HIPAA Privacy Compliance Manual

1/30/16

HOW TO USE THIS MANUAL

This HIPAA Compliance Manual is an interactive workbook to help you comply with the HIPAA Privacy Rule. (45 CFR 164.500 et. seq.)

We intend for you to download the electronic version of this Workbook so that you have a paper copy to work with. You may wish to put the Workbook in a three ring binder for ease of use. In this format, more than one person in your office can be working on the various sections of the Workbook simultaneously. It will also allow you to insert additional pages if you need to in your compliance effort, or to store other HIPAA materials that you may have in a single place.

When you use this Workbook, you will be asked questions about your current privacy practices. Based upon your answers, you will be able to decide if a particular HIPAA privacy requirement applies to you or not. If it does, the Workbook will help you determine what specific action steps you need to take in order to comply. You will have model policies, procedures, and forms to work with to get you started.

When you finish using this Workbook, you should have developed a series of new or revised policies and procedures for privacy protections in your office. It will then be up to you to train your work force in how to use these, and to enforce them. When you have appropriate written policies and procedures, appropriate forms and contracts, and a work force that is trained and ready to implement them, you can then consider yourself to be compliant with HIPAA's Privacy Rule.

HIPAA compliance will take effort and possibly some funds. The Workbook will help you organize yourself and establish a budget that you can live with. You don't need to spend thousands of dollars to become HIPAA compliant if you use your existing resources and personnel wisely.

As you know, HIPAA is a federal law. Your own state may already have laws relating to the privacy of health information. This Workbook explains how these state laws will relate to HIPAA. You may have to comply with both an existing state law and the new HIPAA requirements. Sometimes the state law will "trump" HIPAA, and you will only have to comply with the existing state law. Because the laws in states vary, this Workbook cannot give you detailed information on how to satisfy your state laws. You are advised to consult your own attorney or state association for assistance.

Similarly, this Workbook cannot presume to know how each doctor's professional practice is set up. The Workbook provides you with general information; you will need to tailor it to your own practice.

This Workbook does not address HIPAA's electronic data interchange (EDI) rules, or the proposed security rules.

Finally, this Workbook is not legal advice. It is provided as an informational tool to assist you in becoming compliant with HIPAA. Nothing in this Workbook is intended to create any attorney-client relationship between you and either NYSDA or NYSDA's legal counsel. For legal advice, you are advised to consult your own private attorney.

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TITLE **CHART #**

Completed _____ Date _____

IS YOUR PRACTICE SUBJECT TO HIPAA?

_____

Signature of responsible person

Assessment Question	Yes	No	Comments
1. Do you furnish, bill or receive payment for health care in the normal course of business?	Go on to question 2.	You are not affected by HIPAA unless you are a "health plan" or a "health care clearinghouse."	Dentists always furnish health care.
2. Do you conduct (either directly or through a contracted organization like a billing company) any of the following health care financial or administrative transactions: • health care claims or equivalent encounter information. • health care payment and remittance advice. • coordination of benefits. • health care claim status. • enrollment and disenrollment in a health plan. • eligibility for a health plan. • health plan premium payments. • referral certification and authorization. • first report of injury. • health claims attachments.	Go on to question 3.	You are not affected by HIPAA.	1. Read the definitions on the accompanying page carefully before answering the questions. HIPAA uses very specific meanings for its financial or administrative transactions. 2. You cannot avoid HIPAA by contracting with third parties to conduct any of these transactions on your behalf. See charts 20-21 for more information about using contracted service providers.
3. Do you conduct any of these transactions using electronic media?	You are affected by HIPAA.	You are not affected by HIPAA.	1. Read the definitions on the accompanying page carefully before answering this question. HIPAA uses a very specific meaning for what is electronic media. 2. The following is not considered electronic media: • Using a word processor to prepare bills printed on paper. • Using a standard fax machine (distinguish from computer generated faxes).

Question 1 Definitions: "Health care" means care, services, or supplies related to the health of an individual. It includes, but is not limited to, the following:
(1) preventive, diagnostic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
(2) sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription. See 45 C.F.R. 160.103

Question 2 Definitions: 45 C.F.R. 162.1101: Health care claims or equivalent encounter information transaction is either of the following:
(a) A request to obtain payment, and necessary accompanying information, from a health care provider to a health plan, for health care.
(b) If there is no direct claim, because the reimbursement contract is based on a mechanism other than charges or reimbursement rates for specific services, the transaction is the transmission of encounter information for the purpose of reporting health care.
45 C.F.R. 162.1201: The eligibility for a health plan transaction is the transmission of either of the following:
(a) An inquiry from a health care provider to a health plan, or from one health plan to another health plan, to obtain any of the following information about a benefit plan for an enrollee: (1) eligibility to receive health care under the health plan. (2) coverage of health care under the health plan. (3) benefits associated with the benefit plan.
(b) A response from a health plan to a health care provider's (or another health plan's) inquiry described in paragraph (a) of this section.
45 C.F.R. 162.1301: The referral certification and authorization transaction is any of the following transmissions:
(a) A request for the review of health care to obtain an authorization for the health care; (b) A request to obtain authorization for referring an individual to another health care provider; OR (c) A response to a request described in paragraph (a) or paragraph (b) of this section.
45 C.F.R. 162.1401: A health care claim status transaction is the transmission of either of the following:
(a) An inquiry to determine the status of a health care claim; OR (b) A response about the status of a health care claim.
45 C.F.R. 162.1501: The enrollment and disenrollment in a health plan transaction is the transmission of subscriber enrollment information to a health plan to establish or terminate insurance coverage.
45 C.F.R. 162.1601: The health care payment and remittance advice transaction is the transmission of either of the following for health care:
(a) The transmission of any of the following from a health plan to a health care provider's financial institution: (1) payment. (2) information about the transfer of funds. (3) payment processing information.
(b) The transmission of either of the following from a health plan to a health care provider: (1) explanation of benefits. (2) remittance advice.
45 C.F.R. 162.1701: The health plan premium payment transaction is the transmission of any of the following from the entity that is arranging for the provision of health care or is providing health care coverage payments for an individual to a health plan:
(a) Payment
(b) Information about the transfer of funds.
(c) Detailed remittance information about individuals for whom premiums are being paid.
(d) Payment processing information to transmit health care premium payments including any of the following: (1) payroll deductions. (2) other group premium payments. (3) associated group premium payment information.
45 C.F.R. 162.1801: The coordination of benefits transaction is the transmission from any entity to a health plan for the purpose of determining the relative payment responsibilities of the health plan, of either of the following for health care: (a) Claims or (b) Payment information.

Question 3 Definitions: Using electronic media, as that term is defined at 45 C.F.R. 162.103. It includes transmissions over the Internet (wide-open), Extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, and private networks, and those transmissions that are physically moved from one location to another using magnetic tape, disk, or CD media.

Completed _____ Date _____

WILL YOU HAVE TO BILL MEDICARE ELECTRONICALLY?

_____

Signature of responsible person

Assessment Question	Definitions	Answers and Instructions	Comments
1. Do you provide services for which you presently bill Medicare?		If yes, go to question 3. If no, go to question 2.	
2. Do you plan to provide services for which you bill Medicare on or after October 16, 2003?		If yes, go to question 3. If no, skip the remainder of this chart. Your relationship with Medicare is not relevant to whether you are affected by HIPAA.	
3. How many "full time equivalent" employees do you have?	One "full time equivalent" employee is any combination of people who collectively work 2080 hours per year. If one person works all these hours, this one person is one FTE. If two people each work half time (e.g. 1040 hours per year each), together they make up one FTE.	1. If ten or more, go to question 4. 2. If fewer than ten, skip the remainder of this chart. You do not have to bill Medicare electronically, even after October 16, 2003, when larger practitioners will. If you bill other payors electronically, or conduct any of the other HIPAA transactions in electronic form, you are nonetheless subject to HIPAA. If not, then you are not subject to HIPAA.	1. DHHS is preparing regulations to implement the Medicare electronic billing mandate of the Administrative Simplification Compliance Act of 2001, including the exception for "small practitioners" – e.g. practitioners having fewer than ten FTEs. These regulations have not been published in even proposed form as of the publication of this HIPAA compliance manual. When published, these regulations may affect the analysis in this chart.

WILL YOU HAVE TO BILL MEDICARE ELECTRONICALLY?

Assessment Question	Definitions	Answers and Instructions	Comments
4. Do you currently bill Medicare electronically?		1. If yes: After October 16, 2003, Medicare will only pay claims that are submitted electronically. Accordingly, as a practical matter, your current electronic billing practices will become mandatory as of that date. Because you use electronic media to submit claims, you are subject to HIPAA. 2. If no: After October 16, 2003, Medicare will no longer pay your claims in hard copy form. Accordingly, if you wish to be paid by Medicare after that date, you will need to submit claims to Medicare in electronic form, using HIPAA standard transactions. Because you will be required to submit bills electronically to Medicare, you will be subject to HIPAA privacy rules whether or not you use electronic media to conduct any of the other HIPAA transactions.	

Completed _____ Date _____

DOES THE WAY THAT YOUR BUSINESS IS ORGANIZED AFFECT HOW YOU COMPLY WITH HIPAA?

_____

Signature of responsible person

Assessment Question	Yes/No	Comments	Action Steps
1. Do you practice in a clinically integrated care setting with other professionals who are not legally affiliated with you ? • Example: a multi-specialty dental clinic or a dental clinic in a hospital.	If yes, you practice in what HIPAA calls an "organized health care arrangement." (See definitions accompanying this chart.) Organized health care arrangements can issue a joint notice of privacy practices (See chart 14) and can freely share PHI among participants in the organized health care arrangement for joint business. If no, go to question 2.	1. Some commentators on HIPAA have expressed concern that there may be adverse "spillover" effects of operating as an organized health care arrangement, such as exposure to liability for the actions of the other participants in the arrangement. DHHS downplays this concern, and no consensus exists amongst commentators. You are advised to consult your own attorney or HIPAA advisor on the pros and cons of operating as an organized health care arrangement.	If you operate in an organized health care arrangement, develop a joint notice of privacy practices, if desired.
2. Do you openly join with other health care professionals to share certain activities, including at least one of the following: • Utilization review. • Quality assessment and improvement. • Payment, if financial risk is shared.	If yes, you practice in what HIPAA calls an "organized health care arrangement." (See definitions accompanying this chart.) Organized health care arrangements can issue a joint notice of privacy practices (see chart 14), and can freely share PHI among participants in the organized health care arrangement for joint business. If no, go to question 3.	1. Some commentators on HIPAA have expressed concern that there may be adverse "spillover" effects of operating as an organized health care arrangement, such as exposure to liability for the actions of the other participants in the arrangement. DHHS downplays this concern, and no consensus exists amongst commentators. You are advised to consult your own attorney or HIPAA advisor on the pros and cons of operating as an organized health care arrangement.	If you operate in an organized health care arrangement, develop a joint notice of privacy practices, if desired.

DOES THE WAY THAT YOUR BUSINESS IS ORGANIZED AFFECT HOW YOU COMPLY WITH HIPAA

Assessment Question	Yes/No	Comments	Action Steps
3. Do you operate two or more separate legal entities (like corporations) that are connected by common ownership or control?	If yes, then you can elect to be considered an "affiliated covered entity" for HIPAA purposes. (See definitions accompanying this chart.) Affiliated covered entities must use a joint notice of privacy practices, and must satisfy all HIPAA requirements as a single unit. However, members of the affiliated covered entity may freely share PHI amongst themselves. If no, go to question 4.	1. Commentators on HIPAA have expressed concern that an election to operate as an affiliated covered entity may have adverse "spillover" effects, such as exposure to liability for the actions of the other participants. No consensus exists amongst commentators on this point. You are advised to consult with your own attorney or HIPAA advisor prior to electing to operate as an affiliated covered entity.	1. If you wish to operate as an affiliated covered entity, prepare a written election to this effect and related policy. (See policy #3A.) 2. Retain this documentation in your permanent office files for at least six years. 3. Prepare a joint notice of privacy practices
4. Do you practice in a setting that combines health care services with other services? • Examples: dental practices in retail stores; dental clinics at universities.	If yes, you practice at what HIPAA calls a "hybrid entity." A hybrid entity can elect to comply with HIPAA across all product/service lines, or it may elect to identify its "health care components" as the aspects of its business that must comply with HIPAA. If no, then no special features of your business organization will affect your HIPAA compliance.	1. "Health care components" consist of those areas of the entity that perform health care functions, and may also include those areas of the entity that support the health care functions. 2. Health care components cannot share PHI with non-health care components of the entity without an authorization or other HIPAA permission. 3. The entity must build "firewalls" between health care components and other aspects of the business to avoid wrongful disclosure of PHI.	1. If you elect to designate health care components to comply with HIPAA, prepare a policy so stating and addressing how the health care components will function for HIPAA purposes. (See policy #3B.)

DOES THE WAY THAT YOUR BUSINESS IS ORGANIZED AFFECT HOW YOU COMPLY WITH HIPAA

Questions 1 and 2 Definitions: "Organized health care arrangement" means:
(1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;
(2) An organized system of health care in which more than one covered entity participates, and in which the participating covered entities:
(i) Hold themselves out to the public as participating in a joint arrangement; and
(ii) Participate in joint activities that include at least one of the following:
(A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;
(B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or
(C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.
Common control exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.
Common ownership exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.

Question 4 Definitions: "Hybrid entity" means a single legal entity:
(1) That is a covered entity;
(2) Whose business activities include both covered and non-covered functions; and
(3) That designates health care components.

"Health care component" means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with paragraph (c)(3)(iii) of this section.

Doctor's Name
Address
Phone

AFFILIATED COVERED ENTITIES

Policy Number: 3A Effective Date _____

1. Pursuant to HIPAA's Privacy Rule, the following organizations elect to be considered an affiliated covered entity for purposes of compliance with the Privacy Rule:

[specify each organization that is affiliating by correct legal name]

2. These organizations will use and distribute a joint notice of privacy practices, and will otherwise comply with HIPAA's Privacy Rule as a single unit.

3. These organizations disclaim any intention to affiliate for any purpose other than HIPAA Privacy Rule compliance. For all other purposes, each organization is an individual legal entity.

Doctor's Name
Address
Phone

HEALTH CARE COMPONENTS

Policy Number: 3B Effective Date _____

1. For purposes of compliance with HIPAA's Privacy Rule, [name of organization] is classified as a hybrid entity. As such, we designate the following portions of our business as "health care components":

[Specify those service/product lines or business operations
that are health care in nature, or that support health care.]

2. These health care components will comply with all of the requirements of HIPAA's Privacy Rule. Health care components will not disclose protected health information to non-health care components without a signed patient authorization or other HIPAA permission. All health care components will institute appropriate safeguards to prevent improper disclosure of protected health information to non-health care components.

Completed _____ Date _____

DO YOU HAVE AN OVERALL WORK PLAN AND BUDGET FOR HIPAA COMPLIANCE IMPLEMENTATION?

_____

Signature of responsible person

Assessment Question	Comments	Action Steps
1. What financial and human resources do you have to devote to implementing HIPAA compliance measures?	1. Financial resources need to address EDI compliance as well as privacy compliance. 2. Privacy implementation costs include: • Salary of privacy officer and/or HIPAA contact person (if you decide to hire a new person), or overtime if existing staff needs additional time in order to work on HIPAA. • Cost of outside HIPAA consultant(s), if you need additional resources. • Cost of developing and implementing new privacy policies and procedures. – Soft time in determining appropriate policies and procedures. – Cost of implementing process changes. • Cost of purchasing or creating privacy forms. • Cost of implementing physical, administrative and technical safeguards for protected health information ("PHI"). • Cost of acquiring a master business associate contract, tailoring the contract to your business associates, and negotiating signature of the contract. • Cost of training your work force in HIPAA privacy rules and your privacy procedures. • Cost of obtaining and storing HIPAA required documentation. This list is not exhaustive, just illustrative. Also, individual practices may have other costs.	

DO YOU HAVE AN OVERALL WORK PLAN AND BUDGET FOR HIPAA COMPLIANCE IMPLEMENTATION?

Assessment Question	Comments	Action Steps
2. How much time per week does your existing staff have to devote to HIPAA compliance, and will you need outside help in order to meet the deadlines?	1. You must achieve compliance with the privacy rule by April 14, 2003. 2. You may qualify for additional time to negotiate some of your business associate contracts. (See charts 20-21.)	
3. If you need outside help, have you identified resources?		1. Identify the type of outside help that you need: • Legal help – interpreting the rules, drafting documents, drafting or reviewing policies and procedures, conducting training sessions. • IS help – for EDI issues. • Consulting firms. 2. The internet is a good starting place to locate resources in your identified need areas. Search under "HIPAA" and your state/city in any search engine.
4. How will you prioritize the tasks necessary for Privacy Rule compliance?		1. Consider the estimated complexity of each task. 2. Consider the estimated time necessary to accomplish each task. Remember to include time for activities like printing of forms, negotiating with vendors, and other activities involving third parties. 3. Based upon your prioritization, prepare a time line with compliance benchmarks, assigned individuals, budget allocation, and reporting dates. (See the model time line accompanying this chart.)
5. Do you need to obtain board or other management approval for expenditure of funds for compliance efforts?		

MODEL TIME LINE

December 1, 2002	Appoint a Privacy Officer and Public Information Officer
January 2, 2003	Complete all assessment questions in workbook, and complete all worksheets
January 15, 2003	Start installing any technical or physical safeguards for PHI
February 1, 2003	Devise and adopt policies and procedures needed to comply with HIPAA
Between February 1 and April 1, 2003	Conduct work force training
February 15, 2003	Order final customized HIPAA forms, with delivery by April 1, 2003
April 14, 2003	Compliance deadline

NOTE: This timeline is only an example. The dates shown are not mandatory, just suggestions. Pick the dates that work for you, so long as you are in compliance by April 14, 2003.

Completed _____ Date _____

YOU MUST APPOINT A PRIVACY OFFICER AND A PUBLIC INFORMATION OFFICER

_____

Signature of responsible person

Assessment Question	Comments	Action Steps
1. Identify the candidates (list names) – either internal to your organization or from outside sources, as applicable – for the position of privacy officer. Use the worksheet accompanying this chart, if desired.	1. The privacy officer role is to implement and sustain compliance with the privacy rule. 2. The job involves mostly internal management.	
2. Which of the candidates best satisfies the following criteria for the position of privacy officer: • *Knowledge* of the HIPAA privacy rules. • *Available* time to devote to compliance effort. • *Available* time to attend educational seminars on privacy compliance, and to summarize seminar content for staff. • *Capable* of sustained and detailed effort. • *Capable* of effectuating change, when needed. • *Capable* of creative or innovative solutions to privacy issues. • *Good* communication skills. • *Good* organizational skills. • *Motivates* staff to achieve compliance. • *Prudent* fiscal manager. • *Works well* with governing body or management. • *Works well* with outside resources, if applicable.		1. Based upon your assessment of the strengths of each candidate, select a privacy officer, and determine if compensation adjustments are necessary. 2. Obtain governing body or management approval of appointment, if needed. 3. Document the appointment in writing. 4. Keep this documentation with your office permanent records. 5. Prepare a job description for the privacy officer and incorporate it into your human resources manual. – See policy #5A for a model privacy officer job description.

YOU MUST APPOINT A PRIVACY OFFICER AND A PUBLIC INFORMATION OFFICER

Assessment Question	Comments	Action Steps
3. Identify the candidate(s) for the position of public information officer (list names). Use the worksheet accompanying this chart, if desired.	1. The position of public information officer is a public relations/patient ombudsman position. Job duties include explaining your privacy policies and procedures to patients, and receiving, investigating and resolving patient privacy grievances. 2. The same individual can serve as both privacy officer and public information officer if desired, or the positions can be held by different individuals. 3. The public information officer function can be performed by a department or office (such as the public relations office) if desired, in organizations large enough to have such offices.	
4. Which of the candidates best satisfies the following criteria for the position of public information officer? • *Knowledge* of the HIPAA privacy rule, and of your privacy policies and procedures. • *Knowledge* of your organizational structure, and who are the "go to" people to accomplish any task. • *Good* interpersonal skills. • *Sympathetic* to patient concerns. • *Good* communication skills. • *Good* investigational skills. • *Capable* of prompt and thorough resolution of identified problems, in conjunction with the privacy officer, as indicated in particular cases.		1. Based upon your assessment of the strengths of each candidate, select a public relations officer, and determine if compensation adjustments are necessary to accommodate new responsibilities. 2. Obtain governing body or management approval of the appointment, if needed. 3. Document the appointment in writing. 4. Keep this with your office permanent records.. 5. Prepare a job description for the public information officer and incorporate it into your human resources materials. – See policy #5B for a model public information officer job description.

Completed _____ Date _____

YOU MUST APPOINT A PRIVACY OFFICER AND A PUBLIC INFORMATION OFFICER (WORKSHEET)

_____
Signature of responsible person

Privacy Officer Candidates	Public Information Officer Candidates

Doctor's Name
Address
Phone

PRIVACY OFFICER JOB DESCRIPTION

Policy Number: 5A Effective Date _____

In order to comply with HIPAA's Privacy Rule, this office will have a privacy officer.

1. Qualifications to serve as privacy officer:

- Knowledge of the HIPAA Privacy Rule.
- Available time to devote to compliance effort.
- Available time to attend educational seminars on privacy compliance, and to summarize seminar content for staff.
- Capable of sustained and detailed effort.
- Capable of effectuating change, when needed.
- Capable of creative or innovative solutions to privacy issues.
- Good communication skills.
- Good organizational skills.
- Motivates staff to achieve compliance.
- Prudent fiscal manager.
- Works well with governing body or management.
- Works well with outside resources, as applicable.

2. Duties of the privacy officer:

- Creates and implements policies and procedures to comply with HIPAA's Privacy Rule.
- Monitors compliance efforts.
- Responds to specific HIPAA Privacy Rule compliance questions.
- Conducts educational sessions for our work force about HIPAA requirements and compliance.
- Receives and investigates allegations of non-compliance, and resolves any problems.

We appoint [insert name] as our privacy officer, effective _____.

Doctor's Name
Address
Phone

PUBLIC INFORMATION OFFICER JOB DESCRIPTION

Policy Number: 5B Effective Date _____

In order to comply with HIPAA's Privacy Rule, this office will have a public information officer.

1. Qualifications to serve as public information officer:

- Knowledge of the HIPAA Privacy Rule, and of our privacy policies and procedures.
- Knowledge of our organizational structure, and who are the "go to" people to accomplish any task.
- Good interpersonal skills.
- Sympathetic to patient concerns.
- Good communication skills.
- Good investigational skills.
- Capable of prompt and thorough resolution of identified problems, in conjunction with the privacy officer, as indicated in particular cases.

2. Duties of the public information officer:

- Receive, investigate, substantiate/not substantiate patient privacy complaints.
- Correct problems identified through investigation of privacy complaints.
- Provide information to patients and the public about our privacy practices and compliance.
- Report any concerns about privacy compliance to our privacy officer, and cooperate in the investigation and resolution of the problem.
- Accept and act upon patient requests for confidential methods of communication.
- Accept and act upon patient's requests to restrict the way we handle protected health information for treatment, payment, or health care operations.
- Accept and act upon patient requests for access to their own protected health information.
- Accept and act upon patient requests to amend their own protected health information.
- Accept and act upon patient requests for an accounting of our disclosures of their protected health information.

We appoint [insert name] to serve as our public information officer, effective _____.

Completed _____ Date _____

WHERE AND HOW ARE YOU USING OR DISCLOSING PROTECTED HEALTH INFORMATION?

_____

Signature of responsible person

Assessment Question	Uses of PHI
1. Identify the activities that you do which involve protected health information (PHI). See the definition of PHI accompanying this chart. *Mark those activities that apply to you in the "uses of PHI" column and add any others that are not already listed. If you need additional space, use the worksheet accompanying this chart, if desired.*	The following is a list of activities that many dentists perform. This list is not exhaustive. 1. Making appointments with patients. – New appointments. – Sending reminders of existing appointments. – Reviewing patient lists to suggest that the patient make an appointment. 2. Intake when the patient comes to the appointment. – Sign in sheets. – Waiting room procedures. – Checking insurance coverage. – Validating demographic information. – Retrieving old clinical charts. 3. Technician work up of patient before your professional examination. 4. Your professional examination. 5. Writing or phoning medication prescriptions, including responding to validation calls from the pharmacy. 6. Writing prescriptions for drugs and prosthetic devices. 7. Assisting patients with selection of dental prostheses. 8. Writing and filling orders for dental devices. – Communicating with outside dental laboratories. – Communicating with dental device manufacturers. 9. Referring patients to specialists, and on-going communication with other professionals involved in the patient's care. 10. Performing surgical procedures. 11. Preparing and submitting bills to third party payors (including coding), or to the patient, and collecting those bills.

WHERE AND HOW ARE YOU USING OR DISCLOSING PROTECTED HEALTH INFORMATION?

Assessment Question	Uses of PHI
	12. Marketing or advertising your products and services. 13. Responding to subpoenas or court orders in connection with litigation. 14. Reporting suspected child abuse. 15. Providing relevant information to patient caregivers. 16. Returning patient phone calls. 17. Defending licensure, and/or Medicare/Medicaid or other payor investigations or audits. 18. Obtaining accreditation for your office or specialty board certification for yourself. 19. Consulting with certain lawyers, accountants, practice managers, and others. 20. Performing quality assessment and improvement. 21. Making hiring decisions about your professional staff. 22. Training professional and non-professional staff. 23. Training professional interns or students. 24. Reporting adverse events or contagious diseases to the FDA or other public health authorities. 25. Sending clinical files or portions of them to follow-up providers or others that the patient directs. 26. Communicating with school nurses regarding student dental exams. 27. Participating in managed care organization credentialing. 28. Conducting clinical research. 29. Writing articles for professional journals. 30. Business planning and administrative management. 31. Other (specify).
2. Identify the staff that handles each function that you checked (list names or titles). Use the worksheet accompanying this chart, if desired.	

WHERE AND HOW ARE YOU USING OR DISCLOSING PROTECTED HEALTH INFORMATION?

Protected health information means information that identifies an individual patient (alone or in combination with other publicly available information) and that is:

1. Generated or received by a health care provider, health plan, health care clearinghouse or employer.

2. Relates to the past, present, or future physical or mental health or condition of the individual; the provision of health care to the individual; or the past, present, or future payment for the provision of health care to the individual.

3. PHI includes demographic information collected from the individual.

4. PHI can take any form:

- Hard copy Electronic
- Oral Photographs, video, audio recordings.

5. Identifiers include:

- Names.
- All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geo codes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
  - The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
  - The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
- All elements of dates (except year) directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
- Telephone numbers. Fax numbers.
- Electronic mail addresses. Social security numbers.
- Medical record numbers. Health plan beneficiary numbers.
- Account numbers. Certificate/license numbers.
- Vehicle identifiers and serial numbers, including license plate numbers.
- Device identifiers and serial numbers.
- Web universal resource locators (URLs)
- Internet protocol (IP) address numbers.
- Biometric identifiers, including finger and voice prints.
- Full face photographic images and any comparable images.
- Any other unique identifying number, characteristic, or code.

Completed _____ Date _____

WHERE AND HOW ARE YOU USING OR DISCLOSING PROTECTED HEALTH INFORMATION? (WORKSHEET)

_____

Signature of responsible person

Activity	Name/Title of Staff

WHERE AND HOW ARE YOU USING OR DISCLOSING PROTECTED HEALTH INFORMATION? (WORKSHEET)

Activity	Name/Title of Staff

Completed _____ Date _____

WHEN DO YOU NEED TO HAVE THE PATIENT SIGN AN AUTHORIZATION?

_____

Signature of responsible person

General Rule	Exceptions	Action Steps
1. You must have a signed patient authorization before you use or disclose PHI, unless HIPAA specifically makes an exception. HIPAA makes three kinds of exceptions. The exceptions to authorizations are discussed in detail in charts 8 through 12. **2. If you need a signed patient authorization, it must be in the form discussed in chart 13.**	1. Chart 8 discusses uses or disclosures for patient treatment, payment, or "health care operations." This is the broadest and most common of the exceptions to authorization. 2. Chart 9 discusses situations in which no authorization is required, but the patient must have the opportunity to object to a use or disclosure before you make it. 3. Chart 10 discusses a list of very specific uses or disclosures that do not require a signed authorization, and the conditions attached to these uses and disclosures.	1. HIPAA requires that you have a written policy describing when you need a signed patient authorization before you use or disclose PHI. The policy should include the following points: • A statement that you will get a signed patient authorization if necessary unless HIPAA makes a specific exception. • A description of those uses or disclosures of PHI that you make that do not need a signed patient authorization, including any special rules or conditions relating to them. • Who is responsible for getting any needed authorization. This may be one person for all uses or disclosures of PHI, or different people. • A process for getting any needed authorization. (See model policy #7A.)

Doctor's Name
Address
Phone

NO AUTHORIZATION IS REQUIRED TO MAKE CERTAIN DISCLOSURES OF PROTECTED HEALTH INFORMATION

Policy Number: 7A Effective Date _____

In order to comply with HIPAA's Privacy Rule, it is the policy of this office to obtain a signed patient authorization before making a use or disclosure of protected health information, except in those circumstances in which HIPAA does not require such an authorization. As stated in HIPAA, we will not obtain a signed patient authorization in the following circumstances:

1. Uses and disclosures for treatment, payment, or health care operations. This includes, among other activities:

- Providing care to patients in our office
- Seeking assistance from consultants
- Making referrals of patients for follow-up care
- Writing/sending, and filling prescriptions for drugs and dental devices
- Preparing and submitting claims and bills
- Receiving/posting payments, and collection efforts
- Managed care credentialing
- Professional licensure and specialty board credentialing
- Quality assurance
- Financial audits/management
- Training of professional and non-professional staff, including students
- Office management
- Fraud and abuse prevention activities
- Personnel activities
- The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or any entity that following such activity will become a covered entity, and due diligence related to such activity
-

NO AUTHORIZATION IS REQUIRED TO MAKE CERTAIN DISCLOSURES OF PROTECTED HEALTH INFORMATION

Policy Number: 7A Effective Date _____

[Notwithstanding the lack of need for a signed patient authorization, in order to comply with applicable state law, we will obtain permission from our patients before we disclose protected health information for the following activities:

(specify those treatment, payment or health care operations
for which your state law requires that you obtain
patient permission before sharing information)]

2. Disclosures to business associates that have signed a business associate contract with us.

3. Disclosures that are required by our state law, provided that we disclose only the precise protected health information required, and only to the recipient required.

4. Disclosures to state, local or federal governmental public health authorities to prevent or control disease, injury, or disability.

5. Disclosures to local, state, or federal governmental agencies to report suspected child abuse or neglect.

6. Disclosures to individuals or organizations under the jurisdiction of the federal Food and Drug Administration ("FDA"), such as drug or medical device manufacturers, regarding the quality or safety of drugs or medical devices.

7. Disclosures to local, state, or federal governmental agencies in order to report suspected abuse, neglect, or domestic violence regarding children, as required by law.

8. Disclosures for health oversight audits, investigations, or disciplinary activities, provided that we only disclose to a federal, state or local governmental agency (or a private person or organization acting under contract with or grant of authority from the governmental agency) that is authorized by law to conduct oversight activities.

9. Disclosures in response to a court order, provided that we disclose only the precise protected health information ordered, and only to the person ordered.

10. Disclosures in response to a proper subpoena, provided that:

- We make sure that either we or the person seeking the subpoenaed information makes a reasonable effort to notify the patient in advance, and the patient has a chance to object to the court about the disclosure.

- We make sure that either we or the person seeking the subpoenaed information makes a reasonable effort to have the court issue a protective order.

[substitute state law requirements, if they are more stringent than these]

NO AUTHORIZATION IS REQUIRED TO MAKE CERTAIN DISCLOSURES OF PROTECTED HEALTH INFORMATION

Policy Number: 7A Effective Date _____

11. Disclosures to police or other law enforcement officers regarding a crime that we think happened at our office, provided that we reasonably believe that the protected health information is evidence of a crime.

12. Disclosures to organizations involved in the procurement, banking, or transplantation of organs in order to facilitate organ donation and transplantation.

13. Uses of protected health information to market or advertise our own health care products or services, or for any other marketing exception (see related policy on marketing, # 11A).

14. Disclosures to a researcher with a waiver of authorization from an IRB or privacy board; to a researcher using the protected health information only for purposes preparatory to research or to a researcher only using the protected health information of deceased patients, provided that the researcher gives us the assurances required by HIPAA (see related policy on research, #12A).

15. If at any time a proposed use or disclosure does not fit exactly into one of the exceptions to the need for an authorization described in paragraphs 1 through 14, we will obtain a signed patient authorization before making the use or disclosure.

YOU DO NOT NEED A SIGNED PATIENT AUTHORIZATION TO USE OR DISCLOSE PHI FOR TREATMENT, PAYMENT OR HEALTH CARE OPERATIONS

Completed _____ Date _____

_____

Signature of responsible person

Assessment Question	Conditions Upon Use or Disclosure	Role of State Law	Action Steps
1. Which of your practice's activities involving PHI fall into the HIPAA definition of treatment? List them on the worksheet accompanying this chart, if desired.	1. You do not need a signed patient authorization to use or disclose PHI for your treatment purposes. 2. You do not need to be concerned about using the minimum necessary amount of PHI when you use or disclose PHI for treatment. (See chart 24.) 3. You must take reasonable steps to avoid incidental disclosures of PHI during treatment. (See chart 23.)	Notwithstanding HIPAA, your state law may require that you get patient permission before you use or disclose PHI for treatment. For example, your state law may require you to get patient permission before you send a patient's charts to a consultant. If this is the case, then you must follow the state law. Your state law may require a particular kind of permission form. If so, you must use it. If not, you are free to use any form of permission.	1. Write a policy describing what permission from the patient, if any, you will get before using or disclosing PHI for treatment purposes. Use the model policy, 8A accompanying this chart, if desired. 2. Keep this policy in your office's permanent records.
2. Which of your practice's activities involving PHI fall into the HIPAA definition of payment? List them on the worksheet accompanying this chart, if desired.	1. You do not need a signed patient authorization to use or disclose PHI for your payment purposes. 2. You must use or disclose only the minimum necessary amount of PHI to accomplish the payment task. (See chart 24) *Note:* Standard EDI transactions are considered to be the minimum necessary amount of PHI.	Notwithstanding HIPAA, your state law may require that you get patient permission before you disclose PHI for payment purposes. For example, some states require patient permission before a doctor can send PHI to an insurer for payment of a claim. If so, then you must follow your state law. Your state law may require a particular kind of permission form. If so, you must use it. If not, you are free to use any form	1. Write a policy describing the permission you will require (if any) before you use or disclose PHI for your payment purposes. Use the model policy, 8A accompanying this chart, if desired. 2. Keep this policy in your office's permanent records.
3. Which of your practice's activities involving PHI fall into HIPAA's definition of "health care operations"? List them on the worksheet accompanying this chart, if desired.	1. You do not need a signed patient authorization before you use or disclose PHI for your own health care operations. 2. You must use or disclose only the least amount of PHI necessary for a health care operation. (See chart 24.) 3. You must safeguard PHI and take reasonable steps to avoid incidental disclosure.	Notwithstanding HIPAA, your state law may require that you get patient permission before you disclose PHI for some or all of HIPAA's health care operations. If so, you must follow your state law. Your state law may require a particular form of permission. If so, you must use it. If not, you are free to use any form.	1. Write a policy describing what patient permission you will get before using or disclosing PHI for health care operations (if any) and the process that you will use. Use the model policy, 8A accompanying this chart, if desired. 2. Keep this policy in your office's permanent records.

YOU DO NOT NEED A SIGNED PATIENT AUTHORIZATION TO USE OR DISCLOSE PHI FOR TREATMENT, PAYMENT OR HEALTH CARE OPERATIONS

Assessment Question	Conditions Upon Use or Disclosure	Action Steps
4. Do you provide PHI to third parties for their treatment, payment or health care operations?	1. *Treatment* – without a signed patient authorization, you can disclose PHI to another doctor or provider so they can treat a patient. You can do this whether or not the doctor or other provider is himself obligated to follow HIPAA. (See chart 1.) 2. *Payment* – without a signed patient authorization, you can disclose PHI to another doctor or provider, or a health plan so that they can be paid. 3. *Health care operations* – without a signed patient authorization, you can disclose PHI to another provider or health plan so that they can use the PHI for certain of their health care operations. There are three limitations on this disclosure: • You must be sure that the patient has or had a professional relationship with the recipient. • If the intended recipient is a provider, you must be sure that the recipient is obligated to apply HIPAA. (See chart 1.) • You can only make the disclosure for some of the recipient's health care operations. These are: – Conducting quality assessment and improvement activities, – Population-based activities relating to improving health or reducing health care costs, – Protocol development, – Case management and care coordination, – Contacting of health care providers and patients with information about treatment alternatives – Reviewing the competence or qualifications of health care professionals, – Evaluating practitioner and provider performance, – Health plan performance, – Conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, – Training of non-health care professionals, – Accreditation, certification, licensing, or credentialing activities – Health care fraud and abuse detection or compliance - The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or any entity that following such activity will become a covered entity, and due diligence related to such activity.	1. Write a policy describing how these disclosures will be handled and the limitations upon them. Use the model policy, 8A accompanying this chart, if desired. 2. Keep this policy in your office's permanent records.

YOU DO NOT NEED A SIGNED PATIENT AUTHORIZATION TO USE OR DISCLOSE PHI FOR TREATMENT, PAYMENT OR HEALTH CARE OPERATIONS

	4. Except for disclosures for treatment, you must disclose the least amount of PHI necessary for the recipient's payment or health care operations. See chart 24. 5. You must safeguard the PHI and take reasonable steps to avoid incidental disclosures.	

YOU DO NOT NEED A SIGNED PATIENT AUTHORIZATION TO USE OR DISCLOSE PHI FOR TREATMENT, PAYMENT OR HEALTH CARE OPERATIONS

Question 1 Definitions: Treatment means:
The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party;
Consultation between health care providers relating to a patient; or
The referral of a patient for health care from one health care provider to another.

Question 2 Definitions: Payment means:
(1) The activities undertaken by:
(i) A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or
(ii) A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and
(2) The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:
(i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
(ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics;
(iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
(iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
(v) Utilization review activities, including pre-certification and pre-authorization of services, concurrent and retrospective review of services; and
(vi) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:
(A) Name and address;
(B) Date of birth;
(C) Social security number;
(D) Payment history;
(E) Account number; and
(F) Name and address of the health care provider and/or health plan.

Question 3 Definitions: Health care operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions:

YOU DO NOT NEED A SIGNED PATIENT AUTHORIZATION TO USE OR DISCLOSE PHI FOR TREATMENT, PAYMENT OR HEALTH CARE OPERATIONS

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalized knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;
(3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;
(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
(6) Business management and general administrative activities of the entity, including, but not limited to:

(i) Management activities relating to implementation of and compliance with the requirements of HIPAA;

(ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.

(iii)Resolution of internal grievances;

(iv)The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and

(v) Creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

Completed _____ Date _____

YOU DO NOT NEED A SIGNED PATIENT AUTHORIZATION TO USE OR DISCLOSE PHI FOR TREATMENT, PAYMENT OR HEALTH CARE OPERATIONS (WORKSHEET)

_____
Signature of responsible person

Treatment Activities	Payment Activities	Health Care Operations

Doctor's Name
Address
Phone

NO AUTHORIZATION IS REQUIRED TO MAKE CERTAIN DISCLOSURES OF PROTECTED HEALTH INFORMATION

Policy Number: 8A Effective Date _____

In order to comply with HIPAA's Privacy Rule, it is the policy of this office to obtain a signed patient authorization before making a use or disclosure of protected health information, except in those circumstances in which HIPAA does not require such an authorization. As stated in HIPAA, we will not obtain a signed patient authorization in the following circumstances:

1. Uses and disclosures for treatment, payment, or health care operations. This includes, among other activities:

- Providing care to patients in our office
- Seeking assistance from consultants
- Making referrals of patients for follow-up care
- Writing/sending, and filling prescriptions for drugs and dental devices
- Preparing and submitting claims and bills
- Receiving/posting payments, and collection efforts
- Managed care credentialing
- Professional licensure and specialty board credentialing
- Quality assurance
- Financial audits/management
- Training of professional and non-professional staff, including students
- Office management
- Fraud and abuse prevention activities
- Personnel activities
- The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or any entity that following such activity will become a covered entity, and due diligence related to such activity.

NO AUTHORIZATION IS REQUIRED TO MAKE CERTAIN DISCLOSURES OF PROTECTED HEALTH INFORMATION

Policy Number: 8A Effective Date _____

[Notwithstanding the lack of need for a signed patient authorization, in order to comply with applicable state law, we will obtain permission from our patients before we disclose protected health information for the following activities:

(specify those treatment, payment or health care operations
for which your state law requires that you obtain
patient permission before sharing information)]

2. Disclosures to business associates that have signed a business associate contract with us.

3. Disclosures that are required by our state law, provided that we disclose only the precise protected health information required, and only to the recipient required.

4. Disclosures to state, local or federal governmental public health authorities to prevent or control disease, injury, or disability.

5. Disclosures to local, state, or federal governmental agencies to report suspected child abuse or neglect.

6. Disclosures to individuals or organizations under the jurisdiction of the federal Food and Drug Administration ("FDA"), such as drug or medical device manufacturers, regarding the quality or safety of drugs or medical devices.

7. Disclosures for health oversight audits, investigations, or disciplinary activities, provided that we only disclose to a federal, state or local governmental agency (or a private person or organization acting under contract with or grant of authority from the governmental agency) that is authorized by law to conduct oversight activities.

8. Disclosures in response to a court order, provided that we disclose only the precise protected health information ordered, and only to the person ordered.

9. Disclosures in response to a proper subpoena, provided that:

- We make sure that either we or the person seeking the subpoenaed information makes a reasonable effort to notify the patient in advance, and the patient has a chance to object to the court about the disclosure.

- We make sure that either we or the person seeking the subpoenaed information makes a reasonable effort to have the court issue a protective order.

[substitute state law requirements, if they are more stringent than these]

10. Disclosures to police or other law enforcement officers regarding a crime that we think happened at our office, provided that we reasonably believe that the protected health information is evidence of a crime.

NO AUTHORIZATION IS REQUIRED TO MAKE CERTAIN DISCLOSURES OF PROTECTED HEALTH INFORMATION

Policy Number: 8A Effective Date _____

11. Disclosures to organizations involved in the procurement, banking, or transplantation of organs in order to facilitate organ donation and transplantation.

12. Uses of protected health information to market or advertise our own health care products or services, or for any other marketing exception (see related policy on marketing, # 11A).

13. Disclosures to a researcher with a waiver of authorization from an IRB or privacy board; to a researcher using the protected health information only for purposes preparatory to research or to a researcher only using the protected health information of deceased patients, provided that the researcher gives us the assurances required by HIPAA (see related policy on research, #12A).

14. If at any time a proposed use or disclosure does not fit exactly into one of the exceptions to the need for an authorization described in paragraphs 1 through 13, we will obtain a signed patient authorization before making the use or disclosure.

Completed _____ Date _____

YOU DO NOT NEED A SIGNED PATIENT AUTHORIZATION FOR FACILITY DIRECTORIES, OR TO SHARE PHI WITH CAREGIVERS

_____

Signature of responsible person

Assessment Question	Yes/No	Comments	Action Steps
1. Do you operate any kind of "facility" (e.g. oral surgery clinic) where patients stay for several hours or more?	If yes, go to question 2. If no, go to question 3.		
2. Do you want to keep a directory of current patients (name, locations within the facility and general condition) so that callers can be updated about their progress?	If yes: • You can do this without a signed patient authorization so long as the patient does not object. • The patient can object to including some or all information in the directory. • The patient can object to disclosing the information to some or all callers.	1. You must advise the patient of your directory policy. 2. You must give the patient the chance to object. 3. HIPAA allows the advice and any objections to be oral, but this may not be good policy because you will not have proof of compliance with these steps.	1. Write a policy describing the following items: • How you will advise patients of your directory policy. • How you will allow patients to object to being included in the directory, or to disclosure of directory information. • Who in your practice will be responsible for advising patients and accepting objections. • How you will make disclosures of directory information to inquirers. See model policy 9A.

YOU DO NOT NEED A SIGNED PATIENT AUTHORIZATION FOR FACILITY DIRECTORIES, OR TO SHARE PHI WITH CAREGIVERS

Assessment Question	Yes/No	Comments	Action Steps
3. Do you provide information about a patient's care needs to family or friends who are involved in their care?	If yes: • You can do this without a signed patient authorization so long as the patient has a chance to object. • You must advise the patient of your policy before you give information to family or friends. • You must give the patient a chance to object to what PHI you want to disclose or to the person that you want to disclose it to.	1. If the patient is present or available at the time that you want to inform family or friends about a care need, you can: • Advise the patient and allow any objection. • Get a specific agreement. • Infer lack of objection from the circumstances. 2. If the patient is not present or available when you want to provide information to family or friends, you can: • Provide information if that is in the best interest of the patient. One example would be giving ordered glasses to a family member who comes to pick them up for the patient. • Provide only the PHI that is directly relevant to the family or friend's involvement with the patient's care. • You can only disclose PHI to a family member or close personal friend of the patient, unless the patient identifies some other person.	1. Write a policy that defines when and how you will provide PHI to family and friends involved in a patient's care. Elements of the policy include: • How you will advise patients of your practice of sharing PHI with people involved in their care. • How will you allow a patient to object to sharing PHI? • What circumstances allow you to infer that the patient does not object to sharing PHI? • How will you know if someone is a family member or close personal friend of a patient if they initiate the contact? • How will you decide if sharing of PHI is in a patient's best interest if they are not available? See model policy 9B.

Doctor's Name
Address
Phone

FACILITY DIRECTORY

Policy Number: 9A Effective Date _____

In order to comply with HIPAA's Privacy Rule, it is the policy of this office to give patients an opportunity to object to including their protected health information in our facility directory.

1. Our facility directory will consist of only the following information:

    3. patient name

    4. location within the facility

    5. general status information (procedure not started, procedure in progress, procedure completed).

2. If we receive a call from someone knowing the patient's name, we will disclose the directory information about the named patient to the caller, unless the patient has previously objected to such disclosure. We will not disclose more information than that specified in paragraph 1 to any caller.

3. [Insert name/title] is responsible for managing our facility directory and for providing patients the chance to object to being included or to having certain information disclosed.

4. At the time that a patient checks in to our facility, [insert name/title from paragraph 3] will orally advise the patient of our directory, the information that is ordinarily contained in it, and our disclosure policy. [insert name/title of person from paragraph 3] will ask the patient if he/she has any objection to being included in the directory. The patient is free to object to

    6. being included at all

    7. having particular elements of information included

    8. disclosing some or all of the information to certain callers.

5. If a patient objects, [insert name/title from paragraph 3] will note the objection [specify how and where it will be noted]. [Insert name/title from paragraph 3] will provide the note to all phone operators who might receive a call requesting directory information. All phone operators will abide by patient's objections regarding directory information.

Doctor's Name
Address
Phone

PROVIDING INFORMATION TO FAMILY AND FRIENDS OF PATIENTS INVOLVED IN CARE

Policy Number: 9B Effective Date _____

In order to comply with HIPAA's Privacy Rule, it is the policy of this office to give patients a chance to agree or object to providing protected health information to close family or friends who are helping with the patient's care.

1. If we feel that it is necessary or appropriate to inform a close family member or friend who is involved in a patient's care about certain protected health information relevant to their involvement, we will give the patient a chance to agree or object to such disclosure before we make it. If the patient is present or available when this need arises, we will do any of the following:

- Get an oral agreement from the patient that the disclosure is acceptable.
- Give the patient a chance to object to the disclosure.
- Infer from the circumstances that the patient does not object. For example, we can reasonably infer that the patient does not object if the family member or friend is in the examining room with the patient.

If the patient is not present or available when the need arises, we will use our best judgment about whether it is in the patient's best interest to disclose the information. An example might be when a family member or friend comes to our office to pick up dentalwear that the patient previously ordered, as a convenience to the patient.

2. If we make a disclosure to a close family member or friend under the circumstances described in paragraph 1, we will only disclose information that is relevant to the family member or friend's involvement with the patient's care. Examples:

- If the patient's spouse will pick up ordered dental devices, we will provide the dental device but not disclose any diagnoses or special features of the dental device.
- If a son or daughter will assist a patient with dental drugs or devices, we will provide information about when and how the drugs or devices should be administered or installed, but will not disclose the patient's diagnosis.

3. If someone claiming to be a family member or friend of the patient initiates contact with us seeking information, we will:

- Verify the identity of the caller and their relationship to the patient.
- Determine if they are involved in the patient's care.
- Determine if the patient is available (by phone, email, or other communications method) to either agree or object to the disclosure. If so, we will give the patient the chance to agree or object. If the patient objects, we will not disclose any information to the caller. If the patient is not available by any reasonable means, we will use our best judgment to determine whether disclosure of information is in the patient's best interest.

Completed _____ Date _____

YOU DO NOT NEED AN AUTHORIZATION FOR DISCLOSURES FOR "PUBLIC POLICY" PURPOSES

_____

Signature of responsible person

Assessment Question	Conditions on Disclosure	Comments	Action Steps
1. Does your state law require that you disclose PHI for any reason? Some examples include reporting of gunshot wounds, or providing information to professional licensing authorities.	1. A signed patient authorization is not required, provided that you comply with the following points. • You are considered by HIPAA to be "required" to make a disclosure of PHI only if state law compels you to do it (e.g., you can be punished or adversely affected if you do not make the disclosure). • You must disclose only the exact PHI that the law compels, and only to the recipient named in the law.		1. Consult your attorney or advisor for information about state law requirements. 2. Make a list of those requirements. Use the worksheet following this chart, if desired. 3. Write a policy describing when you are required by law to disclose PHI and how you will disclose it. Use the model policy, 10A accompanying this chart, if desired. 4. Keep this policy with your practice's permanent records.
2. Do you currently give PHI to public health authorities for the purpose of preventing or controlling disease, injury, or disability?	1. You do not need a signed patient authorization to make this type of disclosure of PHI, so long as you comply with the following points: • The recipient must be a local, state or federal government agency authorized by law to receive the information, not a private organization. • You must disclose only the least amount of PHI necessary to inform the public health agency. • You must safeguard the PHI and take reasonable steps to prevent incidental disclosures.	1. Some examples include: • Reporting communicable diseases. • Reporting work hazards. • Reporting environmental hazards.	1. Make a list of the situations in which you disclose PHI to public health authorities. Use the worksheet accompanying this chart, if desired. 2. Write a policy describing those disclosures of PHI and how you will disclose it. Use the model policy, 10A accompanying this chart, if desired. 3. Keep this policy with your practice's permanent records.

YOU DO NOT NEED AN AUTHORIZATION FOR DISCLOSURES FOR "PUBLIC POLICY" PURPOSES

Assessment Question	Conditions on Disclosure	Comments	Action Steps
3. Do you currently make reports of suspected child abuse or neglect?	1. You do not need a signed patient authorization in order to make a report of suspected child abuse or neglect so long as you comply with the following points: • The recipient of the report must be a local, state or federal government agency that is authorized by law to receive such information. • You must disclose the minimum amount of PHI necessary to properly inform the authority about the suspected abuse or neglect. • If you make the disclosure because your state law requires it, you must disclose only the PHI that the law requires. • You must safeguard the PHI and take reasonable steps to avoid incidental disclosures of PHI.		1. Make a list of the situations in which you report suspected child abuse/neglect, and to whom the report is made. Use the worksheet accompanying this chart, if desired. 2. Write a policy describing those disclosures of PHI and how you will disclose it. Use the model policy, 10A accompanying this chart, if desired. 3. Keep this policy with your practice's permanent records.
4. Do you currently disclose PHI to drug or medical device manufacturers, sponsors of clinical trials or others working under the FDA, regarding the quality or safety of drugs or devices? • Examples include: reporting adverse events with a drug or medical device, tracking implanted devices to help with product recalls.	1. You do not need a signed patient authorization for this kind of disclosure, provided that you comply with the following points. 2. You may only disclose PHI for this purpose to someone who is working under the jurisdiction of the Food and Drug Administration (FDA): • Drug manufacturers. • Medical device manufacturers. • Sponsors of clinical trials. • Principal investigators in clinical trials. • Clinical research organizations (CROs) managing clinical trials on behalf of sponsors. • FDA staff.		1. Make a list of the situations in which you disclose information about the safety of drugs or medical devices, and to whom. Use the worksheet accompanying this chart, if desired. 2. Write a policy describing those disclosures of PHI and how you will disclose it. Use the model policy, 10A accompanying this chart, if desired. 3. Keep this policy with your practice's permanent records.

YOU DO NOT NEED AN AUTHORIZATION FOR DISCLOSURES FOR "PUBLIC POLICY" PURPOSES

Assessment Question	Conditions on Disclosure	Comments	Action Steps
5. Do you currently disclose PHI about suspected victims of abuse, neglect or domestic violence (other than children)?	1. You do not need a signed patient authorization in order to make these types of disclosures, so long as you comply with the following points: • You may only make the disclosure to a local, state or federal government agency authorized by law to receive the information. • You must get an informal agreement from the patient (oral is fine – a full written authorization is not needed) unless: – You are required by law to report your suspicions. – You are permitted, but not required by law to disclose the PHI, **and** you believe that a report is necessary to prevent harm to your patient or other potential victims. • You must tell the patient that you are making this disclosure, unless: – Telling the patient would put the patient at risk for serious harm, or – Someone else is acting on behalf of the patient and you think that this person is the abuser and that telling him or her would not be in the best interest of the patient. (See chart 13.)	If you do not meet all the stipulations in "conditions on disclosure," then you need a full signed patient authorization before you can make the report.	1. Make a list of the situations in which you report suspected abuse, neglect, or domestic violence, and to whom the report is made. Use the worksheet accompanying this chart, if desired. 2. Write a policy describing those disclosures of PHI and how you will disclose it. Use the model policy, 10A accompanying this chart, if desired. 3. Keep this policy with your practice's permanent records.
6. Is it possible that you may need to respond to health oversight audits, investigations, or disciplinary activities? Some examples include: • Medicaid fraud unit	1. You do not need a signed patient authorization in order to make this kind of disclosure, so long as you comply with the following points: • You may only disclose PHI for this purpose to a federal, state or local governmental agency (or a private person or organization acting under contract with or grant of authority from the governmental	You must verify the identity of the requestor, and the authority for their request for PHI. (See chart 25.)	1. Make a list of the situations that you typically encounter in your practice involving health care oversight. Use the worksheet accompanying this chart, if desired.

YOU DO NOT NEED AN AUTHORIZATION FOR DISCLOSURES FOR "PUBLIC POLICY" PURPOSES

Assessment Question	Conditions on Disclosure	Comments	Action Steps
investigations. • Professional licensure sanction proceedings. • Fiscal intermediary financial audits.	agency) that is authorized by law to conduct oversight activities. • You must disclose the minimum amount of PHI necessary for the investigation. You can rely upon the representation of the governmental agency (or private contractor) about what PHI is the least amount necessary for it to perform its oversight duties. • You must safeguard the PHI and take reasonable steps to avoid incidental disclosures of PHI.		2. Write a policy describing those disclosures of PHI and how you will disclose it. Use the model policy, 10A accompanying this chart, if desired. 3. Keep this policy with your practice's permanent records.
7. Is it possible that you will receive a subpoena or court order calling for the release of PHI?	1. You do not need a signed patient authorization in order to release PHI as ordered by a court. However, you can only release the specific PHI so ordered. 2. You do not need a signed patient authorization in order to disclose PHI as commanded in a subpoena, so long as you comply with the following points: • You or the person seeking the subpoena must make a reasonable effort to notify the patient in advance, and the patient must have a chance to object to the court about the disclosure. • Alternatively, you or the person sending the subpoena must make a reasonable effort to have the court issue a protective order. These are orders restricting the further use or disclosure of the PHI. They are intended to further protect the confidentiality of the PHI.	1. Your state may have rules regarding subpoenas that require specific patient permission before you can disclose PHI. 2. Consult your own attorney or advisor if you receive a subpoena commanding the disclosure of PHI. 3. Never ignore a subpoena even if you think that you do not have the proper authority to disclose the PHI that it commands. Your attorney can help you sort through the requirements.	1. Make a list of the kinds of court orders or subpoenas that you might encounter in your practice. Use the worksheet accompanying this chart, if desired. Examples might include: subpoenas for patient records in a malpractice lawsuit; subpoenas or patient billing records in a collection lawsuit; subpoenas for records of a minor patient in a child abuse/neglect case or custody lawsuit. 2. Write a policy describing those disclosures of PHI and how you will disclose it. Use the model policy, 10A accompanying this chart, if desired. 3. Keep this policy with your practice's permanent records.

YOU DO NOT NEED AN AUTHORIZATION FOR DISCLOSURES FOR "PUBLIC POLICY" PURPOSES

Assessment Question	Conditions on Disclosure	Comments	Action Steps
8. Is it possible that you may need to disclose PHI to police or other law enforcement authorities regarding a crime at your office?	1. You do not need a signed patient authorization in order to make this type of disclosure, so long as you comply with the following points: • Before you make the disclosure, you must believe in good faith that the PHI is evidence of a crime. • You can only disclose such PHI if the crime occurred at your office. • You must disclose the minimum amount of PHI necessary to apprise police of the crime. • You must safeguard the PHI and take reasonable steps to avoid incidental disclosures.	HIPAA has additional provisions specific to the disclosure of PHI to law enforcement in a variety of other situations. We have assumed that these situations are not typical in a dental practice, and do not discuss them. If a law enforcement officer asks you to disclose PHI: • Consult your attorney or advisor about the specific HIPAA rules that might apply, or • Review Section 512(f) of the Privacy Rule for further guidance.	1. Make a list of the situations that you think you might encounter in your practice involving criminal activity at your office. Use the worksheet accompanying this chart, if desired. Examples might include theft of office property, theft of employee property, physical assaults. 2. Write a policy describing these disclosures of PHI and how you will disclose it. Use the model policy, 10A accompanying this chart, if desired. 3. Keep this policy with your practice's permanent records.
9. Do you typically facilitate prearranged or family-initiated organ donations after a patient has died?	1. You do not need a signed patient authorization from the representative of the deceased patient in order to disclose PHI in connection with organ donations, so long as you comply with the following points: • You may only disclose PHI under these circumstances to an organization involved in the procurement, banking, or transplantation of organs. • You may only disclose PHI under these circumstances in order to facilitate organ donation and transplantation. • You must disclose only the minimum amount of PHI that is necessary to facilitate the donation or transplantation. • You must safeguard the PHI and take reasonable steps to avoid incidental disclosures.		1. Consult with the organ bank in your area to determine what PHI they may need from you in order to accomplish an organ donation or transplantation. 2. Write a policy describing these disclosures of PHI and how you will disclose it. Use the model policy, 10A accompanying this chart, if desired. 3. Keep this policy with your practice's permanent records.

Completed _____ Date _____

YOU DO NOT NEED AN AUTHORIZATION FOR DISCLOSURES FOR "PUBLIC POLICY" PURPOSES (WORKSHEET)

_____

Signature of responsible person

Type of Disclosure	Specific Instances in Your Practice	Comply with HIPAA Requirements (Yes/No)	Procedure Changes to Avoid Need for Authorization
Required by state law			
Prevention of disease			
Suspected child abuse or neglect			
Quality or safety of drugs or devices			
Suspected abuse or neglect (other than children)			
Health oversight audits, investigations or disciplinary activities			
Subpoena or court order			
Organ donations			

Doctor's Name
Address
Phone

NO AUTHORIZATION IS REQUIRED TO MAKE CERTAIN DISCLOSURES OF PROTECTED HEALTH INFORMATION

Policy Number: 10A Effective Date _____

In order to comply with HIPAA's Privacy Rule, it is the policy of this office to obtain a signed patient authorization before making a use or disclosure of protected health information, except in those circumstances in which HIPAA does not require such an authorization. As stated in HIPAA, we will not obtain a signed patient authorization in the following circumstances:

1. Uses and disclosures for treatment, payment, or health care operations. This includes, among other activities:

- Providing care to patients in our office
- Seeking assistance from consultants
- Making referrals of patients for follow-up care
- Writing/sending, and filling prescriptions for drugs and dental devices
- Preparing and submitting claims and bills
- Receiving/posting payments, and collection efforts
- Managed care credentialing
- Professional licensure and specialty board credentialing
- Quality assurance
- Financial audits/management
- Training of professional and non-professional staff, including students
- Office management
- Fraud and abuse prevention activities
- Personnel activities

[Notwithstanding the lack of need for a signed patient authorization, in order to comply with applicable state law, we will obtain permission from our patients before we disclose protected health information for the following activities:

NO AUTHORIZATION IS REQUIRED TO MAKE CERTAIN DISCLOSURES OF PROTECTED HEALTH INFORMATION

Policy Number: 10A Effective Date _____

(specify those treatment, payment or health care operations
for which your state law requires that you obtain
patient permission before sharing information)]

2. Disclosures to business associates that have signed a business associate contract with us.

3. Disclosures that are required by our state law, provided that we disclose only the precise protected health information required, and only to the recipient required.

4. Disclosures to state, local or federal governmental public health authorities to prevent or control disease, injury, or disability.

5. Disclosures to local, state, or federal governmental agencies to report suspected child abuse or neglect.

6. Disclosures to individuals or organizations under the jurisdiction of the federal Food and Drug Administration ("FDA"), such as drug or medical device manufacturers, regarding the quality or safety of drugs or medical devices.

7. Disclosures for health oversight audits, investigations, or disciplinary activities, provided that we only disclose to a federal, state or local governmental agency (or a private person or organization acting under contract with or grant of authority from the governmental agency) that is authorized by law to conduct oversight activities.

8. Disclosures in response to a court order, provided that we disclose only the precise protected health information ordered, and only to the person ordered.

9. Disclosures in response to a proper subpoena, provided that:

- We make sure that either we or the person seeking the subpoenaed information makes a reasonable effort to notify the patient in advance, and the patient has a chance to object to the court about the disclosure.

- We make sure that either we or the person seeking the subpoenaed information makes a reasonable effort to have the court issue a protective order.

[substitute state law requirements, if they are more stringent than these]

10. Disclosures to police or other law enforcement officers regarding a crime that we think happened at our office, provided that we reasonably believe that the protected health information is evidence of a crime.

11. Disclosures to organizations involved in the procurement, banking, or transplantation of organs in order to facilitate organ donation and transplantation.

12. Uses of protected health information to market or advertise our own health care products or services, or for any other marketing exception (see related policy on marketing, # 11A).

NO AUTHORIZATION IS REQUIRED TO MAKE CERTAIN DISCLOSURES OF PROTECTED HEALTH INFORMATION

Policy Number: 10A Effective Date _____

13. Disclosures to a researcher with a waiver of authorization from an IRB or privacy board; to a researcher using the protected health information only for purposes preparatory to research or to a researcher only using the protected health information of deceased patients, provided that the researcher gives us the assurances required by HIPAA (see related policy on research, #12A).

14. If at any time a proposed use or disclosure does not fit exactly into one of the exceptions to the need for an authorization described in paragraphs 1 through 13, we will obtain a signed patient authorization before making the use or disclosure.

Completed _____ Date _____

YOU MAY NEED AN AUTHORIZATION TO USE OR DISCLOSE PHI FOR MARKETING OR ADVERTISING – IT DEPENDS ON THE AVAILABILITY OF AN EXCEPTION

_____

Signature of responsible person

Assessment Question	Conditions on Use/Disclosure	Comments	Action Steps
1. Do you conduct any marketing or advertising, either yourself or through a hired agency or company?		If the answer is "no", this chart does not apply to you. If the answer is yes, go to question 2.	
2. Do you use or disclose PHI when you market or advertise?	1. The general rule is that you need a signed patient authorization before you can use or disclose PHI for marketing purposes. However, there are many exceptions to this rule. The exceptions are so broad that you may be able to make most of your marketing communications without a signed authorization. The exceptions are: • Marketing about your own health care products or services. • Marketing during treatment. • Marketing during case management or care	1. You use PHI in connection with marketing or advertising when you review a patient database or patient records in order to target a particular communication. Examples include • Reviewing your patient records for those patients with clinical indications for implants and sending those patients a brochure about your implant services, or • Reviewing your patient records or database for tooth whitening and sending them a flyer announcing a new tooth whitening package that you offer. 2. You disclose PHI in connection with marketing or	1. List the marketing or advertising activities involving PHI that you do. Use the worksheet accompanying this chart if desired. 2. Determine if any of these marketing or advertising activities relate to your own health care products or services. 3. If they do, then you do not need a signed patient authorization in order to use PHI to make them. You need a signed patient authorization in order to use PHI in the content of these communications . 4. If your marketing or advertising efforts involve PHI and relate to the products or services of a third party, or relate to your own non-health care products or services, determine if they fall into any of the other marketing exceptions. 5. If you need a signed patient authorization for a particular marketing communication, be sure to include the special language about whether or not you are receiving anything of value in connection with the communication. 6. Write a policy that describes the following items: • How you use or disclose PHI for marketing or advertising.

YOU MAY NEED AN AUTHORIZATION TO USE OR DISCLOSE PHI FOR MARKETING OR ADVERTISING – IT DEPENDS ON THE AVAILABILITY OF AN EXCEPTION

Assessment Question	Conditions on Use/Disclosure	Comments	Action Steps
	coordination. • Marketing during face-to-face encounters. • Marketing that is promotional gifts of nominal value. The exceptions are discussed in questions 3, 4, 5, and 6.	advertising if you include patient photos, testimonials, or similar identifiers in the content of your marketing/advertising communication. Examples include: • TV commercials showing patients with dental devices that you sell, or • Explaining how pleased they are with your service. 3. Much marketing does not involve any PHI. Examples include: • Brochures mailed to "occupant" in a particular zip code, or • TV ads that do not include pictures or testimonials of patients.	• When a signed patient authorization is needed. • Who in your practice will obtain signed authorizations, when they are needed. • How you will use the least amount of information necessary, and how you will safeguard PHI. (See charts 23-24.) 7. Keep this policy with your permanent office records. You may use model policy, #11A if desired.
3. Is any of your marketing or advertising about the health care products or services that you provide or sell?	1. This is one of the exceptions to the general rule that marketing communications need a signed patient authorization. 2. You do not need a	1. Dental exams and treatment are health care. 2. The provision of dental devices is health care. 3. If you need a signed patient authorization in order to use or disclose PHI in connection with	1. List the marketing or advertising activities involving PHI that you do. Use the worksheet accompanying this chart if desired. 2. Determine if any of these marketing or advertising activities involve any products or services that are your own health care products or services. 3. If your marketing or advertising efforts involve PHI and relate to the products or services of a third party, or relate to your own

YOU MAY NEED AN AUTHORIZATION TO USE OR DISCLOSE PHI FOR MARKETING OR ADVERTISING – IT DEPENDS ON THE AVAILABILITY OF AN EXCEPTION

Assessment Question	Conditions on Use/Disclosure	Comments	Action Steps
	signed patient authorization in order to use PHI to make a marketing communication about your own health care products or services. 3. You need a signed patient authorization if the communication relates to non-health care products or services that you may provide. 4. You need a signed patient authorization if the content of the marketing includes photos, testimonials or other PHI. 5. You may only use the minimum necessary amount of PHI to make the communication. 6. You must safeguard the PHI and take reasonable steps to avoid incidental disclosures.	a marketing communication, the authorization must state whether you will receive anything of value from a third party in connection with making the communication. This is in addition to satisfying all the core elements of an authorization.	non-health care products or services, determine if they fall into any of the other marketing exceptions. These are addressed in questions 4, 5, and 6. 4. If you need a signed patient authorization for a particular marketing communication, be sure to include the special language about whether or not you are receiving anything of value in connection with the communication. 5. Write a policy that describes the following items: • How you use or disclose PHI for marketing or advertising. • When a signed patient authorization is needed. • Who in your practice will obtain signed authorizations, when they are needed. • How you will use the least amount of information necessary, and how you will safeguard PHI. (See charts 23-24.) 6. Keep this policy with your permanent office records. You may use model policy, #11A if desired.

YOU MAY NEED AN AUTHORIZATION TO USE OR DISCLOSE PHI FOR MARKETING OR ADVERTISING – IT DEPENDS ON THE AVAILABILITY OF AN EXCEPTION

Assessment Question	Conditions on Use/Disclosure	Comments	Action Steps
4. Do you make marketing communications in connection with the treatment or care coordination/case management of individual patients? • Examples include recommending a specific brand product or alternate sources of a product or service.	1. This is one of the exceptions to the general rule that marketing communications need a signed patient authorization. 2. You do not need a signed patient authorization to use or disclose PHI in order to make a marketing communication in connection with treatment or care coordination/case management of an individual patient. This is true whether the product or service involved in the communication is your own or not. 3. You may only use or disclose the least amount of PHI necessary to make the communication. 4. You must safeguard the PHI and take reasonable steps to avoid incidental disclosures.		1. List the marketing or advertising activities involving PHI that you do. Use the worksheet accompanying this chart if desired. 2. Determine if any of these marketing or advertising activities involve any products or services that are not • your own, or • health care. 3. If your marketing or advertising efforts involve PHI and relate to the products or services of a third party, or relate to your own non-health care products or services, determine if they fall into any of the other marketing exceptions. 1. If you need a signed patient authorization for a particular marketing communication, be sure to include the special language about whether or not you are receiving anything of value in connection with the communication. 2. Write a policy that describes the following items: • How you use or disclose PHI for marketing or advertising. • When a signed patient authorization is needed. • Who in your practice will obtain signed authorizations, when they are needed. • How you will use the least amount of information necessary, and how you will safeguard PHI. (See charts 23-24.) 6. Keep this policy with your permanent office records. You may use model policy, #11A if desired.

YOU MAY NEED AN AUTHORIZATION TO USE OR DISCLOSE PHI FOR MARKETING OR ADVERTISING – IT DEPENDS ON THE AVAILABILITY OF AN EXCEPTION

Assessment Question	Conditions on Use/Disclosure	Comments	Action Steps
5. Do you use or disclose PHI in order to make marketing communications during a face-to-face patient encounter? • Examples include: providing free drug samples or free dental accessories during an appointment.	1. This is one of the exceptions to the general rule that marketing communications need a signed patient authorization. 2. You do not need a signed authorization in order to use or disclose PHI to make a marketing communication during a face-to-face encounter with a patient. • This is true whether the products or services that you are marketing are your own or not, and whether they are health care or not. • The face-to-face encounter can take place anywhere. • You may only use the minimum necessary amount of PHI to make the communication. • You must safeguard the PHI and take reasonable steps to avoid incidental disclosures.		1. List the marketing or advertising activities involving PHI that you do. Use the worksheet accompanying this chart if desired. 2. Determine if any of these marketing or advertising activities involve any products or services that are not • your own, or • health care. 3. If your marketing or advertising efforts involve PHI and relate to the products or services of a third party, or relate to your own non-health care products or services, determine if they fall into any of the other marketing exceptions. 4. If you need a signed patient authorization for a particular marketing communication, be sure to include the special language about whether or not you are receiving anything of value in connection with the communication. 5. Write a policy that describes the following items: • How you use or disclose PHI for marketing or advertising. • When a signed patient authorization is needed. • Who in your practice will obtain signed authorizations, when they are needed. • How you will use the least amount of information necessary, and how you will safeguard PHI. (See charts 23-24.) 6. Keep this policy with your permanent office records. You may use model policy, #11A if desired.

YOU MAY NEED AN AUTHORIZATION TO USE OR DISCLOSE PHI FOR MARKETING OR ADVERTISING – IT DEPENDS ON THE AVAILABILITY OF AN EXCEPTION

Assessment Question	Conditions on Use/Disclosure	Comments	Action Steps
6. Do you ever distribute promotional gifts of nominal value as part of your marketing efforts?	1. This is one of the exceptions to the general rule that marketing communications need a signed patient authorization. 2. You do not need a signed authorization to use or disclose PHI in order to make a marketing communication in the form of a promotional gift of nominal value that you distribute. 3. You need a signed patient authorization if you disclose PHI to a gift distribution company that sends items on your behalf. 4. You may only disclose the least amount of PHI necessary to make the promotional gift. 5. You must safeguard the PHI and take reasonable steps to avoid incidental disclosures.	1. The government has defined a promotional gift of nominal value in a health care context other than HIPAA. It is not clear whether these definitions will carry over to HIPAA. In this other context, the government places a limit of $10 per item, $50 per year to the same individual on what is considered "nominal". New York does **NOT** allow any such gifts, no matter what their value. • Although there is no direct authority, you might be better able to claim this exception if your promotional gifts stay under these dollar limits. 2. If you need a signed patient authorization in order to use or disclose PHI in connection with a marketing communication, the authorization must state whether you will receive anything of value from a third party in connection with making the communication. This is in addition to satisfying all the core elements of an authorization.	1. List the marketing or advertising activities involving PHI that you do. Use the worksheet accompanying this chart, if desired. 2. Determine if any of these marketing or advertising activities involve any products or services that are not • your own, or • health care. 3. If your marketing or advertising efforts involve PHI and relate to the products or services of a third party, or relate to your own non-health care products or services, determine if they fall into any of the other marketing exceptions. 4. If you need a signed patient authorization for a particular marketing communication, be sure to include the special language about whether or not you are receiving anything of value in connection with the communication. 5. Write a policy that describes the following items: • How you use or disclose PHI for marketing or advertising. • When a signed patient authorization is needed. • Who in your practice will obtain signed authorizations, when they are needed. • How you will use the least amount of information necessary, and how you will safeguard PHI. (See charts 23-24.) 6. Keep this policy with your permanent office records. You may use model policy, #11A if desired.

YOU MAY NEED AN AUTHORIZATION TO USE OR DISCLOSE PHI FOR MARKETING OR ADVERTISING – IT DEPENDS ON THE AVAILABILITY OF AN EXCEPTION

Assessment Question	Conditions on Use/Disclosure	Comments	Action Steps
7. Do you send appointment reminders to patients?	1. You do not need a signed patient authorization in order to use PHI to send an appointment reminder to a patient, so long as you comply with the following points: • You may only use the least amount of PHI necessary to make the communication. • You must safeguard the PHI and take reasonable steps to avoid incidental disclosures.	1. Appointment reminders can be oral (usually by telephone) or written. 2. Appointment reminders can remind patients of an existing appointment, or can suggest that it is time for a patient to make a new appointment.	1. List the marketing or advertising activities involving PHI that you do. Use the worksheet accompanying this chart if desired. 2. Determine if any of these marketing or advertising activities involve any products or services that are not • your own, or • health care. 3. If your marketing or advertising efforts involve PHI and relate to the products or services of a third party, or relate to your own non-health care products or services, determine if they fall into any of the other marketing exceptions. 4. If you need a signed patient authorization for a particular marketing communication, be sure to include the special language about whether or not you are receiving anything of value in connection with the communication. 5. Write a policy that describes the following items: • How you use or disclose PHI for marketing or advertising. • When a signed patient authorization is needed. • Who in your practice will obtain signed authorizations, when they are needed. • How you will use the least amount of information necessary, and how you will safeguard PHI. (See charts 23-24.) 6. Keep this policy with your permanent office records. You may use model policy, #11A if desired.

YOU MAY NEED AN AUTHORIZATION TO USE OR DISCLOSE PHI FOR MARKETING OR ADVERTISING – IT DEPENDS ON THE AVAILABILITY OF AN EXCEPTION

Assessment Question	Conditions on Use/Disclosure	Comments	Action Steps
8. Do you ever sell PHI or receive anything of value from someone else for giving PHI to them so that they can market their own products or services?	1. You always need a signed patient authorization to sell PHI to someone else for their own marketing purposes. • The authorization must disclose the fact that you are receiving something of value for the PHI.	1. The most common example of this is selling your patient lists to someone so that they can mail your patients information about their products or services. HIPAA strictly regulates this behavior.	1. List the marketing or advertising activities involving PHI that you do. Use the worksheet accompanying this chart if desired. 2. Determine if any of these marketing or advertising activities involve any products or services that are not • your own, or • health care. 3. If your marketing or advertising efforts involve PHI and relate to the products or services of a third party, or relate to your own non-health care products or services, determine if they fall into any of the other marketing exceptions. 4. If you need a signed patient authorization for a particular marketing communication, be sure to include the special language about whether or not you are receiving anything of value in connection with the communication. 5. Write a policy that describes the following items: • How you use or disclose PHI for marketing or advertising. • When a signed patient authorization is needed. • Who in your practice will obtain signed authorizations, when they are needed. • How you will use the least amount of information necessary, and how you will safeguard PHI. (See charts 23-24.) 6. Keep this policy with your permanent office records. You may use model policy, #11A if desired.

YOU MAY NEED AN AUTHORIZATION TO USE OR DISCLOSE PHI FOR MARKETING OR ADVERTISING – IT DEPENDS ON THE AVAILABILITY OF AN EXCEPTION

Definitions - Question 1:

Marketing means:

1. To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

2. An arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.

45 CFR 164.502

Completed _____ Date _____

_____

Signature of responsible person

YOU MAY NEED AN AUTHORIZATION TO USE OR DISCLOSE PHI FOR MARKETING OR ADVERTISING – IT DEPENDS ON THE AVAILABILITY OF AN EXCEPTION (WORKSHEET)

Marketing Activity	Use or Disclose PHI (Yes/No)

Doctor's Name
Address
Phone

MARKETING AND ADVERTISING

Policy Number: 11A Effective Date _____

In order to comply with HIPAA's Privacy Rule, it is the policy of this office to require a signed patient authorization to use or disclose protected health information for marketing or advertising purposes, subject to the conditions and exceptions described in this policy.

1. Marketing means to make a communication that encourages the person receiving the communication to purchase a product or service.

2. We use protected health information in connection with a marketing communication if we review patient data bases or records to target the communication to specific recipients. We disclose protected health information in connection with a marketing communication if the content of the communication includes protected health information (photographs, testimonials, and the like).

3. If a marketing communication discloses protected health information, we will always get a signed patient authorization.

4. If we use protected health information in connection with a marketing communication, we will get a signed patient authorization, except for:

- Marketing communications about our own health care products or services.
- Communications made in the course of treatment, case management, or care coordination for an individual patient.
- Communications made during a face-to-face encounter with a patient.

Communications falling into these specified categories do not require a signed patient authorization.

5. Any marketing communication that does not require a signed patient authorization must be included in our accounting of disclosures available to a patient upon request.

6. When we need an authorization, we will include information about any money or other valuable thing that we get from someone else in connection with the communication.

7. Many marketing communications do not use or disclose protected health information. These communications are not affected by HIPAA's Privacy Rule. Examples of these communications are:

- general TV ads
- brochures mailed to "occupant" using a zip code data base

8. [Insert name/title] is responsible for obtaining signed patient authorizations for marketing, when they are required, and for making sure that the authorization discloses any money or thing of value that we get from someone else in connection with the marketing communication.

Completed _____ Date _____

YOU MAY NEED AN AUTHORIZATION TO USE OR DISCLOSE PHI FOR RESEARCH – IT DEPENDS ON THE AVAILABLE EXCEPTIONS

_____

Signature of responsible person

Assessment Question	Conditions on Disclosure	Comments	Action Steps
1. Do you participate in clinical trials? Do you participate in research that uses PHI but is not a clinical trial?	1. You need a signed patient authorization to use or disclose PHI for research, unless you fit one of HIPAA's three exceptions. The exceptions are: • An Institutional Review Board (IRB) or Privacy Board determines that the authorization requirement can be waived or altered. • You need the PHI exclusively for activities preparatory to research and you give certain assurances to the organization holding the PHI. • You want PHI exclusively about deceased people and you give certain assurances to the organization holding the PHI.	1. Clinical trials generally involve testing new drugs or medical devices on patients. Clinical trials always generate PHI, which is used by the researcher and shared with the research sponsor and the Food and Drug Administration (FDA). 2. Other types of research do not involve active treatment of patients, but use PHI. Examples include research using PHI already recorded in patients' clinical records. 3. You must follow HIPAA even if you are not getting federal money for your research, and even if you are not reporting information to the FDA. 4. If a signed patient authorization is needed, it may be combined with the patient's general agreement to participate in the clinical trial. This is an exception to the general rule that authorizations must stand alone.	

YOU MAY NEED AN AUTHORIZATION TO USE OR DISCLOSE PHI FOR RESEARCH – IT DEPENDS ON THE AVAILABLE EXCEPTIONS

Assessment Question	Conditions on Disclosure	Comments	Action Steps
2. How do you get a waiver from an IRB or Privacy Board?	1. In order to use or disclose PHI in connection with research without a signed authorization under the waiver exception, you must satisfy all of the following points: • You must have documentation that the IRB or the Privacy Board determined that a waiver is appropriate because it satisfies certain criteria stated in 45 CFR 512i) of the Privacy Rule. Generally, these criteria are that: – The use or disclosure of PHI during the research poses no more than minimal risk to the privacy of the research participants; – The PHI is necessary for the research; and – As a practical matter, the research could not proceed without a waiver. • You must have documentation of the IRB or the Privacy Board specification of what PHI can be used or disclosed as part of the waiver. • You must have documentation that the IRB or the Privacy Board made all its determinations according to proper procedures. • Your documentation must be signed by the chair of the IRB or Privacy Board. The documentation must include the name of the IRB or Privacy Board and the date of its approval of a waiver.	1. An IRB is an interdisciplinary group that protects the safety of human research subjects. IRBs already follow procedures and rules established under other laws. Almost all clinical trials are under the control of an IRB. 2. A "Privacy Board" is another interdisciplinary group that HIPAA defines. It must: • Have members from a variety of professions relevant to protecting privacy; • Have at least one member that is not connected with the researcher or the organization holding the PHI; • Not allow anyone to participate in the review of research if that person has a conflict of interest. A waiver from an IRB or Privacy Board does not substitute for other approvals that you must have as a researcher from an IRB. Typically, you will also need IRB approval of your research protocol and of your recruitment and patient consent forms.	1. If you regularly work with a particular IRB, discuss the waiver process with it and develop a protocol for submitting waiver requests. 2. Write a policy that includes the following points: • Who will be responsible for seeking a waiver and obtaining necessary documentation from the IRB or Privacy Board? • What information do you need to present to the IRB or Privacy Board so that they can make the necessary determinations? • How will ongoing communications with the IRB or Privacy Board, if any, be handled? 3. Keep this policy with your office's permanent records. See model policy #12A.

YOU MAY NEED AN AUTHORIZATION TO USE OR DISCLOSE PHI FOR RESEARCH – IT DEPENDS ON THE AVAILABLE EXCEPTIONS

Assessment Question	Conditions on Disclosure	Comments	Action Steps
3. Do you need PHI exclusively in order to prepare for research?	1. You do not need a signed patient authorization to use or disclose PHI in preparation for research, provided that you comply with the following points. 2. You must give the holder of the PHI specific assurances that: • You want to review or disclose PHI solely to prepare a research protocol or take other steps in preparation for research. These might include checking a data base to see if any patients are good candidates for the research. • You will not take PHI off-site from where it is held. • You need the PHI for your research purposes. • You may only use or disclose the least amount of PHI necessary to prepare for research. • You must safeguard the PHI and take reasonable steps to avoid incidental uses or disclosures.	1. It is unclear how to comply if you hold the PHI that you want to review to prepare for research. HIPAA contemplates that the PHI is held by another organization. 2. One suggestion is to write a statement containing the three points discussed under "conditions on disclosure", and to include the statement in your research records.	1. Consider and document what PHI you want to review in order to prepare for research. 2. Approach the holder of the PHI, if that is someone other than yourself. 3. Prepare a written statement containing the necessary representations and commitments, and deliver it to the holder of the PHI. If you hold the PHI, keep the statement in your research records. 4. Write a policy describing how you will handle situations in which you want to review PHI in preparation for research. Keep this policy with your office's permanent records. See model policy #12A.
4. Is your research limited to PHI about deceased people?	1. You do not need a signed patient authorization from a representative of a dead patient in order to conduct research on their PHI, so long as you comply with the following points. You must give the holder of the PHI specific assurances that: • You are asking for the PHI strictly to conduct research. • The person identified in the PHI is dead. You	Death certificates are typically available from state vital records offices for a small fee. Sometimes it can take several weeks to receive a death certificate from these offices.	1. Consider and document what PHI you want to use or disclose from the records of dead patients. 2. Approach the holder of the PHI, if that is someone other than yourself. 3. Prepare a written statement containing the necessary representations and commitments, and deliver it to the holder of the PHI. If you hold the PHI, keep the statement in

YOU MAY NEED AN AUTHORIZATION TO USE OR DISCLOSE PHI FOR RESEARCH – IT DEPENDS ON THE AVAILABLE EXCEPTIONS

Assessment Question	Conditions on Disclosure	Comments	Action Steps
	may have to supply a death certificate if the holder of the PHI asks for one. • You need the PHI in order to perform research.		your research records. 4. Obtain death certificates, if the holder of the PHI requests. 5. Write a policy describing how you will handle situations in which you want to review PHI in reparation for research. Keep this policy with your office's permanent records.

Doctor's Name
Address
Phone

DISCLOSURES FOR RESEARCH

Policy Number: 12A Effective Date _____

In order to comply with HIPAA's Privacy Rule, it is the policy of this office to obtain a signed patient authorization before using or disclosing protected health information for research purposes, unless the research satisfies one of HIPAA's exceptions to the need for authorization. In accordance with HIPAA's exceptions:

1. We will not obtain a signed patient authorization if a researcher has obtained, and presents to us, a proper waiver of authorization from an Institutional Review Board ("IRB") or Privacy Board.

2. An IRB is an interdisciplinary group convened to oversee the protection of human subjects in research, pursuant to regulations of the federal Food and Drug Administration or the "common rule". A Privacy Board is an interdisciplinary group that has members from a variety of professions relevant to protecting privacy, has at least one member that is not connected with the researcher or the organization holding the protected health information, and does not allow anyone to participate in the review of research if that person has a conflict of interest.

3. In order to be a proper waiver, the following criteria must be satisfied:

- We must have documentation that the IRB or the Privacy Board determined that a waiver is appropriate because:

    9. The use or disclosure of protected health information during the research poses no more than minimal risk to the privacy of the research participants;

    10. The protected health information is necessary for the research;

    11. As a practical matter, the research could not proceed without a waiver.

- We must have documentation of the IRB or the Privacy Board specification of what protected health information can be used or disclosed as part of the waiver.

- We must have documentation that the IRB or the Privacy Board made all its determinations according to proper procedures.

- The documentation must be signed by the chair of the IRB or Privacy Board. The documentation must include the name of the IRB or Privacy Board and the date of its approval of a waiver.

4. [Insert name/title] is responsible for obtaining proper IRB or Privacy Board waivers of authorization for research that we want to conduct without a signed patient authorization. [Insert name/title] will consult with the IRB or Privacy Board to determine what

information the IRB or Privacy Board wants in order to make its determinations. If an outside researcher wants to use protected health information about our patients, [insert name/title] is responsible for reviewing all documents that the researcher presents to us in support of a waver of authorization, to verify their sufficiency.

5. [Insert name/title] is responsible for any ongoing communication with an IRB or Privacy Board that has granted a waiver of authorization, if any is needed.

6. We will rely upon the IRB or Privacy Board's statement of the protected health information that is subject to the waiver as being the minimum amount of protected health information that is necessary for the research.

7. We will not obtain a signed patient authorization if a researcher gives us specific assurances that:

- The researcher wants to review or disclose protected health information solely to prepare a research protocol or take other steps in preparation for research. These might include checking a data base to see if any patients are good candidates for the research.

- The researcher will not take any protected health information off-site from where it is held.

- The researcher needs the protected health information for research purposes.

8. [Insert name or title] is responsible for reviewing all assurances that an outside researcher may give us in support of a disclosure of protected health information. [Insert name or title] is also responsible for providing specific assurances whenever we want to obtain protected health information from someone else for activities preparatory to research.

9. We will not obtain a signed patient authorization if a researcher wants the protected health information in order to conduct research solely on deceased patients and provides specific assurances that:

- The researcher is asking for protected health information strictly to conduct research.

- The person identified in the protected health information is dead. The researcher should supply a death certificate.

- The researcher needs the PHI in order to perform research.

10. If an authorization is needed, [insert name or title] is responsible for obtaining it, if we want to conduct the research. [Insert name/title] is also responsible for reviewing all authorizations presented to us by outside researchers.

Completed _____ Date _____

YOU MUST PREPARE A SPECIAL FORM FOR PATIENTS TO AUTHORIZE THE USE OR DISCLOSURE OF THEIR PHI

_____

Signature of responsible person

Question	Yes/No	Comments	Action Steps
1. Do you have a form that patients sign to allow you to use or disclose PHI?	If yes, compare your current form to the elements in the Action Steps in this chart. Note any needed revisions. Use the worksheet accompanying this chart, if desired. If no, go to the Action Steps column of this chart.	1. Under HIPAA, a patient authorization cannot be combined with any other patient permission forms. 2. Under HIPAA, patient authorizations must be completely filled out or you cannot rely upon them. 3. You cannot rely upon an authorization if you know that any information is materially false, or that the expiration date or event has passed. 4. You must keep copies of signed authorizations for at least six years. 5. You must give the patient a copy of any authorization that the patient signs.	1. HIPAA requires a particular kind of form for patients to authorize you to use or disclose their PHI, with some exceptions for disclosures that can be made without written permission. (See charts 8-12.) The HIPAA authorization form must: • Be in writing. • Be written in plain language. • Identify the person, organization, or classes of people or organizations that will use or disclose the PHI. • Identify the person, organization, or classes of people or organizations that will receive the PHI. • Identify with specificity the PHI that will be used or disclosed. • Identify the purpose(s) for the use or disclosure. If the patient initiates the request for a disclosure, it is sufficient if the authorization states "at the patient's request" for the purpose. • Identify an expiration date or event that is related to the purpose for the use or disclosure. • Be signed by the patient, or a HIPAA authorized personal representative of the patient. • Specify the authority through which the personal representative is acting in signing the form. • Inform the patient that the authorization can be revoked at any time, unless you have already disclosed PHI or taken other action in reliance upon the effectiveness of the authorization. • Inform the patient that you cannot refuse to serve him or her if he or she does not sign the authorization. • Inform the patient that the recipient of the disclosed PHI may not have any legal obligation to maintain the further confidentiality of the PHI. Policy 13A is a model authorization form. *Comment:* Some states have specific language or terms that must be in

Question	Yes/No	Comments	Action Steps
			patient authorization forms. If this information is not inconsistent with the HIPAA minimum content described in the Action Steps, it may be included in the authorization form. If the language or terms conflict with the HIPAA minimum content, see chart 31 regarding "preemption."
2. If the patient is not able to sign the authorization form, who currently signs it on behalf of the patient? **If someone other than the patient is signing the form, do you have a policy about who can do this?**	If yes, compare your policy with the items under Action Steps in this chart. Note any needed changes. Use the worksheet accompanying this chart if desired. If no, go to Action Steps.	Patients may not sign their own permission forms for a number of reasons. Sometimes it is because the law presumes that they are unable to sign, like a minor. Sometimes the patient has died. Sometimes the patient is mentally disabled or mentally incompetent due to conditions like developmental disability or senility. Other times, the patient may have a physical handicap that interferes with writing. Different people are authorized to sign on behalf of patients in these different circumstances. HIPAA lets your state law determine who can substitute for the patient. HIPAA gives you the discretion not to work with someone who would ordinarily be a personal representative if you think that this person may have abused or neglected the patient, or that the patient may be endangered if you work with them. This usually applies when you think that giving someone access to PHI would	1. HIPAA requires that you have a written policy describing who can sign on behalf of a patient, and what documentation you need to support such signatures. The policy should include the following points: • Identify who, under your state law, is authorized to act on behalf of an adult patient. For example, many states allow a court appointed guardian or a health care power of attorney to agree to disclosure of PHI for an adult patient who cannot personally make that decision. Some states may permit family members to do this as well. Consult your own attorney or advisor. • Identify who, under your state law, has authority to act for a deceased individual or the deceased individual's estate. Some states permit court-appointed Executors, Administrators or personal Representatives to have this authority. Some states may permit some close family members to have this authority. Consult your own attorney or advisor. • Identify who, under your state law, is a "person in loco parentis" regarding a minor patient, who can make health care decisions for the minor. Some states consider foster parents or step parents to qualify. Consult your own attorney or advisor. HIPAA also allows parents and legal guardians of minor patients to sign authorizations. • On an authorization form, accept the signature of any of the individuals identified in the preceding three bullet points. • Obtain copies of court orders appointing the signer as applicable. • Obtain copies of other documents establishing the signer's authority to act on behalf of the patient, if applicable. For example, copies of status as a foster parent, or a power of attorney for health care. • Retain all documents, including the signed authorization, for a minimum of six years.

YOU MUST PREPARE A SPECIAL FORM FOR PATIENTS TO AUTHORIZE THE USE OR DISCLOSURE OF THEIR PHI

Question	Yes/No	Comments	Action Steps
		cause a continuation or worsening of abusive or neglectful behavior or endanger the patient.	• Identify the situations in which you do not have to accept a person as a personal representative. See model policy 13B.

Completed _____ Date _____

YOU MUST PREPARE A SPECIAL FORM FOR PATIENTS TO AUTHORIZE THE USE OR DISCLOSURE OF THEIR PHI (WORKSHEET)

_____

Signature of responsible person

Current Form or Policy	Needed Changes
Patient Permission Form	
Policy on Substitute Signers	

_____, D.D.S. or D.M.D.
[*address*]
[*phone number*]
[*fax number*]
[*E Mail*]
[o*ffice contact person*]

AUTHORIZATION FOR RELEASE OF IDENTIFYING HEALTH INFORMATION

Patient name_____

Patient number _____

Patient address _____

Patient phone number _____

I authorize the professional office of my dentist named above to release health information identifying me [including if applicable, information about HIV infection or AIDS, information about substance abuse treatment, and information about mental health services] under the following terms and conditions:

1. Detailed description of the information to be released:

2. To whom may the information be released [name(s) or class(es) of recipients]:

3. The purpose(s) for the release (if the authorization is initiated by the individual, it is permissible to state "at the request of the individual" as the purpose, if desired by the individual):

4. Expiration date or event relating to the individual or purpose for the release:

It is completely your decision whether or not to sign this authorization form. We cannot refuse to treat you if you choose not to sign this authorization.

If you sign this authorization, you can revoke it later. The only exception to your right to revoke is if we have already acted in reliance upon the authorization. If you want to revoke your authorization, send us a written or electronic note telling us that your authorization is revoked. Send this note to the office contact person listed at the top of this form.

When your health information is disclosed as provided in this authorization, the recipient often has no legal duty to protect its confidentiality. In many cases, the recipient may re-disclose the information as he/she wishes. Sometimes, state or federal law changes this possibility.

[For marketing authorizations, include, as applicable: We will receive direct or indirect remuneration from a third party for disclosing your identifiable health information in accordance with this authorization.]

I HAVE READ AND UNDERSTAND THIS FORM. I AM SIGNING IT VOLUNTARILY. I AUTHORIZE THE DISCLOSURE OF MY HEALTH INFORMATION AS DESCRIBED IN THIS FORM.

Dated _____ Patient signature _____

If you are signing as a personal representative of the patient, describe your relationship to the patient and the source of your authority to sign this form:

Relationship to Patient _____ Print Name _____

Source of Authority _____

Doctor's Name
Address
Phone

PERSONAL REPRESENTATIVES FOR PATIENTS

Policy Number: 13B Effective Date _____

In order to comply with HIPAA's Privacy Rule, it is the policy of this office to allow properly authorized personal representatives to stand in the shoes of a patient in order to exercise all the rights that the patient could exercise regarding the use and disclosure of protected health information and to give any required permission for a use or disclosure of protected health information.

1. Adult patients and emancipated minors:

- Adult patients are those over the age of [specify the age of majority in your state].

- Emancipated minors are people under the age of [specify age of majority in your state] who have the legal right to be treated as an adult. This happens if [specify how a minor becomes emancipated under your state laws].

- Generally, adults and emancipated minors personally handle all matters about their protected health information. Sometimes, however, they may be unable to do so because of mental incapacity. In this case, the following people can substitute for the adult or emancipated minor to sign all permissions and exercise all rights regarding protected health information:

  [specify legally authorized representatives under your state law].

2. Unemancipated minors

- An unemancipated minor is a person under the age of [specify the age of majority in your state].

- Generally unemancipated minors are not able to handle any matters regarding their protected health information because the law presumes them to be incapacitated. The following people can handle signing all permissions and exercise all rights regarding an unemancipated minor's protected health information:

  12. either parent. [Add any special rules in your state if the parents are divorced.]

  13. a court appointed guardian

14. the following people who are considered to be "in loco parentis" –

[specify others authorized by your state law to act for an unemancipated minor].

3. Deceased patients

- The following people have the authority to sign permissions and exercise rights regarding the protected health information of deceased patients:

  [specify those people with authority under your state law to act on behalf of a deceased patient, or the deceased patient's estate]

4. In a few instances, we will not work with the personal representatives listed above. This can happen in the following cases:

- We think that a person claiming to be a personal representative has or may have committed domestic violence, abuse, or neglect against the patient, and it is not in the patient's best interest to treat that person as the personal representative.

- We think that treating such person as the personal representative could endanger a patient, and it is not in the patient's best interest to treat that person as the personal representative.

5. Before we work with someone claiming to be a personal representative, we will check out their authority. This might include:

- checking identification

- looking at court or other documents

- consulting our attorney

If we are unsure of a person's authority to sign permissions or exercise rights regarding protected health information, we will not use or disclose that protected health information until any ambiguity is resolved.

Completed _____ Date _____

YOU MUST NOTIFY PATIENTS ABOUT PRIVACY

_____

Signature of responsible person

Requirement	Comments	Action Steps
1. You must prepare and use a written notice of privacy practices.	1. You must prepare and use a notice of privacy practices that contains, at a minimum, the terms specified in 45 CFR 164520. You can include additional terms that are not inconsistent. You must also describe ways that your state law or your own policies provide more privacy for patients. The minimum terms are: • The notice must contain the following statement as a header or otherwise prominently displayed: – THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY. – • A description, including at least one example, of the types of uses and disclosures of PHI that you are permitted to make for treatment, payment, and health care operations. If your state law has stricter requirements than HIPAA's Privacy Rule, you must discuss those in the notice. You must include sufficient detail to place the patient on notice of the uses and disclosures that are permitted or required. • A description of each of the other purposes for which you are permitted or required to use or disclose PHI without the patient's written authorization. If your state law has stricter requirements than HIPAA's Privacy Rule, you must discuss those in the notice. You must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required. • A statement that you will make other uses and disclosures of PHI only with the patient's written authorization and that the patient may revoke his or her authorization at any time unless you have already acted in reliance on it. • If you want to use appointment reminders, or inform patients about alternate services or products that might benefit him or her, the notice must state that you will do so. • If you are a nonprofit organization and want to contact patients for fundraising, the notice must so state. • The notice must contain a description of the patient's right to request restrictions on certain uses	1. Obtain a notice of privacy practices. • Use the model notice, policy #14A if desired. • Tailor the notice to your practice and to your state laws. 2. Decide how you will get patient acknowledgements. 3. Write a policy about distributing the notice and getting the acknowledgement. The policy should specify: • Who in your practice is responsible for distributing the notice and asking for the acknowledgements. • When the notice will be given to patients and how. • Who will decide whether to change a notice and how changes will be made. • Where acknowledgements and other related documentation will be stored.

YOU MUST NOTIFY PATIENTS ABOUT PRIVACY

Requirement	Comments	Action Steps
	and disclosures of PHI and how to exercise that right. The notice must also state that you are not obligated to agree to these requests. • The notice must contain a description of the patient's right to communicate with you through confidential methods, and how the patient can exercise that right. • The notice must contain a description of the patient's right to inspect and copy their own PHI and how to exercise that right. • The notice must contain a description of the patient's right to amend his or her own PHI, and how the patient may exercise that right. • The notice must contain a description of the patient's right to receive an accounting of disclosures of his or her PHI and how the patient may exercise that right. • The notice must contain a description of the patient's right to get extra hard copies of your notice, and how the patient may exercise that right. • The notice must contain a statement that you are required by law to maintain the privacy of PHI and to distribute a notice of your privacy practices. • The notice must contain a statement that you are required to abide by the terms of the notice currently in effect. • The notice must contain the effective date of the notice. If you want to be able to change your notice and have the revised terms apply retroactively, you must so state in the notice. You must also advise patients how they will get a revised notice under these circumstances. • The notice must contain a description of a patient's right to complain to you or DHHS, and how to exercise that right. • The notice must contain the name, or title, and telephone number of a person or office that the patient may contact for further information about privacy matters.	

YOU MUST NOTIFY PATIENTS ABOUT PRIVACY

Requirement	Comments	Action Steps
2. You must distribute the notice to your patients.	1. You have to give the notice to all of your patients the first time that you see them after April 14, 2003. You can use hard copy or electronic versions of the notice. If your email informs you that an electronic version was not received, you must give it to the patient some other way. 2. You must post the notice in your office. You can put a copy on a bulletin board, make a sign, or use some other method to post it. 3. You must have "take away" hard copies in your office so that patients and visitors can take a copy of your notice. 4. If you change your notice, you must re-distribute it.	
3. You must make a good faith effort to get a written acknowledgement from the patient of receipt of the notice of privacy practices.	1. You can use any form of acknowledgement that you like so long as it is written. 2. The patient must sign, initial or otherwise designate receipt. Email is permitted. 3. You do not have to guarantee that you have an acknowledgement from every patient who gets the notice of privacy practices. You just need to make a good faith effort to get one. Good faith efforts include asking the patient to sign during a treatment encounter, and sending the acknowledgement to the patient in the mail. 4. You must keep the acknowledgement for at least six years. 5. If the patient does not provide a written acknowledgement, you must document your efforts and why they were not successful. You must keep this documentation for at least six years. 6. You can store the acknowledgements and other documentation anywhere that you like. One possibility is in the patient's clinical record; another is with your administrative records.	

[Doctor's Name]
[Address]
[Phone]

NOTICE OF PRIVACY PRACTICES

Policy Number: 14A Effective Date _____

In order to comply with HIPAA's Privacy Rule, it is the policy of this office to:

1. Distribute a Notice of Privacy Practices ("NPP") to every patient at their first appointment, dentalwear pickup, or similar encounter on or after April 14, 2003.

- The NPP to use is attached to this Policy. Only [insert name or title] has authority to change this NPP.
- [Insert name/title] is responsible to distribute the NPP.
- [Insert name/title of responsible person from paragraph b.] must give the patient a copy of the NPP when [specify appropriate point in encounter].
- [Insert name/title of responsible person from paragraph b.] must ask the patient to sign an acknowledgement of receipt of the NPP ("AOR"). The AOR to use is attached to this Policy. Put all signed AORs in [selected location in your office].
- If the patient opts not to sign the AOR, [insert name/title of responsible person from paragraph b.] must make a note of the fact that you asked and that the patient refused. Put this note in [selected location in your office where you keep AORs.]
- It is not necessary to give a NPP to a patient every time they come in after April 14, 2003 unless we change the NPP.

    15. At every patient encounter, [insert name/title of responsible person from paragraph b.] must look in [specify location in your office where AORs of NPPs are stored] to determine if the patient has previously signed an AOR.

    16. If yes, it is not necessary to give that patient another NPP unless we have changed our NPP since the date of the AOR. Our most current NPP will always have an effective date on the front.

    17. If no, then it is necessary to distribute a NPP and ask for signature on an AOR.

- If our first encounter with a patient after April 14, 2003 is electronic, our electronic system will automatically send a NPP and ask for a signed AOR.

2. Post a copy of our NPP on [specify a prominent location in your office].

3. Keep a stock of copies of the NPP in [specify an accessible location in your office] so that patients and visitors can take one, if they wish.

4. Redistribute our NPP as above whenever we change it.

5. We will use and disclose protected health information in a manner that is consistent with HIPAA and with our NPP. If we change our NPP, the revised NPP will apply to all protected health information that we have, not just protected health information that we generate or obtain after we have changed the NPP.

Effective date of notice: _____

NOTICE OF PRIVACY PRACTICES

_____, D.D.S.
[*mailing address*]
[*phone number*]
[*fax number*]
[*E Mail*]
[*office contact person*]

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

We respect our legal obligation to keep health information that identifies you private. We are obligated by law to give you notice of our privacy practices. This Notice describes how we protect your health information and what rights you have regarding it.

TREATMENT, PAYMENT, AND HEALTH CARE OPERATIONS

The most common reason why we use or disclose your health information is for treatment, payment or health care operations. Examples of how we use or disclose information for treatment purposes are: setting up an appointment for you; examining your teeth, mouth, and oral health; prescribing medications and faxing them to be filled; prescribing dental appliances and dental prostheses; showing you treatment options; referring you to another dentist for specialty care; or getting copies of your health information from another professional that you may have seen before us. Examples of how we use or disclose your health information for payment purposes are: asking you about your dental or medical care plans, or other sources of payment; preparing and sending bills or claims; and collecting unpaid amounts (either ourselves or through a collection agency or attorney). "Health care operations" mean those administrative and managerial functions that we have to do in order to run our office. Examples of how we use or disclose your health information for health care operations are: financial or billing audits; internal quality assurance; personnel decisions; participation in managed care plans; defense of legal matters; business planning; and outside storage of our records.

We routinely use your health information inside our office for these purposes without any special permission. If we need to disclose your health information outside of our office for these reasons, [we will] [we usually will not] ask you for special written permission.

[We will ask for special written permission in the following situations: anything related to HIV/AIDS status, any sale of information, any use of information for marketing or fundraising purposes, and _____ .]

USES AND DISCLOSURES FOR OTHER REASONS WITHOUT PERMISSION

In some limited situations, the law allows or requires us to use or disclose your health information without your permission. Not all of these situations will apply to us; some may never come up at our office at all. Such uses or disclosures are:

- when a state or federal law mandates that certain health information be reported for a specific purpose;
- for public health purposes, such as contagious disease reporting, investigation or surveillance; and notices to and from the federal Food and Drug Administration regarding drugs or medical devices;
- disclosures to governmental authorities about victims of suspected abuse, neglect or domestic violence;
- uses and disclosures for health oversight activities, such as for the licensing of doctors; for audits by Medicare or Medicaid; or for investigation of possible violations of health care laws;

- disclosures for judicial and administrative proceedings, such as in response to subpoenas or orders of courts or administrative agencies;
- disclosures for law enforcement purposes, such as to provide information about someone who is or is suspected to be a victim of a crime; to provide information about a crime at our office; or to report a crime that happened somewhere else;
- disclosure to a medical examiner to identify a dead person or to determine the cause of death; or to funeral directors to aid in burial; or to organizations that handle organ or tissue donations;
- uses or disclosures for health related research;
- uses and disclosures to prevent a serious threat to health or safety;
- uses or disclosures for specialized government functions, such as for the protection of the president or high ranking government officials; for lawful national intelligence activities; for military purposes; or for the evaluation and health of members of the foreign service;
- disclosures of de-identified information;
- disclosures relating to worker's compensation programs;
- disclosures of a "limited data set" for research, public health, or health care operations;
- incidental disclosures that are an unavoidable by-product of permitted uses or disclosures;
- disclosures to "business associates" who perform health care operations for us and who commit to respect the privacy of your health information.

APPOINTMENT REMINDERS

We may call or write to remind you of scheduled appointments, or that it is time to make a routine appointment. We may also call or write to notify you of other treatments or services available at our office that might help you. Unless you tell us otherwise, we will mail you an appointment reminder on a post card, and/or leave you a reminder message on your home answering machine or with someone who answers your phone if you are not home.

OTHER USES AND DISCLOSURES

We will not make any other uses or disclosures of your health information unless you sign a written "authorization form." The content of an "authorization form" is determined by federal law. Sometimes, we may initiate the authorization process if the use or disclosure is our idea. Sometimes, you may initiate the process if it's your idea for us to send your information to someone else. Typically, in this situation you will give us a properly completed authorization form, or you can use one of ours.

If we initiate the process and ask you to sign an authorization form, you do not have to sign it. If you do not sign the authorization, we cannot make the use or disclosure. If you do sign one, you may revoke it at any time unless we have already acted in reliance upon it. Revocations must be in writing. Send them to the office contact person named at the beginning of this Notice.

YOUR RIGHTS REGARDING YOUR HEALTH INFORMATION

The law gives you many rights regarding your health information. You can:

- ask us to restrict our uses and disclosures for purposes of treatment (except emergency treatment), payment or health care operations. We do not have to agree to do this, but if we agree, we must honor the restrictions that you want. We must honor a restriction not to send information to a health care plan regarding any service for which you have already made full payment. To ask for a restriction, send a written request to the office contact person at the address, fax or E Mail shown at the beginning of this Notice.
- ask us to communicate with you in a confidential way, such as by phoning you at work rather than at home, by mailing health information to a different address, or by using E mail to your personal E Mail address. We will accommodate these requests if they are reasonable, and if you pay us for any extra cost. If you

want to ask for confidential communications, send a written request to the office contact person at the address, fax or E mail shown at the beginning of this Notice.

- ask to see or to get photocopies of your health information. By law, there are a few limited situations in which we can refuse to permit access or copying. For the most part, however, you will be able to review or have a copy of your health information within 10 days of asking us. You may have to pay for photocopies in advance. If we deny your request, we will send you a written explanation, and instructions about how to get an impartial review of our denial if one is legally available. If you want to review or get photocopies of your health information, send a written request to the office contact person at the address, fax or E mail shown at the beginning of this Notice.

- ask us to amend your health information if you think that it is incorrect or incomplete. If we agree, we will amend the information within 60 days from when you ask us. We will send the corrected information to persons who we know got the wrong information, and others that you specify. If we do not agree, you can write a statement of your position, and we will include it with your health information along with any rebuttal statement that we may write. Once your statement of position and/or our rebuttal is included in your health information, we will send it along whenever we make a permitted disclosure of your health information. By law, we can have one 30 day extension of time to consider a request for amendment if we notify you in writing of the extension. If you want to ask us to amend your health information, send a written request, including your reasons for the amendment, to the office contact person at the address, fax or E mail shown at the beginning of this Notice.

- get a list of the disclosures that we have made of your health information within the past six years (or a shorter period if you want). By law, the list will not include: disclosures for purposes of treatment, payment or health care operations; disclosures with your authorization; incidental disclosures; disclosures required by law; and some other limited disclosures. You are entitled to one such list per year without charge. If you want more frequent lists, you will have to pay for them in advance. We will usually respond to your request within 60 days of receiving it, but by law we can have one 30 day extension of time if we notify you of the extension in writing. If you want a list, send a written request to the office contact person at the address, fax or E mail shown at the beginning of this Notice.

- get additional paper copies of this Notice of Privacy Practices upon request. It does not matter whether you got one electronically or in paper form already. If you want additional paper copies, send a written request to the office contact person at the address, fax or E mail shown at the beginning of this Notice.

- be notified by us in a timely manner of any breach of the privacy and confidentiality of your unsecured protected health information, which we will provide to you in accordance with law and take all appropriate measures to address

OUR NOTICE OF PRIVACY PRACTICES

By law, we must abide by the terms of this Notice of Privacy Practices until we choose to change it. We reserve the right to change this notice at any time as allowed by law. If we change this Notice, the new privacy practices will apply to your health information that we already have as well as to such information that we may generate in the future. If we change our Notice of Privacy Practices, we will post the new notice in our office, have copies available in our office, and post it on our Web site.

COMPLAINTS

If you think that we have not properly respected the privacy of your health information, you are free to complain to us or the U.S. Department of Health and Human Services, Office for Civil Rights. We will not retaliate against you if you make a complaint. If you want to complain to us, send a written complaint to the office contact person at the address, fax or E mail shown at the beginning of this Notice. If you prefer, you can discuss your complaint in person or by phone.

FOR MORE INFORMATION

If you want more information about our privacy practices, call or visit the office contact person at the address or phone number shown at the beginning of this Notice.

----------tear here----------

ACKNOWLEDGEMENT OF RECEIPT

I acknowledge that I received a copy of [*name of dentist's*] Notice of Privacy Practices.

Patient name _____

Signature _____ Date _____

Completed _____ Date _____

YOU NEED TO ALLOW PATIENTS TO INSPECT AND COPY THEIR PHI

_____

Signature of responsible person

Requirement	Comments	Action Steps
1. Patients have a right to inspect or copy PHI about them if the information is contained in a "designated record set."	A designated record set is defined at 45 CFR 164.501. It includes all records containing PHI that you use to make decisions about a particular patient. At a minimum, this includes: • Clinical record • Billing record	1. Determine if you have any records other than billing records and clinical records that meet the definition of "designated record set." 2. Define your designated record set in a written policy. You can use model policy 15A, if desired. 3. Keep this policy with your office's permanent records.
2. Decide who in your office will be responsible for handling patient's inspection and copying requests.	This person could be your Public Information Officer, if you wish. Or it could be any other person who has time to handle this responsibility.	1. Designate the person who will handle inspection and copying requests in writing. 2. Keep this designation in your office's permanent records.
3. After receiving a patient's request to inspect or copy their PHI, you must either grant or deny it within 10 days.		1. Use the model letter accompanying this chart, if desired.
4. You can deny the patient's request only for any of the following reasons: • A patient cannot inspect or copy information if the requested PHI is not in a designated record set. • A patient cannot inspect or copy information if the requested PHI was prepared in connection with a lawsuit. • A patient cannot inspect or copy information if the requested PHI is generated as part of the patient's participation in a clinical trial and the request is made during the clinical trial. You must have informed the patient about this restriction when	1. If you refuse a patient or personal representative access to their PHI for any of the last three reasons, you must give the patient a chance to have your decision reviewed by another health care professional who was not involved in the final decision. Otherwise, the patient has no right to ask for a review of your refusal. 2. If you refuse a patient or personal	1. Designate a licensed health care professional to act as the "review officer." 2. Prepare master letters to send to patients if you deny a request to inspect or copy their PHI. You will need two letters: • One saying that you deny the request and stating the reasons. • One stating that you deny the request, stating the reasons and describing the patient's review rights. 3. If you are denying a patient request to inspect

YOU NEED TO ALLOW PATIENTS TO INSPECT AND COPY THEIR PHI

Requirement	Comments	Action Steps
the patient signed up for the clinical trial. The patient must be allowed to inspect or copy this PHI when the clinical trial is over. • A patient cannot inspect or copy information if you got the information from someone else who is not a health care provider, and you promised that person that his/her identity would remain confidential. • A patient cannot inspect or copy information if you, or another health care professional, determine that this would likely endanger the life or physical safety of the patient or someone else. • A patient cannot inspect or copy information if it references someone else, and you, or another health care professional, determine that access would likely cause substantial harm to such other person. • A patient's personal representative (for example, legal guardian, or parent of a minor) cannot inspect or copy information about the patient if you, or another health care professional, determines that this would likely cause substantial harm to the patient or another person. If you have a record that contains some PHI that falls into one of the reasons for denial , and some that does not, you must allow the patient or personal representative to access the PHI that doesn't fall into the reason for denial. If you do not have the PHI that the patient wants, you must tell the patient where to get it.	representative access to PHI for any reasons(whether or not you have to give a patient a review of that decision), you must give them a written explanation of your reason.	or copy, the letter has to include certain minimum terms specified by HIPAA. These are: • The basis for the denial. • If applicable, a statement of the patient's right to review and how to exercise the review rights, and • A description of how to complain to you or to DHHS. You must include the name, or title, and telephone number of the contact person or office that you have designated to handle complaints. (See chart 27.) • Use the model letters accompanying this chart, if desired. 4. Decide how review of a denied patient request will be handled. 5. Write a policy describing the denial of access. This can be part of a single policy describing all access rights. Keep this policy with your office's permanent records. Use model policy 15B, if desired.

YOU NEED TO ALLOW PATIENTS TO INSPECT AND COPY THEIR PHI

Requirement	Comments	Action Steps
5. If there is no basis to deny a request, you must allow a patient (or authorized representative) to inspect or copy their PHI.	1. You must give the patient access to the information in the form or format they request if the information is readily producible in that form or format. If it is not, then you must produce a readable hard copy unless you and the patient agree upon some other form or format. 2. You can provide a summary or an explanation of the requested information instead of giving the patient access to the information, if the patient agrees in advance (including to any fees involved). 3. You can charge a fee for copies. The fee must: • Be reasonable; paper copies cannot exceed 75 cents per page. • Cover only the cost of actual cost of copying. 4. You cannot charge for search and retrieval. 5. You must allow the patient to inspect or copy at a time they choose (within reason).	1. You must send the patient a letter advising that you are granting access to their PHI and setting up the time, place, and manner of the inspection or copying. 2. Write a policy describing how you will handle patient access requests. Use model policy 15B, if desired. Use the model letter, if desired.

Doctor’s Name
Address
Phone

DESIGNATED RECORD SET

Policy Number: 15A Effective Date _____

In order to comply with HIPAA's Privacy Rule, this office designates the following records to be our "designated record set" for purposes of patients' right to access and amend their protected health information:

1. The patient's clinical chart, hard copy or electronic:

    18. reports of screening and diagnostic tests
    19. notes on examinations
    20. consultant reports
    21. refraction results
    22. dental device prescriptions
    23. history and medication reports
    24. all other clinical information

2. The patient's billing records, hard copy or electronic:

    25. insurance claims
    26. remittance advice from insurance companies
    27. electronic fund deposit receipts
    28. bills to patients
    29. evidence of payment by patients
    30. collection records
    31. referrals to collection agencies or attorneys
    32. reports to consumer credit agencies for unpaid balances
    33. all other billing, claim, payment and collection records

3. Dental device order and receipt forms specific to a particular patient, hard copy or electronic:

    34. orders for dental prostheses
    35. orders for other dental devices
    36. acceptance of delivery of ordered dental devices
    37. patient pick up records
    38. repair requests and documentation of completion
    39. fitting information
    40. distribution of dental device accessories
    41. any other records relating to dental devices

4. [Specify other information in any form that you use to make decisions about a particular patient. This does not include any documents created in connection with litigation.]

Doctor's Name
Address
Phone

PATIENTS' ACCESS TO THEIR PROTECTED HEALTH INFORMATION

Policy Number: 15B Effective Date _____

In order to comply with HIPAA's Privacy Rule, it is the policy of this office to allow patients to inspect and/or copy their own protected health information under the conditions stated in this policy. If the patient has a personal representative (see policy #13B), the personal representative can inspect or copy the patients protected health information on behalf of the patient.

1. We may require that patients send a written request to inspect or copy their protected health information. If a patient calls on the telephone asking to inspect or copy their protected health information, we will inform the patient if we require the patient to send the request in writing.

2. Our public information officer is responsible for handling patient requests to inspect or copy their protected health information.

3. We will respond to a patient's request to inspect or copy their protected health information within 10 days of receiving a written request. Use the form letter, attached.

4. We can deny the patient's request only for one or more of the following reasons:

a. A patient cannot inspect or copy information if it was prepared in connection with a lawsuit.

b. A patient cannot inspect or copy information if it is generated as part of the patient's participation in a clinical trial and the request is made during the clinical trial. We must have informed the patient about this restriction when the patient signed up for the clinical trial. The patient must be allowed to inspect or copy this information when the clinical trial is over.

c. A patient cannot inspect or copy information if we got the information from someone else who is not a health care provider, and we promised that person that his/her identity would remain confidential.

d. A patient cannot inspect or copy information if we, or another health care professional, determine that this would likely endanger the life or physical safety of the patient or someone else.

e. A patient cannot inspect or copy information if it references someone else, and we, or another health care professional, determine that access would likely cause substantial harm to such other person.

f. A patient's personal representative (for example, legal guardian, or parent of a minor) cannot inspect or copy information about the patient if we, or another health care

professional, determines that this would likely cause substantial harm to the patient or another person.

g. A patient cannot inspect or copy information that is not in a designated record set. (See policy #15A.)

5. If we deny a patient access to their protected health information, we will notify the patient of our decision.

6. If the denial is based upon reasons 4 d, e, or f, the patient has a right to a review of our decision.

a. [Insert name or title, a licensed health care professional] will handle the review.

b. Our public information officer will look at the information that the patient wants to inspect or copy, and decide if we were correct in thinking that the patient's circumstances meet the specifications of paragraph 4d, e, or f.

(i) If not, the patient may inspect or copy the information.
(ii) If so, the patient may not inspect or copy the information.

The patient may not further question our decision. Our notice to the patient will include instructions about how the patient may take advantage of this review right. We will use the denial notice letter accompanying this policy.

7. When we permit a patient to inspect or copy the requested information, we will:

a. Provide the information in the form or format that the patient requests, if we can reasonably produce it that way. If we cannot, we will either agree with the patient about another format or give it to the patient in hard copy.

b. Allow the patient to inspect or copy the information at our office during normal business hours. Within these limits, the patient can select the date and time to inspect or copy the records.

c. Charge the patient [insert price per page] for copying the requested information for the patient.

d. If the patient agrees in advance, we may summarize the requested information and give this to the patient instead of having the patient inspect all the information or copy all of it. If we do this, we will charge the patient the cost of preparing the summary. We will collect all charges before preparing the summary.

8. We will notify the patient that their request to access information is granted. We will use the access notice letter attached to this policy.

[office letterhead]

[patient address info]

Dear [name of patient]:

Thank you for your request to inspect or copy information that we have about you. Ordinarily, we would be able to respond to your request within 10 days, but due to unusual circumstances we need an additional 10 days in order to respond to you. Accordingly, please expect to hear from us by [insert farthest date].

We look forward to working with you in the future.

[signature block]

[office letterhead]

[patient address info]

Dear [name of patient]:

Thank you for your request to inspect or copy information that we have about you. We are pleased to be able to grant this request.

If you want to inspect your information or make copies of it yourself, you may do so at our office during our normal business hours. Please let us know what date and time you would like to come. We will do our best to accommodate your requested date and time.

If you would like us to make a copy of your information for you, we are happy to do so. However, we will charge you [insert price per page].

If you prefer, we can summarize our information and give that to you instead of having you inspect or copy all of the information. If you want to do this, we will charge [insert price for a summary], and we require payment of this amount before we start making the summary.

You requested the information in [insert form or format requested]. We [can/cannot] accommodate that form or format. [Because we cannot accommodate that form or format, we will provide the information to you in hard copy, unless we can agree upon some other format that we can accommodate.]

Thank you again for your request. We look forward to working with you in the future.

[signature block]

[office letterhead]

[patient address info]

Dear [name of patient]:

Thank you for your request to inspect or copy information that we have about you. Unfortunately, we are unable to permit you to inspect or copy this information.

The reason for this denial is:

[specify one or more permitted reason(s).]

[You are entitled to one review of our decision. If you want to request a review, send a written request to [insert name/title of person designated in paragraph 5 of your access policy] at the address shown in our letterhead. [Insert name/.title of person designated in paragraph 5 of your access policy] will look at the information that you want to inspect or copy, and decide if our decision is correct. If it is, you will not be able to inspect or copy the information. If [insert name/title of the person designated in paragraph 5 of your access policy] concludes that we were wrong in denying you access to the information, you will be able to inspect or copy it, and we will be back in contact with you.]

You always have the option to complain to us, to complain and request review by the New York State Department of Health, or to complain to the U.S. Department of Health and Human Services – Office for Civil Rights if you think that we have not properly respected your privacy. If you want to complain to us, write or call [insert name of public information officer] at the address or phone number in our letterhead.

Thank you again for your request. We look forward to working with you in the future.

[signature block]

Completed _____ Date _____

YOU NEED TO AMEND PHI UPON REQUEST IF IT IS INACCURATE OR INCOMPLETE

_____

Signature of responsible person

Requirement	Comments	Action Steps
1. A patient has a right to amend the PHI that you have about them if the PHI is contained in a "designated record set."	A designated record set is defined at 45 CFR 164.501. It includes all records containing PHI that you use to make decisions about a particular patient. At a minimum, this includes: • Clinical record • Billing record	1. Determine if you have any records other than billing records and clinical records that meet the definition of designated record set. 2. Define your designated record set in a written policy. Use model policy 16A, if desired. 3. Keep this policy with your office's permanent records.
2. Identify someone in your office to handle patient requests to amend their PHI.	This can be your public information officer, if you wish. Or it can be anyone else who has time to handle this responsibility.	1. Designate the identified person in a written policy. 2. Keep this policy with your office permanent records.
3. After receiving a request to amend PHI, you must either grant or deny it within 30 days.		1. Prepare a model extension letter. Use the extension letter accompanying this chart, if desired.
4. You can deny a patient's request to amend his/her PHI only for any of the following reasons: • The PHI is accurate and complete as it is. • You did not create the PHI. • The PHI is not in a designated record set. • The patient would not be able to inspect or copy the PHI. (See chart 15.)	1. If you deny a request to amend PHI for one of the listed reasons, you must send the patient a written notice. The denial notice must include minimum terms specified by HIPAA. The minimum terms are: • The basis for the denial. • A description of the patient's right to write a "statement of disagreement" or alternatively, to have the original request sent with future disclosures of the contested PHI. • A description of how to complain to you or DHHS, including the name or title and phone number of the person handling complaints. 2. If you refuse to amend the PHI, the patient can either: • Write a statement disagreeing with your refusal, to be	1. Prepare a model denial letter. Use the denial letter accompanying this chart, if desired. 2. Decide how you will handle "statements of disagreement" from patients: • Will you write a rebuttal? • How will you append or link the information? 3. Write a policy describing how you will handle amendment requests. (See Requirement 5, Action Steps.) 4. Use model policy 16B, if desired. 5. Keep this policy with your office's permanent records.

YOU NEED TO AMEND PHI UPON REQUEST IF IT IS INACCURATE OR INCOMPLETE

Requirement	Comments	Action Steps
	included with future disclosures of the PHI. • Ask you to send the original amendment request along with future disclosures of the PHI.	
5. If the amendment request doesn't fit one of the reasons for denial, you must amend the PHI.	1. Amendment is accomplished by appending information or creating an electronic link. Never destroy the incorrect information. 2. You must inform the patient that you have accepted the amendment request. 3. You must give the corrected information to anyone that the patient wants, and to anyone that you know got the wrong information previously.	1. Decide how you will append or link information. 2. Prepare a master letter to patients informing them of the amendment. Use the model letter accompanying this chart, if desired. 3. Decide how you will determine who needs to get corrected information, and how you will send it. 4. Write a policy describing how you will handle amendments of PHI. (See Requirement 4, Action Steps.) 5. Keep this policy with your office's permanent records.

Doctor’s Name
Address
Phone

DESIGNATED RECORD SET

Policy Number: 16A Effective Date _____

In order to comply with HIPAA's Privacy Rule, this office designates the following records to be our "designated record set" for purposes of patients' right to access and amend their protected health information:

1. The patient's clinical chart, hard copy or electronic:

    42. reports of screening and diagnostic tests
    43. notes on examinations
    44. consultant reports
    45. examination results
    46. dental device prescriptions
    47. history and medication reports
    48. all other clinical information

2. The patient's billing records, hard copy or electronic:

    49. insurance claims
    50. remittance advice from insurance companies
    51. electronic fund deposit receipts
    52. bills to patients
    53. evidence of payment by patients
    54. collection records
    55. referrals to collection agencies or attorneys
    56. reports to consumer credit agencies for unpaid balances
    57. all other billing, claim, payment and collection records

3. Dental device order and receipt forms specific to a particular patient, hard copy or electronic:

    58. orders for dental prostheses
    59. orders for other dental devices
    60. acceptance of delivery of ordered dental devices
    61. patient pick up records
    62. repair requests and documentation of completion
    63. fitting information
    64. distribution of dental device accessories
    65. any other records relating to dental devices

4. [Specify other information in any form that you use to make decisions about a particular patient. This does not include any documents created in connection with litigation.]

Doctor's Name
Address
Phone

AMENDMENT OF PROTECTED HEALTH INFORMATION

Policy Number: 16B Effective Date _____

In order to comply with HIPAA's Privacy Rule, it is the policy of this office to permit patients to request us to amend their protected health information under the conditions stated in this policy. If the patient has a personal representative, the personal representative may exercise this right on behalf of the patient.

1. We require that all requests to amend protected health information be in writing. If a patient calls on the telephone to request an amendment, we will inform the patient of the requirement to submit this request in writing.

2. Our public information officer is responsible for handling patient requests to amend their protected health information.

3. We will respond to requests for amendment within 30 days after we receive the written request. We will use the form letter attached to this policy.

4. We can deny a requested amendment only for one or more of the following reasons:

   a. The information is accurate and complete as it is.

   b. We did not create the information.

   c. The information is not in a designated record set.

The patient would not be able to inspect or copy the information (see policy #15B).

5. If we deny a request, we will notify the patient. We will inform the patient of the right to either submit a statement of disagreement or to have the original amendment request accompany the information. We will use the form denial letter attached to this policy.

6. If we grant the requested amendment, we will notify the patient. We will use the form amendment letter attached to this policy. We will:

   a. Append or link the corrected information to the information that we are holding.

   b. Send the corrected information to anyone who we know has previously received the incorrect information.

   c. Send the correct information to anyone that the patient requests.

[office letterhead]

[patient address information]

Dear [name of patient]:

Thank you for your request dated [insert date] to amend information that we have about you. Unfortunately, we are unable to amend our information because:

[specify permitted reason]

If you are dissatisfied with our decision, you have two options.

1. You can write a statement disagreeing with our decision and explaining your point of view. We will keep this with your information, and include it in any authorized disclosure of your information from now on. We may decide to write a rebuttal to your statement of disagreement. If we do, it will be included with your information and sent along with any authorized disclosures of it from now on. If you want to do this, send your statement of disagreement to:

   [specify person in your office to accept these documents]

2. At your option, you could alternatively ask us to simply include your original amendment request with your information. If you do this, we will disclose your original request with any authorized disclosure of your information from now on. If you want to do this, call:

   [specify name of person in your office to handle these calls]

It is your right to complain to us, to complain to the New York State Department of Health, or to the U.S. Department of Health and Human Services -- Office for Civil Rights if you feel that your privacy rights have been violated. If you want to complain to us, send a written complaint (either hard copy or electronic) to:

[list the name of your Public Information Officer and contact information]

Thank you, and we look forward to working with you in the future.

[signature block]

[office letterhead]

[patient address information]

Dear [name of patient]:

Thank you for your request dated [insert date] to amend information that we have about you. We have made the change that you requested. The corrected information will be sent whenever we are authorized to send your information to anyone from now on.

Please let us know if there is any one who should get a copy of the corrected information right now. If there is, we will send the corrected information to them as quickly as possible.

We look forward to working with you in the future.

[signature block]

[office letterhead]

[patient address info]

Dear [name of patient]:

Thank you for your request to amend information that we have about you. Ordinarily, we would be able to respond to your request within 30 days, but due to unusual circumstances we need an additional 30 days in order to respond to you. Accordingly, please expect to hear from us by [insert farthest date].

We look forward to working with you in the future.

[signature block]

Completed _____ Date _____

YOU NEED TO GIVE PATIENTS AN ACCOUNTING OF DISCLOSURES OF THEIR PHI

_____

Signature of responsible person

Requirement	Comments	Action Steps
1. If a patient asks, you must give the patient a list ("accounting") of the disclosures you have made of their PHI during the six years before the request is made.	You do not have to include the following PHI in the accounting: 1. PHI disclosed to carry out treatment, payment, or health care operations. 2. PHI disclosed to patients. 3. PHI disclosed as an incident to a permitted use or disclosure. 4. PHI disclosed pursuant to a signed patient authorization. 5. PHI disclosed as part of a facility's directory or to persons involved in a patient's care or other notification purposes. 6. PHI disclosed as part of a limited data set. 7. PHI disclosed before April 14, 2003.	1. Decide how you will track disclosures of PHI in your office so that you have the information available to prepare an accounting. – This can be hard copy or electronic, as suits your practice. – It can be as simple as jotting disclosures down on a special sheet kept in the patient's clinical chart. *Suggestion:* Keep track of all disclosures that are not for treatment, payment, or health care operations. Sort through them to see what needs to be accounted for only if you are asked to prepare an accounting. 2. Write a policy describing how you will track information and prepare accountings. – See Requirement #3, Action Steps. 3. Keep all disclosure information that you have tracked for at least six years.
2. Identify the person in your office who will handle requests for, and preparation of accounts.	This can be your public information officer, if you wish. Or it can be anyone else who has time to handle this responsibility. A good candidate is your medical records clerk.	1. Designate the identified individual in a written policy. You may use model policy 17A, if desired. 2. Keep this policy with your office's permanent records.
3. Accountings must include the following: • The date of the disclosure. • Who received the PHI and if known, the address. • A brief description of the disclosed PHI, and • A brief statement of the purpose of the disclosure or a copy of a written request for a disclosure.		1. Decide how your office will prepare accountings. – This can be manual, or by computer. 2. Write a policy describing how you will handle tracking of information and accountings. – See Requirement #1, Action Steps. You may use model policy 17A, if desired.

YOU NEED TO GIVE PATIENTS AN ACCOUNTING OF DISCLOSURES OF THEIR PHI

Requirement	Comments	Action Steps
4. After receiving a request from a patient for an accounting, you must respond to it within 60 days.	You can have one 30 day extension, so long as you tell the patient before the initial 60 day period has expired**.**	See the model extension letter accompanying this chart.
5. You must keep copies of all accountings for at least six years.	You can keep these anywhere that is convenient for you.	
6. You must give a patient one free accounting per year. You can charge a reasonable fee for more frequent accountings.	If a patient requests more than one accounting in a 12-month period, you must inform them of the charge and give them a chance to change their mind.	

Doctor's Name
Address
Phone

ACCOUNTING FOR DISCLOSURES OF PROTECTED HEALTH INFORMATION

Policy Number: 17A Effective Date _____

In order to comply with HIPAA's Privacy Rule, it is the policy of this office to provide our patients, upon request, with an accounting of the disclosures that we have made of their protected health information during the six years preceding their request, subject to the terms and conditions stated in this policy.

1. We will provide an accounting of all of our disclosures of a patient's protected health information, except for the following:

a. Disclosures for treatment, payment, or health care operations (see related policy #8A).

b. Disclosures made with a signed patient authorization (see related policy #7A).

c. Disclosures that are incident to other permitted disclosures.

d. Disclosures to the patient personally

e. [Disclosures for a facility directory and] disclosures to family or friends involved in a patient's care (see related policies [#9A and] 9B).

f. Disclosures of a limited data set (see related policy #29A).

g. Disclosures made before April 14, 2003.

2. In order to be able to provide an accounting when a patient requests one, we will keep track of all disclosures that we make of our patient's protected health information, except for those disclosures listed in paragraph 1. Only [insert name or title] is authorized to make a disclosure of protected health information that is not listed in paragraph 1. [Insert name or title] will document all these disclosures in [specify where documentation will go]. We will keep this documentation for six years. This documentation will include:

a. The date of the disclosure

b. The name and address (if known) of he person or organization that got the protected health information

c. A description of the protected health information that was disclosed

d. A statement of the purpose or basis for the disclosure, or a copy of any request for the protected health information that prompted the disclosure.

3. We require that all requests for an accounting be in writing. If a request is made by telephone, we will advise the caller to submit it in writing to [insert name or title of person handling accountings].

4. We will respond to a request for an accounting within 60 days from our receipt of the written request. If we are unable to provide the accounting within this 60 day period, we may have an additional 30 days, provided that we notify the patient of this delay before the original 60 day period expires. This notice must include the reason for the delay and the date that we will have the accounting ready. We will use the letter accompanying this policy to inform patients of a needed delay. [Insert name or title] is responsible for advising patients of delays.

5. Our accounting will list all of the information described in paragraph 2 of this policy. We will use the template accompanying this policy to make our accounting. If we make repeated disclosures of protected health information about a patient to the same person or organization for the same purpose, our accounting will provide all of this information for the first such disclosure, and then indicate the frequency or periodicity of the other disclosures, and the date of the last such disclosure. [Insert name or title] is responsible for generating requested accountings and furnishing them to the patient.

6. We will provide patients with one free accounting, upon request, within any 12 month period. For additional accountings within any 12 month period, we will charge [specify charge] for the actual cost of preparing and mailing the accounting. We will require payment of this amount in advance, before we prepare and furnish the accounting.

[office letterhead]

[patient address info]

Dear [name of patient]:

Thank you for your request dated [specify date] for an accounting of disclosures that we have made of your protected health information. Ordinarily, we would provide this accounting to you within 60 days of receipt of your written request. Unfortunately, we are unable to provide your accounting within this time because [specify reason]. We will have your accounting ready by [specify date].

Thank you for your patience, and we look forward to working with you in the future.

[signature block]

Completed _____ Date _____

YOU MUST ALLOW PATIENTS TO ASK YOU TO RESTRICT HOW YOU USE PHI FOR TREATMENT, PAYMENT, OR HEALTH CARE OPERATIONS

_____

Signature of responsible person

Requirement	Comments	Action Steps
1. You must allow a patient to ask you not to use, or to restrict how you use, PHI about them for treatment, payment, or health care operations.	Examples include: – A patient asks you not to include information about their HIV status in your clinical chart. – A patient asks you not to use their clinical chart for quality assurance audits.	1. Identify who in your practice will handle patient restrictions. 2. Designate the identified person in writing. 3. Keep this designation with your office's permanent records.
2. You do not have to agree to a requested restriction.	No restriction can prevent you from using PHI in an emergency treatment situation.	1. Decide whether it is realistic in your practice to accommodate requests for restrictions on how you use PHI for treatment, payment, or health care operations. 2. Decide how you will handle requests for restrictions, if you agree to them. 3. Write a policy describing how you will handle patient requests for restrictions. You may use model policy 18A, if desired. 4. Keep this policy with your office's permanent records.
3. You cannot terminate your agreement, once you have made it, unless: • The patient agrees, or • You notify the patient in advance. – In this case, the termination only applies to PHI that you get after the date of the termination.		
4. If you agree to a restriction, you must honor it.		2. Decide how you will alert everyone affected by the restriction about its existence.

Doctor's Name
Address
Phone

RESTRICTIONS ON USE OF PROTECTED HEALTH INFORMATION

Policy Number: 18A Effective Date _____

In order to comply with HIPAA's Privacy Rule, it is the policy of this office to permit patients to request that we restrict the way that we use some protected health information for purposes of treatment, payment, or health care operations.

1. Our Public Information Officer ("PIO") will handle requests from patients for restrictions on the way we use protected health information for treatment, payment, or health care operations.

2. Generally, we will not agree to restrictions requested by patients. In unusual circumstances that the PIO thinks are meritorious, we may agree to a requested restriction.

3. If we agree to a requested restriction, the PIO will document its terms and put this documentation [specify location in your office where this information will be housed]. The PIO will communicate the terms of the restriction to all of our staff who need to know about it. If one or more of our business associates need to know about it as well, the PIO will inform them.

4. We will honor any restriction that we have agreed to. However, no restriction can prevent us from using any protected health information in an emergency treatment situation.

5. If we have agreed to a restriction but can no longer practically honor it, our PIO will do either of the following things:

a. Contact the patient to work out a mutually agreeable termination of the restriction. Our PIO will document this agreement , and keep it in [specify location where these documents will be housed].

b. Contact the patient and advise that we are no longer able to honor the restriction that we previously agreed to. This notice will only apply to protected health information that we obtain or generate after the notice is given.

Completed _____ Date _____

YOU MUST ALLOW PATIENTS TO SPECIFY CONFIDENTIAL METHODS OF RECEIVING COMMUNICATIONS FROM YOU

_____

Signature of responsible person

Requirement	Comments	Action Steps
1. You must have a process to allow patients to specify particular ways that they want you to communicate with them in order to protect their privacy. Examples: • Special phone number. • Special address. • Only by email.	1. You must accommodate these requests whenever reasonable. 2. You can charge the patient the reasonable cost of the requested communication method, if any. 3. You cannot make the patient tell you why they want a special communication method.	1. Identify a person in your office to handle patient requests for confidential communication methods. 2. Designate the identified person in a written policy. 3. Keep this policy with your office permanent records. 4. Determine what kinds of confidential communication methods your practice can reasonably accommodate, and how you will accomplish the accommodations. 5. Write a policy describing how you will handle requests for confidential communication methods. 6. Use the model policy 19A accompanying this chart, if desired. Keep this policy with your office permanent records.

Doctor's Name
Address
Phone

CONFIDENTIAL COMMUNICATION METHODS WITH PATIENTS

Policy Number: 19A Effective Date _____

In order to comply with HIPAA's Privacy Rule, it is the policy of this office to accommodate requests from patients to send protected health information to them in a confidential way, subject to the conditions in this policy.

1. If a patient requests that we use a particular method to communicate with them in order to preserve the confidentiality of their information, we will accommodate that if we reasonably can. We can accommodate the following kinds of confidential communication methods:

[specify methods that your office can handle.]

2. We require that such requests be in writing. If a request comes in by telephone, we will advise the patient how to send the request in writing.

3. We will not ask or require a patient to explain why they want the particular communication method.

4. We will charge the patient the reasonable cost of complying with their request, if any.

5. Our Public Information Officer ("PIO") is responsible for receiving and acting upon patient requests for confidential communication methods.

WHAT IS A BUSINESS ASSOCIATE?

Completed _____ Date _____

_____

Signature of responsible person

THIS DECISION TREE AND ACCOMPANYING WORKSHEET WILL HELP YOU IDENTIFY YOUR BUSINESS ASSOCIATES, AND DETERMINE WHICH BUSINESS ASSOCIATES NEED TO SIGN HIPAA CONTRACTS WITH YOU IMMEDIATELY AND WHICH CAN WAIT

Assessment Question	Comments	Action Steps
1. Who are your business associates?	Dental laboratories are not considered business associates. A guidance document, issued by DHHS Office for Civil Rights (OCR) in December 2002, notes "a physician is not required to have a business associate contract with a laboratory as a condition of disclosing protected health information for the treatment of an individual."	1. Identify all the outside companies with which you do business. Use the accompanying worksheet, if desired. 2. Flag the names of those companies that perform a health care service on your behalf. In other words, those companies to which you have outsourced a health care function. Examples include billing, service delivery, quality assurance, or staff training. 3. Flag the names of those companies that provide the following services to you: – Legal – Accounting – Consulting – Management 4. Of the companies that you have flagged, flag again those companies that need to generate, maintain, use, or disclose PHI in order to perform their job. For example, a billing agent needs to use PHI in order to prepare and send bills or claims, and to post payments. A janitorial service does not need to see or use PHI in order to clean your office even though PHI may be in the rooms being cleaned. 5. Companies with two flags are your business associates. Indicate them on the accompanying worksheet, if desired.

WHAT IS A BUSINESS ASSOCIATE?

Assessment Question	Comments	Action Steps
2. Which business associates need attention right now, and which can wait?	1. Business associates that need attention right now fall into any of the following groups: • You do not currently have a written services contract with them. • You have a written services contract with them, but you entered into it after October 15, 2002. • You have a written services contract, but it will expire or need to be renewed before April 14, 2003. Note these business associates on the worksheet accompanying this chart, if desired. 2. Business associates that do not need immediate action are those that: • You have a written contract with, and • The written contract existed before October 15, 2002, and • The contract automatically renews, or • The contract will not expire or be renewed before April 14, 2003. 3. You have to act on this latter group on the earlier of: • The date that you will renew the contract, or • April 14, 2004.	See chart 21 for information on what action you need to take regarding your business associates.

Completed _____ Date _____

BUSINESS ASSOCIATE IDENTIFICATION (WORKSHEET)

_____

Signature of responsible person

Name of Outside Contractor	Business Associate Yes/ No	Written Services Contract in Place as of 10/15/02?	Expiration Date	Immediate Action Yes/No	Comments

BUSINESS ASSOCIATE IDENTIFICATION (WORKSHEET)

Name of Outside Contractor	Business Associate Yes/ No	Written Services Contract in Place as of 10/15/02?	Expiration Date	Immediate Action Yes/No	Comments

Completed _____ Date _____

YOU MUST HAVE A CONTRACT WITH YOUR BUSINESS ASSOCIATES

_____
Signature of responsible person

YOU MUST HAVE A "BUSINESS ASSOCIATE CONTRACT" WITH YOUR BUSINESS ASSOCIATES. THE MINIMUM TERMS OF THE CONTRACT ARE SPECIFIED BY LAW. YOU MAY ADD TERMS THAT ARE NOT INCONSISTENT.

Action Steps	Comments
1. Obtain a master business associate contract from which you can work. You can: • **Use the model DHHS contract found at http://www.hhs.gov/ocr/hipaa/ You can use it as it is, or you can adapt it to your needs. A copy printed from the *Federal Register* accompanies this chart.** • **Use the model business associate contract, 21A, if desired.**	The minimum terms of a business associate contract are found at 45 CFR 164.504(e)(2) and are: • The contract must define what uses or disclosures the business associate can make of PHI. The contract cannot authorize any use or disclosure that would violate the HIPAA Privacy Rule. The contract may permit the business associate to use and disclose PHI for the proper management and administration of the business associate. The contract may permit the business associate to provide data aggregation services relating to your health care operations. • The contract must prevent the business associate from making other uses or disclosures. • The contract must require the business associate to use appropriate safeguards for PHI. • The contract must require the business associate to report to you any use or disclosure of PHI that violates the contract, if the business associate becomes aware of the violation. • The contract must require the business associate to ensure that any agents or subcontractors to which it provides PHI agrees to the same restrictions and conditions that apply to the business associate. • The contract must require the business associate to make PHI available to the patient, upon request. (See chart 15.) • The contract must require the business associate to amend PHI, upon a proper request. (See chart 16.) • The contract must require the business associate to give you all information that you need in order to provide an accounting of disclosures to the patient. (See chart 17.) • The contract must require the business associate to make its internal practices, books, and records relating to the use and disclosure of PHI available to DHHS for purposes of determining your compliance with HIPAA's Privacy Rule. • The contract must require the business associate to return or destroy all PHI at termination of the contract, unless this is infeasible. If return or destruction is infeasible, the contract must require the business associate to continue to protect the confidentiality of the PHI that it has to keep. • The contract must authorize you to terminate the contract if you determine that the business associate has violated a material term of the contract.

YOU MUST HAVE A CONTRACT WITH YOUR BUSINESS ASSOCIATES

Action Steps	Comments
2. Pick the best negotiator in your practice to work on getting these contracts signed, or use your attorney.	Negotiate a business associate contract with each of your business associates, except: • A business associate who uses PHI only for treatment purposes. • A business associate that **only** uses, generates, maintains or discloses PHI for treatment purposes.
3. Consider whether you want the business associate terms to be a separate contract, or whether you want to fold it into the existing services agreement.	You may want a separate agreement if you prefer not to re-open the services agreement as a whole. For example, you may not want to give the business associate the opportunity to negotiate changes to pricing structures.
4. Use the business associate worksheet (chart 20) to track which of your business associates have a signed business associate contract, if desired.	
5. Keep copies of your signed business associate contracts with your permanent office records.	

Insert the PDF document – 4 pages from the Federal Register containing the DHHS business associate agreement

BUSINESS ASSOCIATE CONTRACT

This Business Associate Contract ("BAC")is made and entered into between _____ D.D.S. or D.M.D. [PC or PLLC] ("DOCTOR"), having its principal place of business at [specify address], and _____ ("Business Associate" or "BA"), having its principal place of business at [specify address].

NOTICE: [*Bracketed and italicized language is not mandated by HIPAA. It is, however, recommended language if it is possible to negotiate it with a particular Business Associate. Not all Business Associates will be able to agree to all of this language, depending upon their individualized circumstances.*]

RECITALS:

DOCTOR is a dentist , and is a "covered entity" within the meaning of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and the standards for the Privacy of Individually Identifiable Health Information ("Privacy Rule") promulgated by the Department of Health and Human Services ("DHHS") pursuant thereto.

BA provides [*insert type of services*] to DOCTOR, which services necessarily involve the access to, generation of, use of, or disclosure of health information that identifies individual patients (protected health information – "PHI"). Accordingly, BA is a business associate of DOCTOR pursuant to HIPAA's Privacy Rule.

DOCTOR is obligated by the Privacy Rule to obtain "satisfactory assurances" from its business associates as a precondition to permitting a business associate to access, generate, use, or disclose PHI on its behalf or in the course of performing services for it.

For the foregoing reasons, DOCTOR and BA desire to enter into an agreement that complies with all the requirements of the Privacy Rule regarding business associate "satisfactory assurances."

NOW THEREFORE, in consideration of the foregoing and of the mutual promises contained herein, DOCTOR and BA agree as follows:

I. DEFINITION OF TERMS

Any terms used in this BAC that are defined in the Privacy Rule shall have the same meaning when used in this BAC as they have in the Privacy Rule.

II. OBLIGATIONS OF BUSINESS ASSOCIATE

(a) BA is authorized to access, generate, use or disclose PHI as necessary and appropriate to perform the following services on behalf of or for DOCTOR:

[insert description of services performed by BA]

(b) Except as otherwise limited in this BAC, BA may also use PHI for the proper management and administration of BA or to carry out the legal responsibilities of BA.

(c) BA agrees to not use or further disclose PHI other than as permitted or required by this BAC or as required by law.

(d) BA agrees to use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by this BAC. [***"Appropriate safeguards" include, but are not limited to, physical, administrative and technical safeguards such as locking cabinets or rooms where PHI is housed, using computer passwords or other security measures to prevent unauthorized access to PHI in electronic format; implementing policies and procedures describing authorized access and use for BA's work*** *force; and human resources policies and procedures to enforce these rules.*]

(e) BA agrees to cooperate with DOCTOR and perform such activities as DOCTOR may from time to time direct, in order to mitigate, to the extent practicable, any harmful effect that is either independently known to BA or brought to BA's attention by DOCTOR, as a result of a wrongful use or disclosure of PHI by BA.

(f) BA agrees to report to DOCTOR any use or disclosure of PHI in violation of this BAC.

(g) BA agrees to ensure that any agent, including a subcontractor, to whom it provides PHI received from, or created or received by BA on behalf of DOCTOR, agrees to the same restrictions and conditions that apply through this BAC to BA.

(h) At the request of DOCTOR, and in the time and manner designated by DOCTOR, BA agrees to provide access to PHI in a Designated Record Set to DOCTOR or to an Individual, in order to meet the inspection and copying requirements of the Privacy Rule.

(i) At the direction of DOCTOR and in the time and manner directed by DOCTOR, BA agrees to make any amendment(s) to PHI in a Designated Record Set in order to comply with an individual's amendment rights under the Privacy Rule.

(j) At the direction of DOCTOR or the Secretary of DHHS, and in the time and manner directed by either of them, BA agrees to make internal practices, books, and records relating to the use and disclosure of PHI available to DOCTOR or the Secretary of DHHS, for purposes of the Secretary of DHHS determining DOCTOR'S compliance with the Privacy Rule.

(k) BA agrees to document all disclosures of PHI and information related to such disclosures as would be required for DOCTOR to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with the Privacy Rule. At DOCTOR'S request, and in the time and manner designated by DOCTOR, BA agrees to provide to DOCTOR the information so collected to permit DOCTOR to respond to a request by an Individual for an accounting of disclosures of PHI.

(l) BA agrees to honor any restriction on the use or disclosure of PHI that DOCTOR agrees to, provided that DOCTOR notifies BA of such restriction.

[(m) BA shall establish specific procedures and mechanisms to implement BA's obligations pursuant to this BAC. Such procedures and mechanisms shall be reduced to writing, and shall be attached to and incorporated into this BAC.]

[(n) BA shall require each member of its work force that has contact with PHI in the course of providing services to DOCTOR to sign a statement indicating that the work force member has read this BAC, understands its terms, and will abide by them, including without limitation, the obligation not to use or disclose PHI except as necessary and appropriate to carry out the services being performed by BA for or on behalf of DOCTOR. BA will make such signed statements available to DOCTOR upon request.]

III. OBLIGATIONS OF DOCTOR

(a) DOCTOR shall provide BA with the notice of privacy practices that DOCTOR produces in accordance with the Privacy Rule, as well as any changes to such notice.

(b) DOCTOR shall notify BA of any restriction to the use or disclosure of PHI that DOCTOR has agreed to in accordance with the Privacy Rule.

(c) DOCTOR shall not request BA to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by DOCTOR, except for uses of PHI for the proper administration and management of BA or as required by law.

IV. TERM AND TERMINATION

(a) Term. The term of this BAC shall commence on April 14, 2003, and shall continue coterminously with the term of all services being performed by BA for or on behalf of DOCTOR, unless sooner terminated in accordance with paragraph IV(b) hereof.

(b) Termination for Cause. Upon DOCTOR'S knowledge of a material breach by BA, DOCTOR shall, at its sole option, do either of the following:

(1) Provide a 15 day opportunity for BA to cure the breach to DOCTOR'S satisfaction, or terminate this BAC and the services relationship with BA if BA does not cure the breach to DOCTOR'S satisfaction, or

(2) Immediately terminate this BAC and the services relationship with BA if DOCTOR determines, in its sole discretion, that cure is not possible.

[(c) In addition to the termination for cause provisions stated in paragraph IV(b), this BAC may also be terminated in any of the following circumstances:

(1) The services relationship between BA and DOCTOR is terminated for any reason;

(2) The provisions of the Privacy Rule are amended, modified or changed such that a BAC such as this is no longer mandated;

(3) By the mutual agreement of DOCTOR and BA, provided that either a new BAC must be substituted or the services relationship between BA and DOCTOR must terminate.]

(d) Effect of Termination.

(1) Except as provided in paragraph (2) of this section, upon termination of this BAC for any reason, BA shall return or destroy all PHI received from DOCTOR, or created or received by BA on behalf of DOCTOR, as directed by DOCTOR. DOCTOR has the sole authority to determine whether PHI shall be returned or destroyed, and shall have the sole authority to establish the terms and conditions of such return or destruction. This provision shall apply to PHI that is in the possession of subcontractors or agents of BA. BA shall retain no copies of PHI.

(2) In the event that BA believes that returning or destroying PHI is infeasible, BA shall provide to DOCTOR an explanation of the conditions that make return or destruction

infeasible. Upon DOCTOR'S concurrence that return or destruction of PHI is infeasible, BA shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as BA maintains such PHI.

[(3) If this BAC is terminated and not immediately replaced with a substitute business associate agreement, and if the privacy rule at that time continues to mandate the execution of a business associate agreement between covered entities and their business associates, then the services relationship between BA and DOCTOR shall immediately terminate in synchronized timing with this BAC.]

V. GENERAL PROVISIONS

[(a) BA shall indemnify DOCTOR for any losses, costs or expenses that DOCTOR sustains, including fines under HIPAA, as a result of any breach by BA of any of its obligations under this BAC.]

[(b) BA shall maintain during the term of this BAC a policy of errors and omissions or other comparable insurance with an insurer acceptable to DOCTOR in the amount of _____, covering BA's obligations under this BAC. The policy of insurance shall name DOCTOR as an additional insured. BA shall furnish to DOCTOR such evidence of this insurance as DOCTOR deems satisfactory upon the commencement of this BAC. BA shall notify DOCTOR of any threatened or actual cancellation or termination of the insurance coverage, at least ten days prior to any such action.]

[(c) BA agrees that the terms and conditions of this BAC shall be construed as a general confidentiality agreement that is binding upon BA even if it is determined that BA is not a business associate as that term is used in the Privacy Rule.]

[(d) DOCTOR and BA shall not be deemed to be partners, joint venturers, agents or employees of each other solely by virtue of the terms and conditions of this BAC.]

[(e) This BAC shall not be modified or amended except by a written document that is signed by both parties. DOCTOR and BA agree to modify or amend this BAC if the Privacy Rule changes in a manner that affects the terms and conditions of this BAC, or the obligations of covered entities and/or business associates.]

[(f) Any communications between DOCTOR and BA regarding this BAC shall be in writing, whether or not oral communications have also occurred. Such communications shall be sent to the following individuals at the following addresses:

To DOCTOR *To BA*

Written communications may be sent by certified or registered U.S. Mail, receipted courier service, receipted hand delivery, receipted fax, or by receipted email.]

[(g) No waiver of any provision of this Agreement, including this paragraph, shall be effective unless the waiver is in writing and signed by the party making the waiver.]

[(h) This BAC is entered into solely for the benefit of the parties, and is not entered into for the benefit of any third party, including without limitation, any patients of DOCTOR or their legal representatives.]

[(i) This BAC is not assignable or delegatable without the express advance written consent of the party not seeking to assign or delegate.]

[(j) This BAC shall be governed by and construed in accordance with the laws of the United States of America and the laws of the state of [insert DOCTOR'S home state].]

[(k) If any provision of this BAC is determined by a court of competent jurisdiction to be invalid or unenforceable, this BAC shall be construed as though such invalid or unenforceable provision were omitted, provided that the remainder of this BAC continues to satisfy all of the Privacy Rule's requirements for a business associate agreement. If it does not, then the parties shall immediately renegotiate this BAC so that it does comply with the requirements of the Privacy Rule, or terminate this BAC and the service relationship between the BA and DOCTOR.]

[(l) This BAC contains the entire agreement between the parties pertaining to this subject matter, and supercedes all prior understandings, whether written or oral, regarding the same subject matter.]

[(m) The provisions of this BAC dealing with indemnification, insurance, and the construction of this BAC as a general confidentiality agreement shall survive the termination of this BAC for any reason.]

In witness whereof, the parties have executed this Business Associate Contract on the ____ day of _____, 200__.

Witness **_____ (DOCTOR)**

_____ By _____

Its _____

Dated _____

Witness **_____ (BA)**

_____ By _____

Its _____

Dated _____

Completed _____ Date _____

DO YOU HAVE CONTINUING OBLIGATIONS TOWARDS YOUR BUSINESS ASSOCIATES?

_____

Signature of responsible person

Question	Answer
1. Do I have to monitor whether my business associates are complying with their contract.	No.
2. What happens if I learn that one of my business associates has violated the contract and wrongfully disclosed PHI?	You have to do the following things: • You and the business associate have to take reasonable steps to mitigate known harm caused by the wrongful disclosure. (See chart 26.) • You must demand that the business associate take appropriate steps to cure their breach of the contract, and terminate the contract if it is not properly cured. • If you think that the business associate cannot cure the breach, you can skip the cure step and terminate the contract right away. • When you terminate the business associate contract, you must also terminate the services contract with the business associate. You will have to find a substitute service vendor. If that is impossible, you can report the breach to DHHS instead of terminating the service contract. It is unclear what DHHS will do with that information.
3. If some of my business associates qualify for the extra time to sign their business associate contracts, do I have to do anything with them in the meantime? (See chart 20.)	Yes. Even if you don't have to sign a full business associate contract with some of your business associates until the earlier of the contract renewal date or April 14, 2004, you must still have a way to be sure that the business associate will do the following things: • Make PHI available to patients upon request. (See chart 15.) • Amend PHI upon request. (See chart 16.) • Give you information so that you can prepare an accounting of disclosures for the patient, upon request. (See chart 17.) You may need to have an informal understanding or agreement with these business associates on these points.
4. Do I have to train my business associates in HIPAA compliance?	No. Business associates are not part of your work force, and you are only obligated to train your work force. (See chart 30.)

YOU MUST SAFEGUARD PHI

Completed _____ Date _____

_____

Signature of responsible person

Assessment Question	Comments	Action Steps
1. Examine your operations to identify areas where unauthorized people may come into contact with PHI. Use the worksheet accompanying this chart, if desired. Common examples of problem areas include: • Waiting rooms – can waiting patients and families overhear discussions with patients, or information about patients? • Unattended clinical charts – often open at a central desk that patients and others pass on their way to exam rooms. • Unattended computer screens visible to patients and others passing through the office. • Dictation equipment in open hallways where you dictate chart notes. • Disposal of PHI in the trash. • Use of open faced postcards or leaving voice messages over answering machines to provide information to patients.	1. HIPAA requires that you take reasonable steps to safeguard PHI from intentional and unintentional disclosure to anyone who does not have proper authority.	
2. Identify any safeguards that you could use to protect PHI from unauthorized access or disclosure in your individual office setting. Use the worksheet accompanying this chart, if desired.	1. Safeguards come in many forms. The three general categories are: • Administrative (policies and procedures). • Physical (physical plant). • Technological (relating to electronics). 2. Examples of safeguards include: • Locks on records' storage rooms or cabinets. • Phones in confidential locations.	1. Have a staff member or an outsider role play that they are a patient in your office. Have them list their observations about where improvements could be made to safeguard PHI. 5. Brainstorm from this list for ways to better protect PHI from inadvertent disclosures. 6. Translate the brainstorming into specific process changes or necessary equipment to be purchased. 7. Obtain proper approval for expenditures

YOU MUST SAFEGUARD PHI

Assessment Question	Comments	Action Steps
	• Closing doors. • Computer passwords. • Computer screen savers or screen shields. • Limited field access for electronic data. • Turning charts to face the wall in boxes outside patients' exam rooms. • Prohibiting calls to the pharmacy or other providers from a receptionist phone in an open waiting area. • Policies prohibiting treatment staff from discussing clinical issues with patients in areas where they can be overheard. • Shredding PHI to be disposed of. 3. This aspect of HIPAA requires unique, individualized solutions based upon your office layout, opportunities to easily make physical plant changes, budget for purchase of physical and technological gadgets; and workable policies and procedures. 4. You are not required to go to extremes to guarantee that no PHI will ever be inadvertently disclosed. "Incidental" disclosures – e.g. unavoidable disclosures secondary to a permitted use or disclosure – are permitted under HIPAA, so long as you have taken reasonable steps to safeguard the PHI and you observe the minimum necessary rule. (See chart 24.)	within your organizational structure. 8. Implement the changes.

Completed _____ Date _____

YOU MUST SAFEGUARD PHI (WORKSHEET)

_____

Signature of responsible person

Observations About How PHI is being Inadvertently Disclosed in Your Practice	Suggestions for Solutions	Final Decision About Solution	Estimated Cost

Completed _____ Date _____

YOU MUST INTERNALLY USE OR EXTERNALLY DISCLOSE ONLY THE MINIMUM NECESSARY AMOUNT OF PHI

_____

Signature of responsible person

Assessment Question	Comments	Action Steps
1. Look at the list of activities that you identified on the chart 6 worksheet as involving the use or disclosure of PHI. For each such activity, determine the minimum amount of PHI that is necessary in order to properly perform the activity. Use the worksheet accompanying this chart, if desired.	This analysis does not apply to PHI that is used or disclosed for treatment purposes.	
2. For each activity listed on chart 6, determine how much and what kind of PHI is actually available now to the individuals performing the activity. Use the worksheet accompanying this chart, if desired. Compare this to your answer in question 1.		
3. Is more than the minimum necessary PHI available to the individuals performing the activities? For example, is a biller who does not also do coding able to look at comprehensive progress notes? Or is an appointment clerk able to review the clinical chart? Are you regularly giving requesters more than the minimum amount of PHI necessary to satisfy their request (for example, disclosing the whole clinical chart when only a portion is needed)? **If so, this violates the minimum necessary rule and must be corrected.**	1. Access to the entire clinical chart is restricted on a "need to know" basis and must be specifically justified. 2. Treating professionals may have access to any PHI that they request for purposes of treatment. 3. When an outside person requests PHI, you can only disclose the minimum necessary amount, unless any of the following exceptions apply: • The patient has authorized the disclosure. (See chart 13.) • You are disclosing a "limited data set." (See chart 29.)	1. Determine what measures you will use to prevent staff from accessing more PHI than is the minimum necessary to perform their job tasks. For example, you might: • Restrict access to certain data fields in electronic records. • Reorganize paper charts so that information needed for particular tasks is segregated, if your clinical needs are not compromised. 2. For disclosures of PHI that are routine, determine the minimum necessary amount of PHI needed to respond. For example, if you regularly work with a school to examine students' dentals, determine what the minimum amount of information is that the school needs about the student. 3. Decide how you will determine the minimum amount of PHI necessary to respond to requests that are not routine. This would include designating a person in your office to be

YOU MUST INTERNALLY USE OR EXTERNALLY DISCLOSE ONLY THE MINIMUM NECESSARY AMOUNT OF PHI

Assessment Question	Comments	Action Steps
	• The disclosure is "incidental" to a permitted disclosure. (See chart 23.)	responsible for making these decisions, and some criteria for how they will make them. 4. Write a policy describing the minimum amount of PHI necessary for activities in your practice involving use or disclosure of PHI. The written policies should: • Be specific to each individual or job title that has access to PHI (for example, receptionist, billers, records clerk.) be specific to routine requests for disclosure of PHI • Establish a process to address minimum necessary issues for unique requests for PHI. • Keep this policy with your office's permanent records. • Design appropriate HR sanctions for breach of this minimum necessary policy. Use model policy 24A regarding the minimum necessary rule, if desired. If you use it, it must be tailored to your individual practice.

Completed _____ Date _____

YOU MUST INTERNALLY USE OR EXTERNALLY DISCLOSE ONLY THE MINIMUM NECESSARY AMOUNT OF PHI (WORKSHEET)

_____

Signature of responsible person

Activity Involving PHI	Minimum Necessary PHI	Current Access to/Disclosure of PHI

Doctor's Name
Address
Phone

MINIMUM NECESSARY USES AND DISCLOSURES OF PHI

Policy Number: 24A Effective Date _____

In order to comply with HIPAA's Privacy Rule, it is the policy of this office to only use or disclose the minimum amount of protected health information necessary to accomplish the purpose for the use or disclosure, under the conditions and exceptions described in this policy.

1. People in the following job categories will only have access to the kind or amount of protected health information indicated:

a. All Dentists – any and all protected health information, including the entire clinical chart, for treatment purposes.

b. Coders/billers – [specify the protected health information needed to perform their job duties]

c. Receptionist – [specify the protected health information needed to perform their job duties]

d. Dental Hygienists and Dental Assistants -- [specify the protected health information needed to perform their job duties]

e. [Other] --[specify the protected health information needed to perform their job duties]

2. We will keep all clinical charts and billing records secure when they are not in use. [Specify how they will be secured.] Only authorized staff will have access to this secure storage. We require that all computers be turned off when the user is away from the workstation. All staff are prohibited from browsing at someone else's workstation or using their computer password. Staff are prohibited from talking about our patients in public areas.

3. All staff will sign a "confidentiality agreement" indicating their commitment to access only the minimum amount of protected health information necessary for them to do their job, and to abide by the restrictions listed in paragraph 2. Violation of this agreement is grounds for employment discipline according to our personnel policies.

4. Whenever we get a request from a third party for protected health information about one of our patients, or whenever we intend to make a unilateral disclosure of protected health information about one of our patients, we will disclose only the minimum necessary amount of protected health information necessary to satisfy the purpose of that disclosure. This does not apply in the following cases:

a. The patient has authorized the disclosure.

b. The disclosure is for treatment purposes (for example, disclosures to a consultant or follow-up health care provider).

5. We will disclose only the indicated protected health information in response to the following routine kinds of disclosures that we make:

a. [Specify the type of routine disclosure, and the protected health information that will be disclosed.]

6. We will rely upon the representations of the following third parties that they have requested only the minimum amount of protected health information necessary for their purposes:

a. Another health care provider or health plan.

b. A public official, like a law enforcement officer.

c. Professionals providing services to us (such as attorneys or accountants).

d. Researchers supplying documentation of IRB waivers (see chart 12).

7. [Insert name or title] is responsible for determining what is the minimum amount of protected health information necessary for us to disclose in situations that are not routine. [Insert name or title] will consider the reason for the disclosure, whether it falls into any of the circumstances described in paragraph 4 of this policy, and the protected health information that we have, in making this determination.

8. Whenever we request protected health information about one of our patients from someone else, we will ask for only the minimum necessary amount of protected health information necessary for us to accomplish the purpose that prompted us to ask for the information.

Completed _____ Date _____

YOU MUST VERIFY THE CREDENTIALS OF THOSE WHO SEEK PHI

_____

Signature of responsible person

Assessment Question	Comments	Action Steps
1. Identify the steps that you currently take to verify the identity and authority of someone who signs an authorization to release PHI on behalf of a patient, or who claims entitlement to PHI without an authorization. Use the worksheet accompanying this chart, if desired.	1. You must check the identity and authority of someone signing an authorization on behalf of a patient or seeking PHI without an authorization, if you don't know this information already. 2. This should include obtaining copies of applicable documents, such as guardianship papers, power of attorney for health care, or official badge. 3. You can rely on documents that appear valid on their face. 4. If questions or problems arise, you must resolve them before you can accept the authorization or request and disclose PHI. **Examples:** • A person claiming to be the patient's legal guardian wants to sign an authorization, or access PHI personally. You must: – Review the guardianship papers from the court and make sure that they have not expired or that they don't limit the guardian's powers in a way that affects the request to disclose PHI, and – Check an ID (like a driver's license) to be sure that the person is the one appointed by the court, unless you know the person's identity already. • Someone claiming to be from your state's Medicaid fraud unit arrives at your office and asks to see patient charts within a particular date range. You must: – Ask to see the agent's badge or ID showing his connection to the fraud unit, and – Ask the agent to state the law that he is relying on as authority for the request.	1. Write a policy describing your verification procedures. The policy should address: • The situations in which you need to verify identity or authority of someone requesting PHI. • What information or documents you will ask for. • How you will try to resolve problems, if any. • A prohibition on releasing PHI if either the requestor's identity or authority cannot be verified. Use model policy #25A, if desired.

What Kinds of Requests do you get for PHI from Someone other than the Patient?	What Information do you get to Verify the Identity and Authority of the Requestor?	What Additional Steps Need to be taken to Verify Identity or Authority of Requestor?

Doctor's Name
Address
Phone

VERIFICATION BEFORE DISCLOSING PROTECTED HEALTH INFORMATION

Policy Number: 25A Effective Date _____

In order to comply with HIPAA's Privacy Rule, it is the policy of this office to verify the authority and identity of people or organizations that request us to disclose protected health information about our patients, subject to the conditions of this policy statement.

1. If a patient has a personal representative who seeks to sign an authorization to disclose the patient's protected health information to a third party, or to exercise any of the rights that patients have regarding their protected health information, we will take the following steps before we accept their signature or allow them to exercise those rights:

a. Ask for copies of any documents that are relevant to their status as personal representative. For example, we will ask for a copy of the court papers appointing a legal guardian, or a power of attorney designating someone to make health related decisions for an incapacitated adult.

b. We will ask for a picture identification of the person serving as personal representative.

2. We will review all documents that we receive and make sure that they in fact authorize the personal representative to control the patient's protected health information, and that there are no limits or expiration dates that affect this authority. [Specify name or title] is responsible for reviewing documents. If there are questions about the documents, [specify name or title] will work with our Privacy Officer to resolve them. We will not disclose any protected health information until all questions are answered and we have proper evidence of the authority of the person acting as personal representative.

3. If we receive a request from a third party to see or have a copy of protected health information that we have about our patients without a signed patient authorization, we will take the following steps before we allow such access:

a. Ask the requestor for evidence that they are affiliated with an organization or government agency that is authorized to have access to protected health information without an authorization (see related policy #8A). Evidence can include an official badge or identification card, an assignment on official letterhead, or similar items.

b. Ask the requestor for a picture identification.

c. Ask the requestor to specify the legal authority that the requestor believes allows access to protected health information.

For example, if we are asked by a representative of a drug or medical device manufacturer to supply protected health information relating to our use of a particular drug or device, we will make sure that the representative is truly affiliated with the drug or device manufacturer; that the drug or medical devise manufacturer is under the jurisdiction of the U.S. Food and Drug Administration; and that the drug or device manufacturer is seeking the information because of a quality or safety concern about a product that they manufacture as provided in 45 CFR 164.512.

4. We will review all evidence supplied by the requestor to make sure that the requestor has proper authority to access protected health information, and that there are no limits or expiration dates that affect this authority. [Specify name or title] is responsible for this review. If there are questions, [specify name or title] will work with our Privacy Officer to resolve them. We will not disclose any protected health information about our patients until all questions have been resolved and we are sure that the requestor has proper authority to access the protected health information.

Completed _____ Date

YOU MUST MITIGATE THE HARM DONE BY A WRONGFUL USE OR DISCLOSURE OF PHI

Signature of responsible person

Question	Answer	Comments	Action Steps
1. Do I have to seek out evidence of harm if I have wrongfully used or disclosed PHI, so that I can mitigate it?	No.	1. The duty only applies if you "know" of the harm. You do not have to actively monitor for evidence of harm. 2. You can "know" of harm if: • Someone tells you about it. • You learn of it when reviewing your records. • You learn of it by reviewing public sources. • You are made aware of it in any other way. 3. You cannot "deliberately ignore" clear indications of harm in order to avoid your duty to mitigate harm.	Identify someone in your office who will be responsible for mitigating harm. 1. Write a policy describing your mitigation obligation and how it will be applied in your office. 2. A model policy, 26A accompanies this chart. Use the model policy if desired.
2. Does it matter if it's a workforce member or business associate who wrongfully used or disclosed the PHI?	No.	1. The duty applies if: • Your work force makes the wrongful use or disclosure; or • Your business associate makes the wrongful use or disclosure. 2. Your business associate contracts obligate your business associates to tell you about any wrongful uses or disclosures of PHI that they know about.	
3. Does it matter if the wrongful use or disclosure was just a mistake?	No.	1. The duty applies if: • The wrongful use or disclosure was an innocent mistake. • The wrongful use or disclosure was intentional. • No one meant any harm	
4. What do I have to do to mitigate a harmful effect of a wrongful disclosure?	It depends on the individual circumstances	1. You only have to mitigate harm if it is "practical" for you to do so. 2. You have full discretion to evaluate each situation, and to take mitigation steps appropriate to it. • Sometimes mitigation can be as simple as an apology or correction. • Sometimes you might have to try to get back PHI that you have disclosed. • Sometimes you may have to ask someone who got PHI when they shouldn't have, to sign an agreement not to use or disclose it. It's up to you in each case.	

Doctor's Name
Address
Phone

MITIGATION OF KNOWN HARM FROM AN IMPROPER DISCLOSURE OF PROTECTED HEALTH INFORMATION

Policy Number: 26A Effective Date _____

In order to comply with HIPAA's Privacy Rule, it is the policy of this office to mitigate known harm from an improper disclosure of protected health information, when it is practicable to do so.

1. Whenever we learn of harm caused by an improper disclosure of our protected health information, we will take reasonable steps to mitigate the harm. We will take these steps whether the improper disclosure was made by us or by one of our business associates.

2. Our Privacy Officer and Public Information Officer will determine what specific steps are appropriate to mitigate particular harm. It is our policy to tailor mitigation efforts to individual harm. Examples of some mitigation steps include:

   a. Getting back protected health information that was improperly disclosed.

   b. Preventing further disclosure through agreements with the recipient.

3. We do not consider money reparations to be appropriate mitigation.

4. If a business associate has made the improper disclosure, we will require the business associate to cure the problem to our satisfaction, or terminate the relationship with the business associate.

Completed _____ Date _____

YOU MUST HAVE A COMPLAINT POLICY AND PROCEDURE

_____

Signature of responsible person

Assessment Question	Yes/No	Comments	Action Steps
1. Does one specific person or department in your office currently take and investigate patient complaints about your services?	If yes, that person or department should be appointed as the public information officer, if they also meet the other qualifications for that position. (See chart 5.) If they do not meet these other criteria, then you need to re-assign the complaint function to the person you appoint as public information officer. If no, identify an individual or department that has the capacity to work on patient complaints. Designate that person or department as the public information officer, if they also meet the other criteria for that position.. (See chart 5.)		
2. Do you currently have a process for patients to complain to you if they are dissatisfied?	If yes, compare your current process to that described in "Action Steps". Use the worksheet attached to this chart, if desired. Note any points that need to be changed. Make necessary changes. You must document your process in a written policy. If no, establish a process. You must document the process in a written policy.	1. You can use the same complaint process for complaints about privacy as you use for other kinds of complaints, so long as the process satisfies the criteria in "Action Steps." 2. Keep the complaint policy in your office's permanent records.	The process and policy for handling patient complaints about privacy issues should contain the following elements: • Be in writing • Describe a process for complaint intake, including written documentation of all new complaints • Describe how to gather facts in order to investigate the complaint – What office documents should be examined? – What personnel should be interviewed or consulted? – What outside resources should be reviewed or involved?

YOU MUST HAVE A COMPLAINT POLICY AND PROCEDURE

Assessment Question	Yes/No	Comments	Action Steps
		3. Keep documentation of each complaint for at least six years.	• Require the public information officer to determine whether the patient's complaint is substantiated or not. • Require the public information officer to propose a way that the complaint should be corrected, if it is substantiated: – Is a new office process needed? – Is mitigation of a wrongful disclosure of PHI needed? What would appropriate mitigation be in a given situation? – Does a work force member need to be sanctioned? – Does a business associate contract need to be terminated? – Is in-service training warranted? – Is there a possibility that other patients experienced the same problem, and should steps be taken to correct the problem for them as well? – Do HIPAA-related documents need to be revised? • Identify who in the office has authority to "sign off" on any proposals from the public information officer, particularly if any such proposals involve spending money or terminating contracts. • Identify a method to communicate the resolution to the patient. • Require the public information officer to propose and get approval for a method to monitor the effectiveness of the solution that was adopted. • If monitoring reveals uncorrected problems, require the public information officer to report this to the privacy officer for action. Use the model complaint policy 27A, if desired.

Completed _____ Date _____

YOU MUST HAVE A COMPLAINT POLICY AND PROCEDURE (WORKSHEET)

_____
Signature of responsible person

Current Complaint Process	Needed Changes

Doctor's Name
Address
Phone

HANDLING PATIENT COMPLAINTS ABOUT PRIVACY VIOLATIONS

Policy Number: 27A Effective Date _____

In order to comply with HIPAA's Privacy Rule, it is the policy of this office to accept complaints from patients who believe that we have not properly respected their privacy, and to thoroughly investigate and resolve them.

1. Our Public Information Officer ("PIO") is responsible for accepting all patient complaints about alleged privacy violations. We require all complaints to be in writing. If a complaint comes over the telephone, the PIO will inform the patient to send it in writing. This can be hard copy or electronic, as the patient wishes. If a patient wishes to remain anonymous, we will accommodate that to the extent practical.

2. The PIO will keep all patient complaints for at least six years. These will be stored, along with information about the investigation and resolution of the complaint, in [specify location in your office where complaints will be stored].

3. Upon receiving a patient complaint about privacy, the PIO will investigate it. The PIO has discretion to conduct the investigation in the manner considered reasonable and logical in light of the nature of the complaint. Generally, the PIO will do at least the following in order to investigate a complaint:

a. Talk to the person in the office whom the patient thinks violated the patient's privacy.

b. Review the patient's clinical chart.

c. Talk to other office staff about the patient's concern.

d. Talk to the patient.

e. Review any information or evidence that the patient presents in support of the claim of a violation of privacy.

4. Based upon the results of the investigation, the PIO will determine if the patient's complaint is substantiated or not. If the complaint is not substantiated, the PIO will notify the patient in writing. If it is substantiated, the PIO will determine what steps are necessary to resolve the issue so that it does not recur.

5. In determining what steps are necessary to resolve a substantiated complaint of a violation of privacy, the PIO will consider at least the following points:

HANDLING PATIENT COMPLAINTS ABOUT PRIVACY VIOLATIONS

Policy Number: 27A Effective Date _____

a. What caused the privacy violation?

b. If the violation was caused by a failure to comply with existing policy, the PIO will report the issue to [insert name/title] for action as a human resources disciplinary matter.

c. If the problem was caused by a lack of an appropriate policy, or an inadequate policy, the PIO will consult with our Privacy Officer (PO) to determine how the policy should be changed, or if a policy needs to be developed. If policy revisions or new policies are needed, the PIO will work with the PO to accomplish that.

d. If a business associate was involved in the violation, what must the business associate do to prevent the violation from recurring. If the business associate cannot cure the breach, the business associate contract must be terminated. The PIO will consult with the PO, who will obtain approval from management before any business associate contracts are terminated.

e. If the privacy violation caused harm, what steps are necessary to mitigate that harm? The PIO will consult with the PO to accomplish the steps.

6. Once a resolution of a complaint is determined, the PIO and the PO will work cooperatively to take the steps identified as necessary for the resolution.

7. If new policies or procedures are put into place as part of the resolution, the PO will conduct mandatory training for our workforce regarding them.

8. The PIO will develop a way to monitor whether the resolution is working to improve our privacy protections. The PIO will report to the PO on the results of the monitoring. If the PIO discovers continued problems through monitoring, the PIO and the PO will work cooperatively to fix the problems.

Completed _____ Date _____

YOU CAN USE OR DISCLOSE DE-IDENTIFIED INFORMATION WITHOUT ANY CONCERN ABOUT HIPAA'S PRIVACY PROTECTIONS

_____

Signature of responsible person

Requirement	Comments	Action Steps
1. De-identified information is PHI that is stripped of all identifiers.	1. You can de-identify PHI in one of two ways: • A statistical expert can give an opinion that PHI has been de-identified; or • You can remove the specific identifiers listed in HIPAA's "safe harbor" method. These are discussed in items 2 and 3 of this chart. 2. HIPAA encourages you to use de-identified information whenever possible. You might be able to use this kind of information for: • Some health care operations • Research	1. HIPAA does not require that you ever use de-identified information. This is an option for you in situations where it is feasible and practical. None of HIPAA's restrictions on the use or disclosure of protected health information apply to the use or disclosure of de-identified information. 2. Consider whether it might be reasonable for your practice to use de-identified information. If you conclude that de-identified information is not practical for you, skip the rest of this chart. Otherwise, go to items 2 and 3.
2. You can consider information to be de-identified if a statistical expert gives you an opinion that there is no reasonable basis to believe that the stripped information can be used to identify a particular patient.	1. The statistician must: • Conclude that the risk is very small that an anticipated recipient of the stripped information could use it, alone or in combination with other reasonably available information, to identify a patient. • Document the methods and analysis that he used to reach this conclusion.	1. If you think you might want to use a statistician, identify community resources. 2. Such a statistician would be your business associate. You would need to have a business associate contract in place. See chart 21.)
3. You can de-identify PHI by removing each of a list of identifiers, so long as you have no actual knowledge that a particular patient could still be identified from the stripped information.	1. If you use this method, you must remove each of the following identifiers about your patient, your patient's relatives, members of your patient's household, or employer: • Name. • All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geo codes, except for the initial three digits of a zip code if, according to the current	1. If you want to use the "safe harbor" method, • Identify someone in your office who will be responsible for removing all the identifiers. • Write a policy describing the steps

Requirement	Comments	Action Steps
	publicly available data from the Bureau of the Census: – The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and – The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000. • All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older. • Telephone numbers; • Fax numbers; • Electronic mail addresses; • Social security numbers; • Medical record numbers; • Health plan beneficiary numbers; • Account numbers; • Certificate/license numbers; • Vehicle identifiers and serial numbers, including license plate numbers; • Device identifiers and serial numbers; • Web Universal Resource Locators (URLs); • Internet Protocol (IP) address numbers; • Biometric identifiers, including finger and voice prints; • Full face photographic images and any comparable images; and • Any other unique identifying number, characteristic, or code.	necessary to de-identify information in this way. 2. Keep this policy with your office records. 3. A model policy 28A, accompanies this chart. Use the model policy, if desired.

Doctor's Name
Address
Phone

DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION

Policy Number: 28A Effective Date _____

It is the policy of this office to use de-identified information instead of protected health information whenever this is feasible. None of HIPAA's Privacy Rule's restrictions on the use and disclosure of protected health information apply to de-identified information, which can be used or disclosed freely.

1. [Specify name or title] is responsible for determining the feasibility of de-identifying any protected health information that we have about our patients, and for performing such de-identification if it is feasible.

2. If we de-identify protected health information, we will use HIPAA's "safe harbor" method of eliminating all specified identifiers. We will remove all the identifiers with respect to our patient, the patient's relatives, the patient's household members, and the patient's employer. The identifiers that we will remove are the following:

a. Names;

b. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

(i) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

(ii) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

c. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

d. Telephone numbers;

e. Fax numbers;

f. Electronic mail addresses;

g. Social security numbers;

h. Medical record numbers;

i. Health plan beneficiary numbers;

j. Account numbers;

k. Certificate/license numbers;

l. Vehicle identifiers and serial numbers, including license plate numbers;

m. Device identifiers and serial numbers;

n. Web Universal Resource Locators (URLs);

o. Internet Protocol (IP) address numbers;

p. Biometric identifiers, including finger and voice prints;

q. Full face photographic images and any comparable images; and

r. Any other unique identifying number, characteristic, or code.

3. Even after we have removed all the identifiers listed in paragraph 2, we will not consider information to be de-identified unless we have no actual knowledge that the remaining information can be used, either alone or in combination with other reasonably available information, to identify a patient.

4. If we disclose de-identified information, we will not disclose any key that we have to re-identify the information.

5. [We may use an outside company to help us de-identify protected health information. If we do, we will enter into a business associate contract with this outside company.]

THE RULES FOR PROTECTION OF PHI ARE RELAXED FOR LIMITED DATA SETS

Completed _____ Date _____

_____

Signature of responsible person

Requirement	Comments	Action Steps
1. A limited data set is a subset of PHI. It is not the same thing as de-identified information. (See chart 28.) • A limited data set is stripped of some identifiers, but not all identifiers. • You are never required to use a limited data set. A limited data set is an option for you in certain circumstances (discussed in this chart) to make certain kinds of disclosures of PHI simpler.	The identifiers that must be stripped from PHI to qualify it as a "limited data set" are listed on the "Definitions" page accompanying this chart.	
2. A limited data set can only be used for the following purposes: – research – public health – health care operations	1. Even if you don't use a limited data set, you can disclose PHI to a health plan or provider affected by HIPAA so that the plan or provider can use it for some of their own health care operations. (See chart 8.) Generally, you can only do this for health care operations relating to quality assurance, or fraud prevention. 2. If you choose to use a limited data set, however, you can share it for any health care operations at all. For example: • Business planning for a health plan or provider. • Sale or merger of a health plan, or • Financial management of a health plan or provider. • Any other health care operation. (See definitions accompanying chart 8.)	1. If you think that you may want to use a limited data set: • Identify someone in your office who can create the limited data set • Write a policy describing how and when you will use the limited data set. 3. A model policy, 29A accompanies this chart. Use the model policy, if desired.

THE RULES FOR PROTECTION OF PHI ARE RELAXED FOR LIMITED DATA SETS

Requirement	Comments	Action Steps
3. You do not need any patient permission to use or disclose a limited data set. However, whenever you disclose a limited data set, you have to get a "data use agreement" from the person you gave the information to.	1. A data use agreement is very similar to a business associate agreement, but it is not the same thing. 2. The minimum terms of a data use agreement are specified by HIPAA. They are: • Describe what uses and disclosures the recipient of the limited data set can make of the information in it. • Describe who is permitted to use or receive the limited data set. • Prohibit the recipient from using or disclosing the information in a way not permitted by the data use agreement or required by law. • Require the recipient to use appropriate safeguards to protect the information. • Require the recipient to tell you about any wrongful use or disclosure of the information that it knows about. • Require the recipient to ensure that any agents or subcontractors agree to the same conditions as the recipient. • Prohibit the recipient from identifying the patient or contacting the patient.	1. If you think that you will use limited data sets, obtain a model data use agreement. 2. Use the model agreement, 29B, accompanying this chart, if desired.
4. If you use a limited data set, you don't have to worry about: • Getting a signed patient authorization • Complying with the minimum necessary rule. (See chart 24.) • Including the disclosed information in a patient accounting. (See chart 17.)		

THE RULES FOR PROTECTION OF PHI ARE RELAXED FOR LIMITED DATA SETS

Definitions: A limited data set means:

1. PHI that excludes the following direct identifiers about a patient or of relatives, employers, or household members of the patient:
    - (i) Names;
    - (ii) Postal address information, other than town or city, State, and zip code;
    - (iii) Telephone numbers;
    - (iv) Fax numbers;
    - (v) Electronic mail addresses;
    - (vi) Social security numbers;
    - (vii) Medical record numbers;
    - (viii) Health plan beneficiary numbers;
    - (ix) Account numbers;
    - (x) Certificate/license numbers;
    - (xi) Vehicle identifiers and serial numbers, including license plate numbers;
    - (xii) Device identifiers and serial numbers;
    - (xiii) Web Universal Resource Locators (URLs);
    - (xiv) Internet Protocol (IP) address numbers;
    - (xv) Biometric identifiers, including finger and voice prints; and
    - (xvi) Full face photographic images and any comparable images.

Doctor's Name
Address
Phone

LIMITED DATA SETS

Policy Number: 29A Effective Date _____

It is the policy of this office to use a limited data set for certain disclosures of protected health information, whenever this is appropriate and feasible.

1. We will only use a limited data set for disclosures that are for research, public health purposes, or health care operations.

2. A limited data set is protected health information from which all of the following identifiers have been removed:

a. Names;

b. Postal address information, other than town or city, State, and zip code;

c. Telephone numbers;

d. Fax numbers;

e. Electronic mail addresses;

f. Social security numbers;

g. Medical record numbers;

h. Health plan beneficiary numbers;

i. Account numbers;

j. Certificate/license numbers;

k. Vehicle identifiers and serial numbers, including license plate numbers;

l. Device identifiers and serial numbers;

m. Web Universal Resource Locators (URLs);

n. Internet Protocol (IP) address numbers;

o. Biometric identifiers, including finger and voice prints; and

p. Full face photographic images and any comparable images.

In order to consider protected health information to be a limited data set, we will remove all of these identifiers about our patient, the patient's elatives, members of the patient's household, and the patient's employer.

3. [Specify name or title] is responsible for determining whether it is feasible and practical for us to disclose a limited data set, and if so, to create it.

4. Whenever we disclose a limited data set, we will require the recipient to enter into a data use agreement with us. The data use agreement restricts the ways in which the recipient can use the limited data set. We will use the master data use agreement accompanying this policy.

DATA USE AGREEMENT

This Data Use Agreement ("DUA")is made and entered into between _____ D.D.S. or D.M.D. ("Doctor"), having a principal place of business at [insert address], and _____ ("Data User") having its principal place of business at _____.

RECITALS:

Doctor is a "covered entity" within the meaning of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and the standards for the Privacy of Individually Identifiable Health Information ("Privacy Rule") promulgated by the Department of Health and Human Services ("DHHS") pursuant thereto.

Doctor will provide Data User with a "limited data set" ("LDS") of information for research, public health, or health care operations purposes.

The Privacy Rule requires that a covered entity enter into a data use agreement as a prerequisite to disclosing a LDS.

For the foregoing reasons, Doctor and Data User desire to enter into an agreement that complies with all the requirements of the Privacy Rule regarding use of a LDS.

NOW THEREFORE, in consideration of the foregoing and of the mutual promises contained herein, Doctor and Data User agree as follows:

I. DEFINITION OF TERMS

Any terms used in this DUA that are defined in the Privacy Rule shall have the same meaning when used in this DUA as they have in the Privacy Rule.

II. OBLIGATIONS OF DATA USER

(a) Data User is authorized to use the LDS as necessary and appropriate to perform the following purposes authorized by the Privacy Rule:

[*insert description of purposes for which Data User can use the LDS – e.g. description of research project, description of public health purpose, etc.*]

(b) The following individuals at the Data User are authorized to receive and use the LDS:

[insert names of authorized recipients and users]

(c) Data User agrees to not use or further disclose the LDS other than as permitted or required by this DUA or as required by law.

(d) Data User agrees to use appropriate safeguards to prevent use or disclosure of the LDS other than as provided for by this DUA. [*"Appropriate safeguards" include, but are not limited to, physical, administrative and technical safeguards such as locking cabinets or rooms where the LDS is housed, using computer passwords or other security measures to prevent unauthorized access to the LDS in electronic format; implementing policies and procedures describing authorized access and use for Data User's work force; and human resources policies and procedures to enforce these rules.*]

(e) Data User agrees to report to Doctor any use or disclosure of the LDS in violation of this DUA.

(f) Data User agrees to ensure that any agent, including a subcontractor, to whom it provides the LDS agrees to the same restrictions and conditions that apply through this DUA to Data User.

(g) Data User agrees that it will not identify the information in the LDS or contact the individuals about whom the LDS pertains.

IV. TERM AND TERMINATION

(a) Term. The term of this DUA shall commence on[insert effective date], and shall continue until [insert expiration date], unless sooner terminated in accordance with paragraph IV(b) hereof.

(b) Termination for Cause. Upon Doctor's actual knowledge of a pattern of activity or practice of Data User that constitutes a material breach by Data User, Doctor shall:

(1) Provide a 15 day opportunity for Data User to cure the breach or end the violation to Doctor's satisfaction, or terminate this DUA and not provide further information to Data User if Data User does not cure the breach to Doctor's satisfaction, and report the matter to DHHS.

[*(c) In addition to the termination for cause provisions stated in paragraph IV(b), this DUA may also be terminated in any of the following circumstances:*

(1) The provisions of the Privacy Rule are amended, modified or changed such that a DUA such as this is no longer mandated;

(2) By the mutual agreement of Doctor and Data User, provided that either a new DUA must be substituted or DOCTOR must stop providing information to Data User pursuant to the LDS.]

(d) Effect of Termination.

(1) Except as provided in paragraph (2) of this section, upon termination of this DUA for any reason, Data User shall return or destroy all the LDS received from Doctor, as directed by Doctor. Doctor has the sole authority to determine whether the LDS shall be returned or destroyed, and shall have the sole authority to establish the terms and conditions of such return or destruction. This provision shall apply to the LDS that is in the possession of subcontractors or agents of Data User. Data User shall retain no copies of the LDS.

(2) In the event that Data User believes that returning or destroying the LDS is infeasible, Data User shall provide to Doctor an explanation of the conditions that make return or destruction infeasible. Upon Doctor's concurrence that return or destruction of the LDS is infeasible, Data User shall extend the protections of this DUA to such LDS and limit further uses and disclosures of such the LDS to those purposes that make the return or destruction infeasible, for so long as Data User maintains such LDS.

[*(3) If this DUA is terminated and not immediately replaced with a substitute DUA, and if the Privacy Rule at that time continues to mandate the execution of a DUA between covered entities and Data users, then the DOCTOR shall immediately stop providing information to Data user pursuant to the LDS.*]

V. GENERAL PROVISIONS

[*(a) DATA User shall indemnify Doctor for any losses, costs or expenses that Doctor sustains, including fines under HIPAA, as a result of any breach by Data User of any of its obligations under this DUA.*]

[*(b) Data User shall maintain during the term of this DUA a policy of errors and omissions or other comparable insurance with an insurer acceptable to Doctor in the amount of _____, covering Data User's obligations under this DUA. The policy of insurance shall name Doctor as an additional insured. Data User shall furnish to Doctor such evidence of this insurance as Doctor deems satisfactory upon the commencement of this DUA. Data User shall notify Doctor of any threatened or actual cancellation or termination of the insurance coverage, at least ten days prior to any such action.*]

[*(c) Data User agrees that the terms and conditions of this DUA shall be construed as a general confidentiality agreement that is binding upon Data User even if it is determined that no DUA is mandatory with respect to the relationship between Doctor and Data User pursuant to the Privacy Rule.*]

[*(d) Doctor and Data User shall not be deemed to be partners, joint venturers, agents or employees of each other solely by virtue of the terms and conditions of this DUA.*]

[*(e) This DUA shall not be modified or amended except by a written document that is signed by both parties. Doctor and Data User agree to modify or amend this DUA if the Privacy Rule changes in a manner that affects the terms and conditions of this DUA, or the obligations of covered entities and/or data users.*]

[*(f) Any communications between Doctor and Data User regarding this DUA shall be in writing, whether or not oral communications have also occurred. Such communications shall be sent to the following individuals at the following addresses:*

To Doctor *To Data User*

Written communications may be sent by certified or registered U.S. Mail, receipted courier service, receipted hand delivery, receipted fax, or by receipted email.]

[*(g) No waiver of any provision of this Agreement, including this paragraph, shall be effective unless the waiver is in writing and signed by the party making the waiver.*]

[*(h) This DUA is entered into solely for the benefit of the parties, and is not entered into for the benefit of any third party, including without limitation, any patients of Doctor or their legal representatives.*]

[*(i) This DUA is not assignable or delegatable without the express advance written consent of the party not seeking to assign or delegate.*]

[*(j) This DUA shall be governed by and construed in accordance with the laws of the United States of America and the laws of the state of[insert state]*.]

[*(k) If any provision of this DUA is determined by a court of competent jurisdiction to be invalid or unenforceable, this DUA shall be construed as though such invalid or*

unenforceable provision were omitted, provided that the remainder of this DUA continues to satisfy all of the Privacy Rule's requirements for a data use agreement. If it does not, then the parties shall immediately renegotiate this DUA so that it does comply with the requirements of the Privacy Rule, or terminate this DUA and the flow of information pursuant to the LDS between the Data User and Doctor.]

[*(l) This DUA contains the entire agreement between the parties pertaining to this subject matter, and supercedes all prior understandings, whether written or oral, regarding the same subject matter.*]

[*(m) The provisions of this DUA dealing with indemnification, insurance, and the construction of this DUA as a general confidentiality agreement shall survive the termination of this DUA for any reason.]*

In witness whereof, the parties have executed this Data Use Agreement on the ____ day of _____, 200__.

Witness **(DOCTOR)**

_____ By _____

Its _____

Dated _____

Witness **(DATA USER)**

_____ By _____

Its _____

Dated _____

Completed _____ Date _____

YOU MUST TRAIN YOUR WORKFORCE

_____

Signature of responsible person

Assessment Question	Comments	Action Steps
1. Identify the members of your work force. Use the worksheet accompanying this chart, if desired.	1. Work force includes more people than your payroll. Work force includes: • All W2 employees. • Students (all kinds). • Volunteers. • Any independent contractor working on-site and under your direct control that you have not treated as a business associate. (See chart 20.)	
2. What training methods are practical in your office? Consider your budget, the time available for training, and how your work force best learns.	1. Training can take any form. It can be: • Live lectures. • Purchased on-line training modules. • Review of policies/procedures. • Workbooks. • Any other method that you devise. 2. Training needs to be job specific.	
3. When is the best time to schedule training in your office? Initial training must take place before April 14, 2003.	1. All existing work force members must be trained before April 14, 2003. 2. Any new work force member must be trained within a reasonable time after joining. 3. All members must be trained within a reasonable time after any change in policy or procedures affecting HIPAA.	1. Select an appropriate training method or source. 2. Schedule training sessions. 3. Document attendance. 4. Keep attendance rosters for at least six years.

Completed _____ Date _____

YOU MUST TRAIN YOUR WORK FORCE (WORKSHEET)

_____

Signature of responsible person

Name of Work Force Member	Date Scheduled for Training	Attended (yes/no)

YOU MUST TRAIN YOUR WORK FORCE (WORKSHEET)

Name of Work Force Member	Date Scheduled for Training	Attended (yes/no)

YOU MUST TRAIN YOUR WORK FORCE (WORKSHEET)

Name of Work Force Member	Date Scheduled for Training	Attended (yes/no)

SOME STATE PRIVACY LAWS REMAIN RELEVANT AFTER HIPAA

Completed _____ Date _____

_____
Signature of responsible person

Type of State Law	Status after HIPAA	Comments	Action Steps
1. A state law that does not either: • **Have a specific purpose to protect privacy of health information, or** • **Relate directly, clearly and substantially to the privacy of individually identifiable health information.**	All such laws remain fully effective after HIPAA.		
2. A state law that relates to the privacy of individually identifiable health information, but which is not contrary to HIPAA.	All such laws remain fully effective after HIPAA. You must comply with both the state law and HIPAA.	A law is "contrary to" HIPAA if it is physically impossible for you to comply with both the state law and HIPAA.	1. Identify state privacy laws that are not contrary to HIPAA that affect your practice. Use the worksheet accompanying this chart, if desired. 2. Decide what you will do to comply with both. For example, if your state law says that a patient authorization must include a term that is not inconsistent with HIPAA, then you can comply with both HIPAA and the state law by writing an authorization form that includes all of HIPAA's required terms plus the term required by your state law. 3. Take the actions that you decide are necessary to comply with both HIPAA and the state law.

SOME STATE PRIVACY LAWS REMAIN RELEVANT AFTER HIPAA

Type of State Law	Status after HIPAA	Comments	Action Steps
3. A state law that relates to the privacy of individually identifiable health information and is contrary to HIPAA.	General rule: HIPAA wipes out the state law, which is no longer effective. You cannot comply with the state law.	1. A law is "contrary to" HIPAA if it is physically impossible for you to comply with both the state law and HIPAA. 2. There is a significant exception to the general rule. A state law is not wiped out if it is contrary to HIPAA but "more stringent than" HIPAA. This exception is discussed in item 4 of this chart.	1. Identify the state privacy laws that affect your practice that are contrary to HIPAA. Use the worksheet accompanying this chart, if desired. In some states, trade associations or other professional groups are analyzing privacy laws. 2. Modify any policies, procedures or practices that you use which are based upon the ineffective state law.
4. A state law that relates to the privacy of individually identifiable health information and is contrary to HIPAA, but is "more stringent than" HIPAA.	All such laws remain in effect after HIPAA. You must comply with the state law, not HIPAA.	1. A law is "more stringent than" HIPAA in any of the following circumstances: • It prohibits a use or disclosure that HIPAA permits. • It allows patients more access or amendment rights than HIPAA does. • It requires that you include more information in notices to patients about their privacy rights than HIPAA does. • It requires patients to give express permission for a use or disclosure when HIPAA doesn't, or makes the kind of express permission more protective of privacy rights than HIPAA does. • It requires you to keep documents longer than HIPAA does, or to give patients more information in an accounting of disclosures than HIPAA does. • It otherwise provides more privacy protections for patients than HIPAA does. 2. If you have to comply with a state law instead of HIPAA, or if a state law affects how you comply with HIPAA, you must discuss the state law in your Notice of Privacy Practices.	1. Identify which contrary state privacy laws are "more stringent than" HIPAA. Use the worksheet accompanying this chart, if desired. In some states, trade associations or other professional organizations are analyzing state law. 2. Make sure that any policies or procedures that you prepare address the state law.

SOME STATE PRIVACY LAWS REMAIN RELEVANT AFTER HIPAA (WORKSHEET)

Completed _____ Date _____

_____
Signature of responsible person

Laws that aren't contrary to HIPAA	Laws that are contrary to HIPAA	Contrary Laws that are more stringent than HIPAA

SOME STATE PRIVACY LAWS REMAIN RELEVANT AFTER HIPAA

END