

TABLE OF CONTENTS

Preface	IX
Introduction	XII

ONE PATIENT RIGHTS AND OBLIGATIONS OF COVERED ENTITIES PERTAINING TO PATIENT RIGHTS 1

Right to receive a notice of privacy practices 1

Disseminating the privacy notice	1
Exceptions to the right to receive a privacy notice	1
Privacy notice standards	2
Privacy notice revisions	3
Documenting notice compliance	5

Right to access records 5

Records a patient may access	6
Records not available for patient access	6
Process for patient information requests	7
When a denial of access to records may not be appealed	7
Notice of denial requirements	7
Appealing a denial of access to records	8
Appeal process	8
Providing access	8
Documenting access requests	9

Right to amend PHI 9

Process for amendment requests	9
When a patient does not have a right to request an amendment	9
Timing of actions	10
Format for a denial to an amendment request	10
Handling a statement of disagreement from a patient denied an amendment to PHI	10
After a request for amendment is accepted	11
Receiving notices of amendment from other covered entities	11
Transmission of amended information	11
Documentation of amendment requests	11

Right to confidential communications	12
Requests from the patient	12
Entity requirements when accommodating requests for confidential communications	12
Right to request additional restrictions on use and disclosure of PHI	12
Disallowed additional restrictions	13
When covered entity agrees to additional restrictions	13
Terminating an agreement to provide additional restrictions	13
Documenting an additional restrictions agreement	14
Right to receive an accounting of PHI disclosures	14
Disclosure exceptions	14
Information pertaining to each disclosure that must be retained by the covered entity	14
Special rules for multiple disclosures	15
Temporary suspension of right to accounting of PHI for health oversight and law enforcement	17
Retention of information pertaining to disclosures of PHI	17
Timing for responding to patient requests for an accounting of disclosures of PHI	17
Allowable fees associated with responding to patient requests for an accounting of disclosures of PHI	17
Documenting requests for an accounting of PHI disclosures	18
TWO ADMINISTRATIVE REQUIREMENTS	19
Personnel designation	19
Mitigation	19
Sanctions for violations	20
Documenting sanctions	20
Sanctions for non-workforce personnel	20
Workforce policies and procedures training	21
Policy changes	21
New staff members	21
Documenting compliance	21

Safeguards for protecting PHI	21
Incidental use of PHI	21
Workforce vigilance	22
Prohibition against intimidation or retaliation	22
Prohibition against actions that cause rights to be waived ...	22
Complaint process	22
Documentation	22
Designing policies and procedures	23
Customizing guidelines	23
Allowable compliance variations	23
Revision of policies and procedures	23
Documenting changes to policies and procedures	24
Documenting reasons for policy changes	24
Retaining documentation	24
The documentation process	24
THREE USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION (PHI)	27
WHEN USE AND DISCLOSURE IS NOT PERMITTED	27
USE AND DISCLOSURE OF PHI FOR TREATMENT, PAYMENT AND HEALTH CARE OPERATIONS	27
Overview	27
Use of PHI within a covered entity	28
Obtaining and Documenting written acknowledgement of privacy notice	28
Obtaining written acknowledgement of privacy notice	28
Documenting receipt of a written acknowledgement	28
When an individual refuses or cannot acknowledge a privacy notice	29

Documenting a “good faith” effort to obtain an acknowledgment	29
Disclosures to others for their treatment, payment and health care operations activities	29
Use and disclosures of PHI by health care providers giving indirect treatment and privacy notice requirements	30
Accommodating privacy notice practices in emergencies	31
Posting the privacy practices notice	31
Notice of electronic privacy practices	31
Privacy practice notices with websites	31
Delivering Privacy Practices Notice by E-mail	31
Retaining documentation about privacy practice notices	32
Use and disclosure of PHI for marketing purposes	32
Exceptions to marketing rules	34
Violations of marketing rules	34
Other special marketing provisions	34
Use and disclosure of PHI for fundraising purposes	35
USE AND DISCLOSURE OF PHI WITH RESPECT TO FAMILY MEMBERS, RELATIVES AND CLOSE PERSONAL FRIENDS	36
Overview	36
Use and disclosure of PHI in facility directories	36
Patient directories and what information may be included	36
Patient opportunity to opt out of facility directory, or to object to uses or disclosures of information in facility directory	36
Patient objection to disclosures of directory information, and patient objections to inclusion in facility directory	37
Disclosing directory information when the patient does not object	37
Directory rules in emergency treatment situations and patient incapacity	37
Disclosing information to others involved in patient care	38
When a patient is available before disclosure	38

When a patient cannot agree or object to disclosure	38
When allowing someone to pick up patient prescriptions, medical supplies, X-rays, or other similar forms of PHI	38
Using or disclosing PHI to assist in disaster relief efforts	38
USE AND DISCLOSURE OF PHI FOR PUBLIC HEALTH, RESEARCH AND GOVERNMENT-REQUESTED PURPOSES	39
Overview	39
Use and disclosure of PHI when required by law	40
Use and disclosure of PHI for public health	40
Use and disclosure of PHI for adult victims of abuse, neglect, and domestic violence	41
Use and disclosure of PHI for health oversight activities	42
Use and disclosure of PHI for judicial and administrative proceedings	42
Use and disclosure of PHI for law enforcement	43
Under law enforcement processes	44
For identification and location purposes	44
Related to victims of a crime	45
About decedents	46
Crime on premises	46
Reporting crime in emergencies	46
Use and disclosure of PHI to coroners, medical examiners and funeral directors	46
Use and disclosure of PHI for cadaveric organ, eye or tissue donation purposes	46
Use and disclosure of PHI for research purposes	47
General criteria for use and disclosure of PHI for research	47
Composition of privacy board	48
Rules on waiving or modifying authorizations	48
Use and disclosure of PHI for recruiting research subjects	49
Disclosing PHI for research registries and research data repositories	50

Use and disclosure of PHI to avert a serious threat to health or safety	50
Use and disclosure of PHI for specialized government functions	51
Disclosures pertaining to U.S. and foreign military	51
Disclosures pertaining to national security	51
Disclosures pertaining to correctional institutions	52
Disclosures pertaining to government public benefits programs	52
Use and disclosure of PHI related to workers' compensation ..	52
Rules on verification for public health, research, and government-requested PHI disclosures	53
Verifying identity and authority prior to disclosure	53
Verification of personal representatives, and overlap with professional judgment rules	53
When specific documents, statements, or representations are required	54
When verifying the identity of public officials	54
When verifying the authority of public officials or their representatives	54
USE AND DISCLOSURE OF PHI WHEN AUTHORIZED BY A PATIENT	55
Overview	55
Authorization forms for use and disclosure of PHI	55
Revocation of authorizations	57
"Conditioning" rules	57
Compound authorizations	58
Invalid authorizations	58
Use and disclosure authorizations pertaining to psychotherapy notes	59

PRINCIPLE OF USING OR DISCLOSING ONLY THE MINIMUM NECESSARY PHI	59
Overview	59
Defining “reasonable efforts” to limit PHI	59
Use and disclosures exempted from the minimum necessary rule	60
Minimum necessary information for external disclosures	60
Routine/recurring disclosures	60
Non-routine requests	60
Standardized requests that meet minimum necessary rule	60
Requests for an entire medical record	61
Minimum necessary information for internal uses	61
Requesting minimum necessary PHI from other covered entities	62
Routine/recurring requests	62
Non-routine requests	62
Requests for entire medical records	62
FOUR OTHER REQUIREMENTS	63
Contracting with business associates	63
When contracts are required	63
When contracts are not required	63
Uses and disclosures of PHI by business associates	64
Permissible contract terms	65
Consequences of breach	66
Rules for government entities	66
Timing of business associate requirements	67
Organizational options	68
Categories of organizational options	68
Qualifying as an OHCA or ACE	69
Qualifying as a hybrid covered entity	69
Benefits of participating in an OCHA	70
Benefits of participating in an ACE	71
Benefits of declaring a hybrid covered entity	72

HIPAA preemption	72
State laws that HIPAA does not override	73
Steps to determine when state laws preempt federal law	73
Documenting state/federal law sovereignty	74
FIVE COMPLIANCE—CARROTS AND STICKS	75
Key incentives and enforcement tools	76
Compliance incentives	76
Deterrents to non-compliance	76
Specific civil and criminal penalties	76
Civil penalties	76
Criminal penalties	76
Application of criminal penalties	77
Who is subject to HIPAA’s enforcement penalties	77
GLOSSARY	78
ATTACHMENT I: SAMPLE FORMS	93
Sample Form 1	
Notice of Privacy Practices Form (for a hospital)	93
Sample Form 2	
Notice of Privacy Practices Acknowledgement of Receipt Form	99
Sample Form 3	
Authorization Form for Use and Disclosure of Health Information	101