

HIPAA Update for Home Care Agencies

TABLE OF CONTENTS

PREFACE	6
CHAPTER I: INTRODUCTION	7
Background and history of HIPAA	7
HIPAA since 2005	11
An overview of the HITECH ACT and its impact on HIPAA compliance	13
Timelines and deadlines	14
How to use and update this manual	16
CHAPTER II: Breach Notification	17
Introduction	17
Definitions	17
Breach	17
Unsecured protected health information	18
Technologies and methods for securing PHI	18
Destruction	18
Encryption	19
Encryption and the Security Rule	19
Discovery of a breach	20
<i>Tool: Breach Risk Assessment</i>	22
<i>Tool: Breach Risk Assessment Summary</i>	24
Breach notification requirements	25
Notification requirements of individual(s) affected by a breach	25
Timeliness of notification	25
Content of a breach notification	26
<i>Template: Breach Notification Letter to an Individual</i>	27
Methods of notification	28
Notification to the media	29
Notification to the government	29
Breaches affecting 500 or more individuals	32
Breaches affecting fewer than 500 individuals	32
<i>Tool: Notice to the Secretary of HHS of Breach of Unsecured PHI</i>	34
Notification requirements for business associates	37
Administrative and burden of proof requirements	37
Training	38
<i>Tool: Sample Policy and Procedure: Privacy and Security Awareness and Training</i>	39
Sanctions	40
<i>Tool: Sample Policy and Procedure: Sanctions for Privacy and Security Violations</i>	41
Complaints and refraining from intimidating or retaliatory acts	42
<i>Tool: Sample Policy and Procedure: Complaint Resolution</i>	43

HIPAA Update for Home Care Agencies

TABLE OF CONTENTS

Documentation and burden of proof	44
Policies and Procedures	44
<i>Tool: Sample Policy and Procedure: Security Incidents</i>	45
<i>Tool: Sample Policy and Procedure: Breach Notification</i>	46
CHAPTER III: Business Associates	48
Introduction	48
Business associate requirements before the HITECH Act	48
What is a business associate?	48
The business associate agreement	49
Business associate requirements after the HITECH Act	50
What agencies need to do to comply with the new business associate requirements	53
<i>Template: Model Letter Notifying Business Associates That New Business Associate Addendum Must Be Executed</i>	54
<i>Template: Sample Privacy And Security Business Associate Addendum</i>	55
<i>Tool: Business associate policy and procedure</i>	62
CHAPTER IV: Other HITECH Changes to the HIPAA Privacy Rule	63
Introduction	63
Accounting of disclosures	
<i>Tool: Requests for an accounting of disclosures policy and procedure [for agencies that do not use an electronic health record]</i>	65
<i>Tool: Requests for an accounting of disclosures policy and procedure [for agencies that use an electronic health record]</i>	67
Requests for restrictions	69
<i>Tool: Requests for restrictions policy and procedure</i>	70
Requests for access	72
<i>Tool: Requests for access policy and procedure</i>	73
Minimum necessary standard	75
Marketing	75
Fundraising	76
<i>Tool: Fundraising and protected health information policy and procedure</i>	78
Notice of Privacy Practices	79
<i>Tool: Notice of Privacy Practices Policy and Procedure</i>	80
<i>Tool: Updated Notice of Privacy Practices</i>	81
CHAPTER V: Looking to the Future of HIPAA – the Future is Now	89
Introduction	89
Enforcement before the HITECH Act	89
Enforcement after the HITECH Act	90

HIPAA Update for Home Care Agencies

TABLE OF CONTENTS

Civil monetary penalties	90
Increased enforcement resources	91
Increased enforcement incentives	91
How to prepare for increased HIPAA scrutiny	91
Summary	92

TABLES:

Table 1: Similarities between the Privacy and Security Rules	10
Table 2: Differences between the Privacy and Security Rules	11
Table 3: HITECH Act's changes to HIPAA privacy and security requirements	14
Table 4: HITECH Act's timeline and deadlines	15
Table 5: Required contents of a breach notification letter	26
Table 6: List of common home care business associates	49
Table 7: Similarities and differences between Privacy Rule and Security Rule business associate requirements	50
Table 8: The HITECH Act's requirements related to business associates	51
Table 9: Standards and implementation specifications of the HIPAA Security Rule	52
Table 10: Violation categories, culpability and penalties	90

HIPAA Update for Home Care Agencies **Electronic Resources Folders**

Additional Resources Folder

Enforcement Resources Folder:

- CMS Compliance Reviews 2008
- CMS Compliance Reviews 2009
- Interview and Documentation Request for HIPA Onsite Investigation and Compliance Reviews
- RFQ – State Attorneys General HIPAA Training/SOW
- Enforcement Rule – October 30, 2009

NIST Publications

- SP 800-88 –Guidelines for Media Sanitation
- SP 800-52 – Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementation
- SP 800-111- Storage Encryption Technologies
- SP 800 – 66 – Introductory Resource Guide for Implementing the HIPAA Security Rule

HIPAA Update for Home Care Agencies

TABLE OF CONTENTS

Regulatory Texts

- Breach Notification Rule – August 24, 1009
- Subtitle D of the HITECH Act – February 17, 2009
- Privacy Final Rule – with Preamble – August 14, 2002
- Security Final Rule – with Preamble – February 20, 2003
- HIPAA Combined Regulation Text – OCR Publication of HIPAA Rules
- Enforcement Rule – October 30, 2009
- Guidance on Technologies and Methodologies for Securing PHI – April 27, 2009

Breach Notification Tools

- Breach Risk Assessment
- Breach Risk Assessment Summary
- Sample Breach Notification Letter to an Individual
- Notice to the Secretary of HHS of Breach of Unsecured PHI
- Breach Notification Policy and Procedure
- Privacy and Security Training Policy and Procedure
- Sanctions Policy and Procedure
- Security Incident Policy and Procedure
- Complaint Resolution Policy and Procedure

Business Associate Tools

- Model Business Associate Letter
- Business Associate Addendum
- Business Associate Policy and Procedure

Miscellaneous Provisions Folder

- Requests for an accounting of disclosures policy and procedure
[for agencies that do not use an electronic health record]
- Requests for an accounting of disclosures policy and procedure
[for agencies that do use an electronic health record]
- Requests for restrictions policy and procedure
- Requests for access policy and procedure
- Fundraising and protected health information policy and procedure
- Notice of Privacy Practices Policy and Procedure
- Updated Notice of Privacy Practices