _____

Date _____

Printed Name and date of birth _____

Effective Date _____

Practice's Response to Request

____ Agrees to entire request.

____ Denies part of requested action: _____

____ Requires more complete/specific information to assess your request.

____ The practice cannot reasonably accommodate your request.

Signed _____

Date _____

Medical Record Amendment Request Form

I, _____, request that Dr. Thomas Cristello change/amend my medical record because:

(Explain what is to be changed/amended and why.)

For my medical record to be more complete/accurate, it should say:

Patient signature: _____

Printed name and date of birth: _____

Date of request: _____

Privacy Officer Action/Comments:

Action must be taken within 60 days of the receipt of the request

___ Request approved without change.

___ Request denied for the following reason:

___ Information is not part of your designated record set.

___ The information is accurate and complete.

___ Under HIPAA you are restricted from accessing or amending this information.

___ Practice requests a 30-day extension to respond due to: _____

Signature of Privacy Officer _____

On _____(date) _____(name) filed a statement of disagreement to the Practice's denial of their request for amendment dated _____. The Practice responds to this statement of disagreement as follows:

Signed by: _____ Date: _____

Patient Access to the Medical Record Request Form

I, _____, request access to my medical records for my personal inspection or by _____, my personal representative. (Please request date and time requested for record access)
Date _____ Time _____

OR

I, _____, request Dr. Thomas Cristello make copies of my medical records for my personal inspection. I understand that these records contain protected health information (PHI). I agree to be responsible for the cost of copying these records, including copying fees, labor, supplies, and postage (if applicable). The charge for this will be \$ 1 per page* and I will be charged a minimum of \$ 5. I agree to pay for this prior to the service being rendered.

Patient Signature _____
Patient Printed Name and Date of Birth _____

Date of request _____

Practice Response to Request (Must be within 60 days of receipt of request.)

- Grants all or part of your request _____
- Denies all or part of your request _____

_____ For the following reason: (Circle all that apply)

Not part of your designated record set; contains psychotherapy notes; information was compiled for civil, criminal or administrative actions; subject to CLIA; regards inmate at correctional institution; was created during research; is subject to Federal privacy act; was not created by this practice.

Patient may not appeal if denial is for any of the above reasons

- Denied at the discretion of the practice as the information may be harmful to the patient or a third party
- Requests a 30-day extension to respond due to _____

Dr. Thomas Cristello D.C.

**Restriction of Use or Disclosure of Protected Health Information (PHI)
Form**

I, _____, request that Dr. Thomas Cristello restrict the use or disclosure of my health information for payment or health care operations in the manner described here: (Please be specific)

I understand that Dr. Thomas Cristello is not required by law to accept my requested restrictions, but if the practice does, Dr. Thomas Cristello agrees to abide by the restrictions except in emergency situations.

I understand that either I or Dr. Thomas Cristello may terminate this restriction in writing at any time in the future.

Patient Signature: _____
Printed Name and date of birth: _____
Date: _____

Privacy Officer Comments:

- Accept this request.
- Reject this request. Reason: _____
- Patient contacted.

**HIPAA PRIVACY
BUSINESS ASSOCIATE ADDENDUM**

This Business Associate Addendum (this "Addendum") is entered into effective as of April 15, 2003, by and among Dr. Thomas Cristello D.C. (herein "Covered Entity") and _____, (herein "Business Associate") in order to comply with 45 C.F.R. §164.502(e) and §164.504(e), governing protected health information ("PHI") and business associates under the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191), 42 U.S.C. Section 1320d, et. seq., and regulations promulgated thereunder, as amended from time to time (statute and regulations hereafter collectively referred to as "HIPAA") [Covered Entity and Business Associate may be referred to herein individually as a "Party" or collectively as the "Parties"]. Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in HIPAA. This Addendum amends the terms and conditions of and is hereby incorporated as part of that certain Agreement between Covered Entity and Business Associate dated _____ and entitled _____ (the "Agreement") [this Addendum and the Agreement will be referred to hereinafter collectively as the "Agreement"].

STATEMENT OF AGREEMENT

§1. HIPAA Compliance and Agents. Business Associate hereby agrees to fully comply with the "Business Associate" requirements under HIPAA, including, without limitation, 45 C.F.R. §164.502(e) and §164.504(e), throughout the term of this Agreement. Further, Business Associate agrees that to the extent it has access to PHI, Business Associate will fully comply with the requirements of HIPAA and this Agreement with respect to such PHI; and, further, that every agent, employee, subsidiary, and affiliate of Business Associate to whom it provides PHI received from, or created or received by Business Associate on behalf of, Covered Entity will be required to fully comply with HIPAA, and will be bound by written agreement to the same restrictions, terms and conditions as set forth in this Agreement. If Covered Entity is required by HIPAA to maintain a Notice of Privacy Policies, Business Associate acknowledges that it has received a copy of such notice, read and understands its terms, conditions, and hereby agrees to the extent applicable, to comply and act in accordance with such Notice as it may be amended from time to time by Covered Entity.

§2. Use and Disclosure; Rights. Business Associate agrees that it shall not to use or disclose PHI except as permitted under this Agreement and HIPAA. Business Associate may use or disclose the PHI received or created by it, (a) to perform its obligations under this Agreement including without limitation _____

_____ in order to properly manage and administer its business, (b) to carry out its legal responsibilities if the disclosure is required by law, or (c) for data aggregation functions, as defined by HIPAA. If pursuant to subsections (a), (b), or (c) above, Business Associate discloses PHI to others, the Business Associate must obtain reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it is disclosed to the person and the person notifies Business Associate of any instances of which it is aware that the confidentiality of the information has been breached.

§3. Safeguards; Location. Business Associate agrees to develop, document, use, and keep current appropriate procedural, physical, and electronic safeguards, sufficient to comply with the requirements of HIPAA, to prevent any use or disclosure of PHI other than as permitted or required by this Agreement. Business Associate agrees to notify Covered Entity of the location of any PHI disclosed by Covered Entity or created by Business Associate on behalf of Covered Entity and held by or under the control of Business Associate or those to whom Business Associate has disclosed such PHI.

§4. Minimum Necessary. Business Associate will limit any use, disclosure, or request for use or disclosure to the minimum amount necessary to accomplish the intended purpose of the use, disclosure, or request in accordance with the requirements of HIPAA. Business Associate covenants that in all uses, disclosures, and requests it will include only the minimum amount of PHI necessary to accomplish the permitted or required use or disclosure as set forth by the agreement and in accordance with the requirements of HIPAA. Covered Entity may, pursuant to HIPAA, reasonably rely on any requested disclosure as the minimum necessary for the stated purpose when the information is requested by Business Associate. Business Associate acknowledges that if Business Associate is also a covered entity, as defined by HIPAA, Business Associate is required, independent of Business Associate's obligations under this Agreement, to comply with the HIPAA minimum necessary requirements when making any request for PHI from Covered Entity.

§5. Records; Covered Entity Access. Business Associate shall maintain such records of PHI received from, or created or received on behalf of, Covered Entity and shall document subsequent uses and disclosures, other than as for treatment, payment, or healthcare operations, pursuant to a valid authorization, or otherwise excepted from the accounting requirement under HIPAA, made by Business Associate as may be deemed necessary and appropriate in the sole discretion of Covered Entity. Business Associate shall provide the Covered Entity with reasonable access to examine and copy such records and documents of Business Associate during normal business hours.

§6. DHHS Access to Books, Records, and Other Information. Business Associate shall make available to DHHS its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Entity for purposes of determining the Covered Entity's or Business Associate's compliance with HIPAA. Business Associate agrees to fully cooperate in good faith with and to assist Covered Entity in complying with the requirements of HIPAA and any investigation of Covered Entity regarding compliance with HIPAA conducted by the U.S. Department of Health and Human Services ("DHHS"), Office of Civil Rights, or any other administrative or judicial body with jurisdiction, including, but not limited to, disclosing, providing access to or an accounting of any PHI as Covered Entity may request.

§7. Designated Record Set; Individual Access. Business Associate shall maintain a designated record set, as defined by HIPAA, for each individual patient for which it has PHI. In accordance with an individual's right to access to their own PHI under HIPAA and the individual's right to copy or append such records, Business Associate shall make available all PHI in that designated record set to Covered Entity, the individual to whom that information pertains or such individual's representative, upon a request by Covered Entity, the individual or such individual's representative.

§8. Accounting. Beginning April 14, 2003, Business Associate shall promptly make available to Covered Entity any PHI or any other information required to prepare, or assist in preparing, an accounting of disclosures in accordance with HIPAA. Business Associate agrees to document disclosures of PHI related to disclosures as would be required for Covered Entity to respond to a request for an accounting of disclosures. Business Associate must have this information and documentation available for the six (6) years preceding any request by such Covered Entity.

§9. Report of Improper Use or Disclosure. Business Associate shall immediately report to Covered Entity any information of which it becomes aware concerning any use or disclosure of PHI that is not permitted by this Agreement. This report shall identify the nature of the violating use or disclosure, the PHI used or disclosed, who made the violating use or received the disclosure, what corrective action Business Associate has or will take to prevent further violations, including any mitigation, and provide any other information Covered Entity requests.

§10. Amendment of and Access to PHI; Notification. Business Associate shall make available PHI for amendment and shall incorporate any amendments to PHI in accordance with HIPAA. Business Associate shall make reasonable efforts to notify persons, organizations, or other entities, including, but not limited to, other business associates, known by Business Associate to have received erroneous or incomplete PHI and who may have relied, or could foreseeably rely, on such PHI to the detriment of the individual. Business Associate must update this information as requested by Covered Entity.

§11. Individual Authorizations; Restrictions. Covered Entity will notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to with an individual or of any changes in or revocation of an authorization or other permission by an individual, to the extent that such restriction, change, or revocation may affect Business Associate's use or disclosure of PHI.

§12. Termination Rights; Mitigation. Business Associate acknowledges and agrees that Covered Entity shall have the right to terminate this Agreement in accordance with this §12 and §13 in the event Business Associate breaches or fails to comply with the requirements set forth in this Addendum. In addition, Covered Entity may immediately terminate the Agreement, if Covered Entity determines, in its reasonable discretion, that Business Associate has failed to comply with a material term of the Addendum required by HIPAA or is substantially not in compliance with the requirements of HIPAA. In addition to its obligations under Sections 9 and 10 of this agreement, Business Associate shall take any other reasonable actions available to it to mitigate any detrimental effects of such violation or failure to comply.

§13. Breach; Knowledge. If Covered Entity knows of a pattern of activity or practice of Business Associate that constitutes a breach or violation of Business Associate's obligations under this Addendum, Covered Entity and Business Associate shall take any steps reasonably necessary to cure such breach and make Business Associate comply, and, if such steps are unsuccessful, Covered Entity shall either (a) terminate this Agreement, if feasible, or (b) if cure and termination are not feasible, discontinue disclosure of PHI to Business Associate and report the breach or violation to DHHS. If Business Associate as a covered entity, defined by HIPAA, violates the terms and conditions of this Agreement or any other agreement in its capacity as a business associate of another covered entity, Business Associate will be, for purposes of §12 of this Addendum, substantially not in compliance with HIPAA.

§14. Electronic Standards and Code Sets Regulations. If Business Associate or any of its subcontractors or agents conducts in whole, or in part, electronic transactions on behalf of covered entity of the type covered by HIPAA any regulations promulgated pursuant thereto, including Standards for Electronic Transactions and Electronic Code Sets, Standards for Security, or others, Business Associate will, and will require any of its subcontractors or agents to comply with each applicable requirement of such regulations.

§15. Return of PHI. Business Associate agrees that upon termination of this Agreement, and if feasible, Business Associate shall, at its expense, (a) return or destroy all PHI received from, or created or received by Business Associate or any of Business Associate's subcontractors or agents on behalf of, Covered Entity that Business Associate or its subcontractors or agents maintain or control in any form or manner and retain no copies of such information or, (b) if such return or destruction is not feasible, immediately notify Covered Entity of the reasons return or destruction are not feasible, and extend indefinitely the protection of this Agreement to such PHI and limit further uses and disclosures to those purposes that make the return or destruction of the PHI not feasible.

§16. Indemnification. Business Associate will indemnify and hold harmless Covered Entity and any Covered Entity affiliate, officer, director, employee or agent in accordance with and to the fullest extent permitted by applicable law, including from and against any claim, cause of action, liability, damage, cost, or expense, including attorney's fees and court or proceeding costs, arising out of or in connection with any violation of this Agreement or the requirements of HIPAA by Business Associate or any of its subcontractors or agents or persons under Business Associate's control.

§17. Survival. All representations, covenants, and agreements in or under this Agreement or any other documents executed in connection with the transactions contemplated by this Agreement, shall survive the execution, delivery, and performance of this Agreement and such other documents. The respective rights and obligations of Business Associate under Section 15 of this Agreement shall survive termination or expiration of this Agreement.

§18. Further Assurances; Conflicts. Each Party shall in good faith execute, acknowledge or verify, and deliver any and all documents which may from time to time be reasonably requested by the other Party to carry out the purpose and intent of this Agreement. The terms and conditions of this Addendum will override and control any conflicting term or condition of the Service Agreement. All non-conflicting terms and conditions of the Service Agreement shall remain in full force and effect. Any ambiguity in this Addendum with respect to this Agreement shall be resolved in a manner that will permit Covered Entity to comply with HIPAA.

Acknowledged and agreed to by:

COVERED ENTITY

By _____
Print Name Dr. Thomas Cristello D.C.
Address: 9 E 19th St. 6th Floor
New York, NY 10003

_____ Date

BUSINESS ASSOCIATE

By _____
Print Name _____
Its _____
Address: _____

_____ Date

**SAMPLE BUSINESS ASSOCIATE AGREEMENT
SEE RELATED GUIDE FOR COMPLETION**

[1]

BUSINESS ASSOCIATE AGREEMENT

[2]

This Business Associate Agreement (this “Agreement”) is entered into effective as of [3], by and among [4] (herein “Covered Entity”) and [5] (herein “Business Associate”) in order to comply with 45 C.F.R. §164.502(e) and §164.504(e), governing protected health information (“PHI”) and business associates under the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191), 42 U.S.C. Section 1320d, et. seq., and regulations promulgated thereunder, as amended from time to time (statute and regulations hereafter collectively referred to as “HIPAA”) [Covered Entity and Business Associate may be referred to herein individually as a “Party” or collectively as the “Parties”].

STATEMENT OF AGREEMENT

§1. HIPAA Compliance and Agents. Business Associate hereby agrees to fully comply with the “Business Associate” requirements under HIPAA, throughout the term of this Agreement. Further, Business Associate agrees that to the extent it has access to PHI, Business Associate will fully comply with the requirements of HIPAA and this Agreement with respect to such PHI; and, further, that every agent, employee, subsidiary, and affiliate of Business Associate to whom it provides PHI received from, or created or received by Business Associate on behalf of, Covered Entity will be required to fully comply with HIPAA, and will be bound by written agreement to the same restrictions and terms and conditions as set forth in this Agreement.

§2. Use and Disclosure; Rights. Business Associate agrees that it shall not to use or disclose PHI except as permitted under this Agreement or as required by law. Business Associate acknowledges that this Agreement does not in any manner grant Business Associate any greater rights than Covered Entity enjoys, nor shall it be deemed to permit or authorize Business Associate to use or further disclose PHI in a manner that would otherwise violate the requirements of HIPAA if done by Covered Entity.

§3. Required or Permitted Uses. [6] Business Associate agrees that it is permitted to use or disclose PHI only: (a) upon obtaining the authorization of the patient to whom such information pertains in accordance with 45 C.F.R. §164.502(a)(1)(iv) and §164.508, (b) upon obtaining the consent of a patient to whom such information pertains, if the use or disclosure is for purposes of treatment, payment, or health care operations, in accordance with 45 C.F.R. §164.502(a)(1)(ii) and §164.506, or (c) without an authorization or consent, if in accordance with 45 C.F.R. §164.506, §164.510, §164.512, §164.514(e), §164.514(f), §164.514(g), or as otherwise permitted or required by agreement or law. [7]

§4. Safeguards; Location. Business Associate agrees to develop and use appropriate procedural, physical, and electronic safeguards to prevent misuse of PHI other than

as provided by this Agreement. Business Associate agrees to notify Covered Entity of the location of any PHI disclosed by Covered Entity or created by Business Associate on behalf of Covered Entity and held by or under the control of Business Associate or those to whom Business Associate has disclosed such PHI.

§5. Minimum Necessary. Business Associate must limit any use, disclosure, or request for use or disclosure to the minimum amount necessary to accomplish the intended purpose of the use, disclosure, or request in accordance with the requirements of HIPAA. Business Associate represents that all uses, disclosures, and requests it will make shall be the minimum necessary in accordance with HIPAA requirements. Covered Entity may, pursuant to HIPAA, reasonably rely on any requested disclosure as the minimum necessary for the stated purpose when the information is requested by Business Associate. Business Associate acknowledges that if Business Associate is also a covered entity, as defined by HIPAA, Business Associate is required, independent of Business Associate's obligations under this Agreement, to comply with the HIPAA minimum necessary requirements when making any request for PHI from Covered Entity.

§6. Records: Covered Entity Access. Business Associate shall maintain such records of PHI received from, or created or received on behalf of, Covered Entity and shall document subsequent uses and disclosures of such information by Business Associate as may be deemed necessary and appropriate in the sole discretion of Covered Entity. Business Associate shall provide the Covered Entity with reasonable access to examine and copy such records and documents of Business Associate during normal business hours. Business Associate agrees to fully cooperate in good faith with and to assist Covered Entity in complying with the requirements of HIPAA and any investigation of Covered Entity regarding compliance with HIPAA conducted by the U.S. Department of Health and Human Services ("DHHS"), Office of Civil Rights, or any other administrative or judicial body with jurisdiction.

§7. DHHS Access to Books, Records, and Other Information. Business Associate shall make available to DHHS its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Entity for purposes of determining the Covered Entity's or Business Associate's compliance with HIPAA.

§8. Designated Record Set: Individual Access. Business Associate shall maintain a designated record set, as defined by HIPAA, for each individual patient for which it has PHI. In accordance with an individual's right to access to their own PHI under HIPAA, Business Associate shall make available all PHI in that designated record set to the individual to whom that information pertains, or such individual's representative, all PHI in that designated record set, upon a request by such individual or such individual's representative.

§9. Accounting. Business Associate shall make available PHI or any other information required to provide, or assist in preparing, an accounting of disclosures in accordance with HIPAA.

§10. Report of Improper Use or Disclosure. Business Associate shall report to Covered Entity any information of which it becomes aware concerning any use or disclosure of PHI that is not provided for by this Agreement.

§11. Amendment of and Access to PHI; Notification. Business Associate shall make available PHI for amendment and shall incorporate any amendments to PHI accordingly. Business Associate shall make reasonable efforts to notify persons, organizations, or other entities, including other business associates, known by Business Associate to have received the erroneous or incomplete information and who may have relied, or could foreseeably rely, on such information to the detriment of the individual patient. Business Associate must update this information when notified by Covered Entity.

§12. Termination Rights. [8] Business Associate acknowledges and agrees that Covered Entity shall have the right to immediately terminate this Agreement in the event Business Associate fails to comply with HIPAA requirements concerning PHI and the above requirements. This Agreement authorizes Covered Entity to terminate the Agreement, if Covered Entity determines, in its sole discretion, that Business Associate has violated a material term of the Agreement required by HIPAA.

§13. Breach or Violation; Knowledge. If Covered Entity knows of a pattern of activity or practice of Business Associate that constitutes a material breach or violation of Business Associate's obligations under this Agreement, Covered Entity shall take any steps reasonably necessary to cure such breach or end such violation, and, if such steps are unsuccessful, shall either (a) terminate this Agreement, if feasible, pursuant to §12, or (b) if termination is not feasible, report the breach or violation to DHHS. If Business Associate as a covered entity, defined by HIPAA, violates the terms and conditions of this Agreement in its capacity as a business associate of another covered entity, Business Associate will be in noncompliance with the standards, implementation specifications, and requirements of HIPAA.

§14. Return of PHI. Business Associate agrees that upon termination of this Agreement, and if feasible, Business Associate shall (a) return or destroy all PHI received from, or created or received by Business Associate on behalf of, Covered Entity that Business Associate still maintains in any form and retain no copies of such information or, (b) if such return or destruction is not feasible, extend the protection of this Agreement to such PHI and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible.

§15. Notices. All notices and other communications under this Agreement to any Party shall be in writing and shall be deemed given when delivered personally, telecopied (which is confirmed) to that Party at the telecopy number for that Party set forth at the end of this Agreement, mailed by certified mail (return receipt requested) to that Party at the address for that Party set forth at the end of this Agreement (or at such other address for such Party as such Party shall have specified in a notice to the other Parties), or delivered to Federal Express, UPS, or any similar express delivery service for delivery to that Party at that address.

§16. Non-Waiver. No failure by any Party to insist upon strict compliance with any term or provision of this Agreement, to exercise any option, to enforce any right, or to seek any remedy upon any default of any other Party shall affect, or constitute a waiver of, any Party's right to insist upon such strict compliance, exercise that option, enforce that right, or seek that remedy with respect to that default or any prior, contemporaneous, or subsequent default. No custom or practice of the Parties at variance with any provision of this Agreement shall affect or constitute a waiver of, any Party's right to demand strict compliance with all provisions of this Agreement.

§17. Gender and Numbers; Headings. Where permitted by the context, each pronoun used in this Agreement includes the same pronoun in other genders and numbers, and each noun used in this Agreement includes the same noun in other numbers. The headings of the various sections of this Agreement are not part of the context of this Agreement, are merely labels to assist in locating such sections, and shall be ignored in construing this Agreement.

§18. Counterparts. This Agreement may be executed in multiple counterparts, each of which shall be deemed to be an original, but all of which taken together shall constitute one and the same Agreement.

§19. Entire Agreement. This Agreement constitutes the entire agreement and supersedes all prior agreements and understandings, bot written and oral, among the Parties with respect to the subject matter of this Agreement.

§20. Binding Effect. This Agreement shall be binding upon, inure to the benefit of and be enforceable by and against the Parties and their respective heirs, personal representatives, successors, and assigns. Neither this Agreement nor any of the rights, interests or obligations under this Agreement shall be transferred or assigned by Business Associate without the prior written consent of Covered Entity.

§21. Severability; Governing Law. With respect to any provision of this Agreement finally determined by a court of competent jurisdiction to be unenforceable, such court shall have jurisdiction to reform such provision so that it is enforceable to the maximum extent permitted by applicable law, and the Parties shall abide by such court's determination. In the event that any provision of this Agreement cannot be reformed, such provision shall be deemed to be severed from this Agreement, but every other provision of this Agreement shall remain in full force and effect. This Agreement shall be governed by and construed in accordance with the laws of the State of Ohio.

§22. Survival. All representations, covenants, and agreements in or under this Agreement or any other documents executed in connection with the transactions contemplated by this Agreement, shall survive the execution, delivery, and performance of this Agreement and such other documents.

§23. Further Assurances. Each Party shall execute, acknowledge or verify, and deliver any and all documents which may from time to time be reasonably requested by the other Party to carry out the purpose and intent of this Agreement.

Acknowledged and agreed to by:

[4]
[9]

Date

[5]
[10]

Date

Confidentiality and Non-Disclosure Agreement

I, _____, do affirm that I will not divulge MEDICAL DATA TO ANY UNAUTHORIZED PERSON FOR ANY REASON. Neither will I directly nor indirectly use, or allow the use of, Medical data for any purpose other than that directly associated with my official assigned duties. I understand that ALL PATIENT INFORMATION, including financial data, is strictly confidential.

Futhermore, I will not, either by direct action or by counsel, discuss, recommend, or suggest to any unauthorized person the nature or content of any Medical information.

Violation of confidentiality is cause for disciplinary action, including immediate dismissal.

I understand that signing this document does not preclude me from reporting instances of breach of confidentiality.

Signed _____ Date _____

GUIDE FOR COMPLETION OF SAMPLE
BUSINESS ASSOCIATE AGREEMENT

- [1] *If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of a business associate in 45 C.F.R. §160.103 to a covered entity, such covered entity may disclose PHI to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of 45 C.F.R. §164.504(e) contained within this Agreement, provided, the covered entity attempts in good faith to obtain satisfactory assurances as required by 45 C.F.R. §164.504(e)(3)(i) (where both parties are governmental entities, they execute a memorandum of understanding or other law, including regulations enacted by the covered entity that apply to the parties, accomplish the same objectives) and if the covered entity fails, it documents the attempt and the reasons for failure. See, 45 C.F.R. §164.504(3)(ii).*
- [2] *If both parties are governmental entities they may, in lieu of executing a business associate agreement, either, execute a “MEMORANDUM OF UNDERSTANDING”, or identify or enact regulations that are applicable to the covered entity and business associate that accomplish these same objectives. See, 45 C.F.R. §164.504(e)(3)(I).*
- [3] Effective date of Agreement.
- [4] Name of covered entity.
- [5] Name of business associate.
- [6] In addition to the restrictions in this Section, Covered Entity may further limit or restrict permitted uses or disclosures. See, 45 C.F.R. §164.504(e)(2)(i).
- [7] *[Optional provision]* In addition, Business Associate may use PHI received in its capacity as a business associate to Covered Entity, if necessary, for Business Associate’s proper management and administration of its business or to carry out its legal responsibilities.
[Optional provision] Business Associate may disclose the PHI received by it in its capacity as business associate of Covered Entity in order to properly manage and administer its business or to carry out its legal responsibilities if the disclosure is required by law or the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person and the person notifies Business Associate of any instances of which it is aware that the confidentiality of the information has been breached.
[Optional provision] Business Associate may provide data aggregation services relating to the health care operations of Covered Entity.
- [8] May omit “Termination Rights” if inconsistent with either party’s statutory obligations. See, 45 C.F.R. §164.504(e)(3)(iii).
- [9] Address and telephone/telecopy number for covered entity party to this Agreement.
- [10] Address and telephone/telecopy number for business associate party to this Agreement.

Sample (Chief) Privacy Officer Job Description

This document was created from the American Health Information Management Association (AHIMA) Web site (<http://www.ahima.org/infocenter/models/privacyofficer2001.htm>) and is provided here for your convenience.

Position Title: (Chief) Privacy Officer¹

Immediate Supervisor: Chief Executive Officer, Senior Executive, or Health Information Management (HIM) Department Head²

General Purpose: The privacy officer oversees all ongoing activities related to the development, implementation, maintenance of; and adherence to the organization's policies and procedures covering the privacy of; and access to, patient health information in compliance with federal and state laws and the healthcare organization's information privacy practices.

Responsibilities:

- Provides development guidance and assists in the identification, implementation, and maintenance of organization information privacy policies and procedures in coordination with organization management and administration, the Privacy Oversight Committee,³ and legal counsel.
- Works with organization senior management and corporate compliance officer to establish an organization-wide Privacy Oversight Committee.
- Serves in a leadership role for the Privacy Oversight Committee's activities.
- Performs initial and periodic information privacy risk assessments and conducts related ongoing compliance monitoring activities in coordination with the entity's other compliance and operational assessment functions.
- Works with legal counsel and management, key departments, and committees to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms, and information notices and materials reflecting current organization and legal practices and requirements.
- Oversees, directs, delivers, or ensures delivery of initial and privacy training and orientation to all employees, volunteers, medical and professional staff, contractors, alliances, business associates, and other appropriate third parties
- Participates in the development, implementation, and ongoing compliance monitoring of all trading partner and business associate agreements, to ensure all privacy concerns, requirements, and responsibilities are addressed.
- Establishes with management and operations a mechanism to track access to protected health information, within the purview of the organization and as required by law and to allow qualified individuals to review or receive a report on such activity.

- Works cooperatively with the HIM Director and other applicable organization units in overseeing patient rights to inspect, amend, and restrict access to protected health information when appropriate.
- Establishes and administers a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.
- Ensures compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, extended workforce, and for all business associates, in cooperation with Human Resources, the information security officer, administration, and legal counsel as applicable.
- Initiates, facilitates and promotes activities to foster information privacy awareness within the organization and related entities.
- Serves as a member of; or liaison to, the organization's IRB or Privacy Committee,⁴ should one exist. Also serves as the information privacy liaison for users of clinical and administrative systems.
- Reviews all system-related information security plans throughout the organization'
- s network to ensure alignment between security and privacy practices, and acts as a liaison to the information systems department.
- Works with all organization personnel involved with any aspect of release of protected health information, to ensure full coordination and cooperation under the organization's policies and procedures and legal requirements
- Maintains current knowledge of applicable federal and state privacy laws and accreditation standards, and monitors advancements in information privacy technologies to ensure organizational adaptation and compliance.
- Serves as information privacy consultant to the organization for all departments and appropriate entities.
- Cooperates with the Office of Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.
- Works with organization administration, legal counsel, and other related parties to represent the organization's information privacy interests with external parties (state or local government bodies) who undertake to adopt or amend privacy legislation, regulation, or standard.

Qualifications:

- Certification as an RHIA or RHIT with education and experience relative to the size and scope of the organization.
- Knowledge and experience in information privacy laws, access, release of information, and release control technologies.
- Knowledge in and the ability to apply the principles of HIM, project management, and change management.
- Demonstrated organization, facilitation) communication, and presentation skills.
- This description is intended to serve as a scalable framework for organizations in development of a position description for the privacy officer.

Notes

1. The title for this position will vary from organization to organization, and may not be the primary title of the individual serving in the position. “Chief” would most likely refer to very large integrated delivery systems. The term “privacy officer” is specifically mention in the HIPAA Privacy Regulation.
2. Again, the supervisor for this position will vary depending on the institution and its size. Since many of the functions are already inherent in the Health Information or Medical Records Department or function, many organizations may elect to keep this function in that department.
3. The “Privacy Oversight Committee” described here is a recommendation of AHIMA, and should not be considered the same as the “Privacy Committee” described in the HIPAA privacy regulation. A privacy oversight committee could include representation from the organization’s senior administration, in addition to departments and individuals who can lend an organization-wide perspective to privacy implementation and compliance.
4. Not all organizations will have an Institutional Review Board (IRB) or Privacy Committee for oversight of research activities. However, should such bodies be present or require establishment under HJPAA or other federal or state requirements, the privacy officer will need to work with this group(s) to ensure authorizations and awareness are established where needed or required.

Copyright © 2001 American Health Information Management Association. All rights reserved. All contents, including images and graphics, on this Web site are copyrighted by AHIMA unless otherwise noted. You must obtain permission to reproduce any information, graphics, or images from this site. For permission, contact media@ahima.org.