

ALICE G. GOSFIELD

& ASSOCIATES, P.C.

**PHYSICIAN AND MEDICAL PRACTICE
HIPAA COMPLIANCE
PLAN DEVELOPMENT PROTOCOL**

by

Alice G. Gosfield and Associates, P.C.
2309 Delancey Place
Philadelphia, PA 19103
(215) 735-2384

E-Mail: Agosfield@gosfield.com, dshay@gosfield.com
Website: www.gosfield.com

The information here is presented as a service to readers. It is not intended as legal advice. We have attempted to provide information which is up to date, but rules often change. No one should rely on this information alone and should obtain current, informed legal guidance with regard to the issues contained herein. We make no representations, nor guarantees regarding the contents of the information contained herein.

Copyright 2016, Alice G. Gosfield and Associates, PC, all rights reserved

Table of Contents

Foreword	5
Glossary	7
1. Introduction	12
<i>1.1 The Transaction Rule</i>	12
<i>1.2 The Privacy Rule</i>	12
<i>1.3 The Security Rule</i>	12
<i>1.4 The Breach Notification Rule</i>	13
<i>1.5 The Omnibus Rule</i>	13
<i>1.6 Compliance and Penalties</i>	14
2. Twelve Common Myths Debunked	14
3. Overall Compliance Planning Considerations	16
<i>3.1. Compliance "Plans" and "Programs"</i>	16
<i>3.2. One Size Does Not Fit All</i>	16
<i>3.3. Usability</i>	17
4. Eight Steps to Privacy Compliance	17
<i>4.1. Determining Whether HIPAA Applies</i>	18
4.1.1 Which Transactions Apply	18
4.1.2 Are You a Covered Entity?	19
<i>4.2. Appointing a Privacy Officer</i>	19
4.2.1 Privacy Officer Overview	19
4.2.2 The Role of the Privacy Officer	20
<i>4.3. Identifying Sources of PHI</i>	21
4.3.1 Which Data is PHI	21
4.3.2 Knowing How PHI Flows In Your Practice	21
<i>4.4. Identifying Business Associates</i>	22
4.4.1 Business Associates Overview	22
4.4.2 Business Associates Duties	23
4.4.3 Analyzing When an Entity Is Your Business Associate	24

4.5.	<i>Drafting a Notice of Privacy Practices</i>	25
4.5.1	Contents of the Notice.....	25
4.5.2	How to Draft Your Notice of Privacy Practices.....	25
4.6.	<i>Drafting Authorizations for the Use of PHI</i>	26
4.6.1	Contents of an Authorization.....	26
4.6.2	Retention of Signed Authorizations and Other Requirements	27
4.6.3	When an Authorization is Needed	27
4.7.	<i>Develop and Implement Safeguards</i>	28
4.7.1	Overview of Safeguards	28
4.7.2	Scaling Safeguards to Meet Your Practice's Needs.....	29
4.8.	<i>Develop and Implement Administrative Policies and Procedures to Address Patient's Rights</i>	29
4.8.1.	The Right to Notice of Privacy Practices	29
4.8.2.	The Right of Access to PHI.....	31
4.8.3.	The Right to Amend PHI.....	33
4.8.4	The Right to Request Restrictions on the Use and/or Disclosure of PHI	34
4.8.5	The Right to Request Alternative Means of Communication	35
4.8.6	The Right to an Accounting of Disclosures of PHI	36
4.9.	<i>Workforce Issues</i>	37
4.9.1	Training.....	37
4.9.2	Complaints.....	38
4.9.3	Sanctions.....	38
4.9.4	Coercion.....	38
4.10.	<i>Additional Requirements</i>	39
4.10.1	Duty to Mitigate.....	39
4.10.2	Minimum Necessary Rule	39
4.10.3	Documentation and Recordkeeping	39
5.	Six Steps to Security Compliance	40
5.1	<i>Appointing a Security Officer</i>	41
5.1.1	Security Officer Overview.....	41
5.1.2	The Role of the Security Officer	41
5.2	<i>Conducting a Security Risk Analysis</i>	42
5.2.1	The Need for a Security Risk Analysis.....	42
5.2.2	Elements of a Security Risk Analysis.....	42
5.3	<i>Establishing Administrative Safeguards</i>	43

5.3.1	Standards for Administrative Safeguards	43
5.3.2	Workforce Access to EPHI	44
5.4	<i>Establishing Physical Safeguards</i>	45
5.4.1	Standards for Physical Safeguards.....	45
5.4.2	Office Layout, Physical Access Controls, and Mobile Devices.....	46
5.5	<i>Establishing Technical Safeguards</i>	46
5.5.1	Standards for Technical Safeguards	46
5.5.2	Password Security, Software Capabilities, and Transmission .	47
5.6	<i>Developing and Implementing Policies and Procedures</i>	47
5.6.1	Documentation Requirements.....	47
5.6.2	Practical Considerations	48
6.	Five Steps to Breach Notification Compliance	48
6.1	<i>Determining Whether a Breach Has Occurred</i>	49
6.1.1	What Is and Is Not a Breach.....	49
6.1.2	Scenarios: Breach or Not?.....	50
6.2	<i>Notifying Individuals</i>	51
6.2.1	Notification: Timeliness Requirements	51
6.2.2	Notification: Content Requirements	51
6.3	<i>Notifying the Media</i>	52
6.3.1	Media Notification Overview	52
6.3.2	Method and Content of Media Notification.....	52
6.4	<i>Notifying the Secretary of Health and Human Services</i>	52
6.4.1	Method for Notifying the Secretary	52
6.4.2	Who Should Submit Notification.....	53
6.5	<i>Addressing Administrative Requirements</i>	53
6.5.1	Privacy Rule Incorporation	53
6.5.2	Privacy Rule Requirements in a Breach Notification Context ..	53
7.	Conclusion	55
Exhibit A	Business Associate Agreement	56
Exhibit B	HIPAA Related Resources	62
Exhibit C	Additional Resources from Alice G. Gosfield and Associates, P.C.	63