

APPLIED DIAGNOSTICS

**PRIVACY AND SECURITY
POLICY AND PROCEDURE MANUAL**

APPLIED DIAGNOSTICS
PRIVACY AND SECURITY
POLICIES AND PROCEDURES

Applied Diagnostics provides a broad spectrum esoteric testing laboratory specializing in Flow Cytometry, Immunohistochemistry, and Molecular Pathology. Applied Diagnostics provides laboratory services only pursuant to written orders from a physician. As an indirect provider under the Health Insurance Portability and Accountability Act (“HIPAA”), and the regulations promulgated thereunder, Applied Diagnostics does not maintain a designated record set as that term is defined under HIPAA. Therefore, patient requests to access, receive copies of, or to amend medical records should be made to the referring physician. As an indirect provider, Applied Diagnostics has adopted the following privacy and security policies and procedures:

	<u>Page</u>
1. PRIVACY PRACTICES OVERVIEW	1
2. AUTHORIZATION POLICY	3
3. PATIENT AUTHORIZATION TO USE OR DISCLOSE	5
4. NOTICE OF PRIVACY PRACTICES	7
5. COMPLAINT POLICY	10
6. COMPLAINT FORM	12
7. POLICY FOR BUSINESS ASSOCIATES	13

1. PRIVACY PRACTICES OVERVIEW

PURPOSE:

Applied Diagnostics is committed to compliance with all federal and state laws that pertain to any aspect of its laboratory practices and business procedures. In particular, privacy and security rules relating to the Health Insurance Portability and Accountability Act (“HIPAA”), along with related state laws, are integral to matters of privacy, medical records, the confidentiality of communications, and other topics addressed throughout this policy and procedure manual.

POLICY:

The HIPAA Privacy Rule applies to all Protected Health Information (“PHI”) in Applied Diagnostics’ practice, including information stored and transmitted electronically paper records, and oral communications. PHI includes any information as it relates to the past, present, or future physical or mental health condition of any of our patients; any treatment they received; and health care payment information.

In keeping with HIPAA compliance, Applied Diagnostics has appointed a Privacy/Security Officer to continually evaluate our privacy practices, train our staff about privacy issues, supervise the sharing of information with third parties, and address any complaints from patients, their friends, and loved ones, staff, other providers, or members of the community. See *Privacy/Security Officer* policy in this Chapter.

All staff members will be trained on these policies and procedures, which will help to keep our practice in compliance with both state and federal law. The Privacy/Security Officer is responsible for both the training of staff, as well as continual review and amendment of this manual as necessary.

Applied Diagnostics does not see any patient in our labs. Therefore, a *Notice of Privacy Practices* (“NPP”) is available to Applied Diagnostic patients on our website. The NPP provides patients with an understanding of how their PHI is stored, used, and shared beyond this practice, and notifies them of their rights under HIPAA. Please note that Applied Diagnostics does not maintain a designated patient record. The record that we maintain is limited to the physician’s order, the results of the lab test, and the costs of the tests performed by Applied Diagnostics. A copy of each of these documents is provided to the ordering physician. Requests related to patient medical records should be addressed directly to the ordering physician(s). Under all circumstances, when PHI must be communicated either within this office or to a third party, only the amount of information that is minimally necessary to accomplish the appropriate purpose will be divulged. The Privacy/Security Officer is responsible for establishing criteria on what information is minimally necessary for recurring situations. Unusual or unique needs to share information, such as subpoenas from attorneys for lab reports or billing information will be conveyed to the Privacy Officer for approval. See *Privacy/Security Officer* policy in this Chapter.

PHI that is shared as part of delivering quality patient care will not be scrutinized under the minimally necessary guidelines and any information necessary for quality care will be shared appropriately.

Only those documents that are immediately necessary to provide laboratory services are to be kept at workstations.

2. AUTHORIZATION POLICY

PURPOSE:

To secure appropriate authorization from patients for purposes other than treatment, payment, and health care operations.

POLICY:

For purposes other than treatment, payment, and health care operations, Applied Diagnostics will obtain patient authorization prior to making uses and disclosures that are not otherwise permitted or required under the HIPAA privacy regulations. Prior to making any disclosure, Applied Diagnostics shall verify the identity and authority of any person requesting Protected Health Information (“PHI”).

CORE ELEMENTS

The authorization shall be written in plain language and include the following elements:

- A specific description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
- The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
- The name or other specific identification of the person(s), or class of persons, to whom Applied Diagnostics may make the requested use or disclosure;
- A description of each purpose of the requested use or disclosure;
- An expiration date or event that relates to the patient or the purpose of the use or disclosure;
- Signature of the patient and date;
- If a personal representative of the patient signs the authorization, the representative’s authority to act for the patient;
- A statement that the patient may revoke the authorization in writing, except to the extent that action has been taken in reliance on the authorization;
- Instructions explaining how the patient may revoke the authorization and the exceptions to the right to revoke;
- A statement that the information used or disclosed may be subject to re-disclosure by the recipient and no longer protected by the Privacy Rule; and

- A statement that treatment and payment for benefits will not be conditioned upon the patient's signing the authorization.

► Applied Diagnostics will supply a copy of the signed authorization to the patient.

AN AUTHORIZATION SIGNED BY A PATIENT SHALL NOT BE EFFECTIVE IF:

- The expiration date passed or the expiration event is known by Applied Diagnostics to have occurred;
- The authorization has not been filled out completely;
- Applied Diagnostics is aware that the authorization has been revoked;
- The authorization violates the conditions for allowable use of a compound or combined authorization;
- Applied Diagnostics knows that the information on the authorization is false; or
- The authorization lacks a required element.

Patients may revoke an authorization AT ANY POINT IN TIME. A revocation must be made in writing and signed by the same person who signed the authorization. The Privacy Officer must receive the written revocation and determine whether it is complete. If complete, the Privacy Officer shall document such revocation in the patient's medical record. If incomplete, the patient shall be asked to submit an adequate revocation.

A patient's revocation is not effective to the extent that Applied Diagnostics has already taken action in reliance thereupon; or The Privacy Officer shall retain the signed authorization and revocation for a period of seven years (7) from the anniversary of the last date of treatment by Applied Diagnostics. If the patient is a minor, Applied Diagnostics shall retain the signed authorization and revocation related to minors until the patient reaches 21 or for seven (7) years from the date of last treatment, whichever is longer.

**3. PATIENT AUTHORIZATION TO USE OR DISCLOSE
PROTECTED HEALTH INFORMATION**

I understand Applied Diagnostics is authorized by me to use or disclose my Protected Health Information for a purpose other than treatment, payment, or health care operations. I have read this authorization and understand what information will be used or disclosed, who may use and disclose the information, and the recipient(s) of that information. I understand that treatment, payment, enrollment, or eligibility for benefits may not be conditioned upon me signing this authorization.

I specifically authorize Applied Diagnostics or its designated employee(s) to disclose my Protected Health Information as described on this form to the recipients listed below. I understand that when the information is used or disclosed pursuant to this authorization, it may be subject to re-disclosure by the recipient and may no longer be protected by state or federal privacy regulations. I further understand that I retain the right to revoke this authorization, if done so according to the steps set forth below.

Description of the information to be used or disclosed (*check all that apply*):

My entire laboratory record
(NOTE: This requires an explanation of why it is necessary to disclose the entire record)

My demographic information (*check all that apply*):

Name Address State/Zip Code only Telephone
 Age Gender Race Other:_____

Medical Data/Information as related to:

Specific condition(s):_____

Specific laboratory service(s):_____

Specific laboratory result(s):_____

Billing information:_____

Other:_____

Name(s) or class of person(s) to whom Applied Diagnostics may disclose my Protected Health Information:

Purpose(s) for disclosure of the information:

(*Note: If the patient is requesting disclosure, the purpose may simply state: "Patient is requesting disclosure."*)

I have a right to revoke this authorization in writing, except to the extent that action has been taken in reliance on this authorization. In order for the revocation of this authorization to be effective, Applied Diagnostics must receive the revocation in writing, and the revocation must include:

- My name, address, and patient number, if applicable,
- The effective date of this authorization, and the recipients of the Protected Health Information according to this authorization,
- My desire to revoke this authorization, and
- The date of the revocation, and my signature.

Applied Diagnostics will accept written revocations of this authorization via:

- Certified U.S. mail
- Facsimile at this number: _____

ALL revocations must be sent to Applied Diagnostics to the attention of the Privacy Officer, and are not effective until received by the Privacy Officer.

This authorization shall expire on (specific date or specific event) . After this date, Applied Diagnostics can no longer use or disclose my Protected Health Information for the above purposes without first obtaining a new authorization form.

I fully understand and accept the terms of this authorization.

Signature of Patient or Patient's Representative

Date

Name of Patient

Patient Identification Number

Name of Representative (if applicable)

Description of Representative's
Authority to act for Patient

FOR OFFICE USE ONLY

Authorization added to the patient's medical record on _____.

Authorization verified by _____ on _____.

Patient has been provided with a copy of the signed authorization.

4. NOTICE OF PRIVACY PRACTICES

Effective Date: May 2008

THIS NOTICE OF PRIVACY PRACTICES (“NPP”) DESCRIBES HOW MEDICAL INFORMATION RELATED TO LABORATORY SERVICES PROVIDED TO YOU MAY BE USED AND DISCLOSED, AND HOW YOU MAY RETRIEVE ACCESS TO THIS INFORMATION. PLEASE REVIEW THIS NPP CAREFULLY.

This Notice describes how we may use and disclose your Protected Health Information (“PHI”) for purposes of treatment, payment and health care operations, and for other purposes that are permitted or required by law. PHI is defined as demographic and individually identifiable health information about you that will or may identify you and relates to your past, present or future physical, mental health or condition, and that involves providing health care services or health care payment.

We are required by law to:

1. Maintain the privacy of your PHI.
2. Provide you with this notice of our Privacy Policy.
3. Abide by the terms of this Policy.

We reserve the right to make changes to this NPP at any time, without notice. Any revised NPP will be posted on our website at www.

According to federal law, providers such as Applied Diagnostics, have the right to use and disclose your PHI for the purpose of treatment, payment and health care operations without authorization from you. However, the law requires providers to obtain your authorization to release your PHI for any reason other than treatment, payment or healthcare operations with certain exceptions (*See* WHEN DISCLOSURE OF YOUR INFORMATION IS REQUIRED).

HOW YOUR MEDICAL INFORMATION IS USED

(1) Internal Uses

We may use your PHI within Applied Diagnostics (1) to provide your ordering physician information about the services and products he/she requests, (2) to assist with questions about our services, billing, payment methods or use of our web site, (3) to process or collect payments made in connection with our services on your behalf, and (4) to evaluate our services and products.

(2) Disclosure of PHI to Third Parties

We will not give, sell, rent, loan or otherwise disclose any PHI to any third party, unless (1) you have authorized us to do so, (2) we are legally required to do so, for example, in

response to a subpoena, court order or other legal proceeding, and/or (3) it is necessary to do so in order to protect and defend the rights or property of Applied Diagnostics. We contractually require third-party vendors and contractors to comply with strict standards regarding security and confidentiality.

We also may share aggregate, non-personal information with unaffiliated third parties. This aggregate information does not contain any personal information about any specific patient.

(3) Specific Examples of How Your PHI May Be Used for Treatment and/or Payment of Healthcare Operations

- We will/may disclose your PHI to your ordering physician and any with other provider for treatment (e.g., specialists who treat you or a physician to whom the ordering physician refers you to).
- We will/may submit claims to you or your insurance company containing PHI.
- We may contact your ordering physician/specialist to discuss treatment alternatives or other health related benefits that may be of interest to you or them.
- We will/may use your PHI for healthcare operations such as assessing quality of Applied Diagnostics' services.

Other healthcare operations include reviewing the competence or qualifications and accrediting/licensing of healthcare professionals and plans, evaluating health care professionals performance, training future health care professionals, insurance activities relating to the renewal of a contract for insurance, conducting or arranging for medical review and auditing services, compiling and analyzing information in anticipation of or for use in civil or criminal legal proceedings, general administrative and business functions necessary for the entity to remain a viable business.

BUSINESS ASSOCIATES

Business Associates are entities or individuals we contract with to perform various activities for our business, such as billing or management services. Applied Diagnostics will contractually require its business associates to follow the same confidentiality laws and rules required of our company, health care providers or health plans.

LINKS TO OTHER SITES

We want to provide users of our website with information, services and products that are valuable to them. Featured programs and other site content on Applied Diagnostics website may link our users to third party sites. Applied Diagnostics does not control and is not responsible for the privacy policies or practices of any third-party site. If you link to third party sites from Applied Diagnostics, we encourage you to consult the privacy policy of each site you visit.

COOKIES (Collection of Non-Personal Information)

In order to provide better service, Applied Diagnostics may use a “cookie.” Cookies are small files browsers placed on computer hard drives. We may use cookies to retrieve certain information previously provided by your ordering physician. We also use this information to monitor how many people are using our site and for what reason(s).

WHEN DISCLOSURE OF YOUR INFORMATION IS REQUIRED

Please note that the law requires certain information to be disclosed under specific circumstances, including but not limited to disclosures to a public health authority or federal/state entity that is authorized by law to collect or receive such information. An example of a state entity is the Texas Department of Health Care Services, which is authorized to receive a variety of information concerning different health conditions. Also, court orders may compel the disclosure of confidential health information in the context of a lawsuit or administrative proceeding.

A SUMMARY OF YOUR RIGHTS:

- When your physician orders a lab test from us on your behalf, you have the right to receive and read this Policy.
- You have the right to inspect and copy your PHI from your treating physician, as permitted by law.
- You have the right to request amendments to your PHI from your treating physician.
- You have the right to an accounting of all entities that obtained information unrelated to treatment, payment or healthcare operations without your authorization.
- You have the right to ask questions and to receive answers.
- Refusal to sign an authorization form will not be used to deny your treatment.
- If you sign an authorization and change your mind, you may revoke your authorization, except to the extent that we have relied on the authorization.
- You have a right to contact our Privacy Officer to request additional information or ask questions. You may mail your question to:

Privacy Officer
Applied Diagnostics
1140 Business Center Dr.
Suite 370
Houston, TX 77043

or email it to: info@applieddiagnostics.com

The Privacy Officer may also be reached at 866-765-4133 or 713-271-4133

5. COMPLAINT POLICY

PURPOSE:

To implement a procedure for receiving, documenting, and taking appropriate action with respect to privacy or security complaints.

POLICY:

All Privacy and Security Complaints must be submitted to the Privacy/Security Officer or his/her designees. The Privacy/Security Officer may be reached at 866-765-4133 and at the following address.

Privacy Officer
Applied Diagnostics
1140 Business Center Dr.
Suite 370
Houston, TX 77043

Privacy and/or Security Complaints must include a statement that describes the basis of the complaint.

The Privacy/Security Officer will determine what healthcare information the complainant claims was misused or improperly disclosed. If the healthcare information at issue were created or maintained by a business associate, the complaint will be forwarded to the business associate.

RESPONSIBILITIES OF THE PRIVACY/SECURITY OFFICER:

The Privacy/Security Officer shall determine:

1. Whether there has been a violation of the privacy or security regulations or Applied Diagnostics' policies.
2. What, if any, internal privacy/security practices need to be changed.
3. What, if any, additional policies need to be developed.
4. What additional training will be provided to the person who violated the privacy or security regulations or policies.

If the Privacy/Security Officer determines that a violation has occurred, he/she in consultation with the Board of Directors determines what appropriate sanctions must be taken against the employee.

The Privacy/Security Officer shall document all complaints received by Applied Diagnostics and the action taken in response to the complaint. Such documentation will be retained in written or

electronic form in the patient's record for seven (7) years from the date of creation or the last effective date, whichever is later.

6. COMPLAINT FORM

Patient Name: _____

Date of Birth: _____ Patient Identification Number: _____

Patient Address: _____

Please describe the basis of your complaint.

On what date did this event occur? _____

What health care information do you allege was illegally used and/or disclosed?

Signature of patient or legal representative: _____

Date: _____

7. POLICY FOR BUSINESS ASSOCIATES

PURPOSE:

To establish procedures so that Business Associates will NOT use or disclose Protected Health Information (“PHI”) other than as provided by the business associate contract.

DEFINITION:

A “Business Associate” is a person who performs a function, involving individual health information, for Applied Diagnostics other than as a member of the workforce.

POLICY:

Privacy/Security Officer must obtain satisfactory assurances that the business associate will appropriately safeguard PHI.

The business associate contract must establish the permitted and required uses and disclosures of PHI by the business associate. Applied Diagnostics may not authorize business associates to use or further disclose PHI that would violate Applied Diagnostics own duties.

A business associate may use and disclose PHI for the proper management and administration of the business associate and to provide data aggregation services relating to the health care operations of Applied Diagnostics.

All business associates must contractually agree in writing:

- Not to use or further disclose the information other than as permitted or required by the applicable service contract (“contract”) or as required by law;
- Use appropriate safeguards to prevent use or disclosure of the information other than as provided by the contract;
- Report to Applied Diagnostics any use or disclosure of the information not provided for by its contract of which it becomes aware;
- That agents and subcontractors agree to the same restrictions and conditions that apply to the business associate in respect to PHI the agent or subcontractor receives or creates on the behalf of the business associate;
- Make available PHI in accordance with the requirements imposed on Applied Diagnostics;
- Make available PHI for amendment and incorporate any amendments to PHI in accordance with the same requirements imposed on Applied Diagnostics;

- Make available the information required to provide an accounting of disclosures in accordance with the same requirements imposed on Applied Diagnostics; and
- Provide the Secretary of HHS and Applied Diagnostics with access to all internal practices and records relating to PHI in order to determine whether Applied Diagnostics is in compliance.

At termination, the business associate must:

- Return or destroy all PHI;
- Not retain copies of the information; and
- If the business associate cannot return or destroy the PHI, extend the protections of the contract to the information and limit further disclosures.

If it is determined that the business associate has violated a material term of the contract, the contract must authorize termination of the relationship.

Applied Diagnostics must take reasonable steps to cure Business Associate breaches or violations that are known to Applied Diagnostics. Sanctions may be imposed against Applied Diagnostics by the United States Office of Civil Right, the Department of Justice, the Texas Attorney General's Office, or the Center for Medicaid and Medicare as a result of a failure by Applied Diagnostics to cure any action in which there was knowledge of a pattern of activity or practice conducted by the business associate that constituted a material breach or violation of the business associate's obligations under the contract. If steps to cure a business associate's violation of the Privacy or Security rules are unsuccessful, Applied Diagnostics must:

- Terminate the contract, if feasible; or
- If termination is not feasible, report the problem to the United States Secretary of Health and Human Services; and
- Seek a protective order if appropriate.

Business associate agreements are not necessary:

- With respect to disclosures of PHI to a health care provider concerning the treatment of the individual; or
- With respect to disclosures to health plans for payment purposes.