

MARSH

MERCER
Human Resource Consulting

Sneak Peek



Security
Assessment for
Employers

HIPAA Self-Assess

Table of Contents

1. INTRODUCTION 7

2. STATEMENT OF SECURITY POLICY 10

3. ADMINISTRATIVE SAFEGUARDS 11

3.01 OVERVIEW 12

3.02 SECURITY MANAGEMENT PROCESS 13

A. RISK ANALYSIS 13

B. RISK MANAGEMENT 14

C. SANCTION POLICY 15

D. INFORMATION SYSTEM ACTIVITY REVIEW 16

E. CITATION 18

3.03 ASSIGNED SECURITY RESPONSIBILITY 19

A. CITATION 20

3.04 WORKFORCE SECURITY 21

A. AUTHORIZATION AND/OR SUPERVISION 21

B. WORKFORCE CLEARANCE PROCEDURE 22

C. TERMINATION PROCEDURES 23

D. CITATIONS 25

3.05 INFORMATION ACCESS MANAGEMENT 26

A. ISOLATING HEALTH CARE CLEARINGHOUSE FUNCTION 26

B. ACCESS AUTHORIZATION 28

C. ACCESS ESTABLISHMENT AND MODIFICATION 29

D. CITATIONS 30

3.06 SECURITY AWARENESS AND TRAINING 31

A. SECURITY REMINDERS 32

B. PROTECTION FROM MALICIOUS SOFTWARE..... 33

C. LOG-IN MONITORING 34

D. PASSWORD MANAGEMENT 35

E. CITATIONS..... 36

3.07 SECURITY INCIDENT PROCEDURES 37

A. RESPONSE AND REPORTING..... 37

B. CITATIONS..... 38

3.08 CONTINGENCY PLAN..... 39

A. DATA BACKUP PLAN..... 39

B. DISASTER RECOVERY PLAN..... 40

C. EMERGENCY MODE OPERATION PLAN..... 41

D. TESTING AND REVISION PROCEDURE 42

E. APPLICATIONS AND DATA CRITICALITY ANALYSIS 43

F. CITATIONS..... 44

3.09 EVALUATION..... 45

A. CITATIONS..... 46

4. PHYSICAL SAFEGUARDS..... 47

4.01 OVERVIEW..... 48

4.02 FACILITY ACCESS CONTROLS 49

A. CONTINGENCY OPERATIONS..... 49

B. FACILITY SECURITY PLANS..... 50

C. ACCESS CONTROL AND VALIDATION PROCEDURES 52

D. MAINTENANCE RECORDS 53

E. CITATIONS..... 54

4.03 WORKSTATION USE 55

A. CITATIONS..... 56

4.04 WORKSTATION SECURITY..... 57

A. CITATIONS..... 57

4.05 DEVICE AND MEDIA CONTROLS 58

A. DISPOSAL..... 58

B. MEDIA RE-USE..... 59

C. ACCOUNTABILITY..... 60

D. DATA BACKUP AND STORAGE..... 61

E. CITATIONS..... 62

5. TECHNICAL SAFEGUARDS 63

5.01 OVERVIEW..... 64

5.02 ACCESS CONTROL 65

A. UNIQUE USER IDENTIFICATION 65

B. EMERGENCY ACCESS PROCEDURE 66

C. AUTOMATIC LOGOFF..... 67

D. ENCRYPTION AND DECRYPTION..... 68

E. CITATIONS..... 69

5.03 AUDIT CONTROLS..... 70

A. CITATIONS..... 72

5.04 INTEGRITY 73

A. MECHANISMS TO AUTHENTICATE E-PHI..... 73

B. CITATIONS..... 74

5.05 PERSON OR ENTITY AUTHENTICATION 75

A. CITATIONS..... 76

5.06 TRANSMISSION SECURITY 77

A. INTEGRITY CONTROLS..... 77

B. ENCRYPTION 78

c. CITATIONS..... 79

6. REQUIRED LEGAL DOCUMENTS..... 80

6.01 OVERVIEW..... 81

6.02 BUSINESS ASSOCIATE CONTRACTS..... 82

A. CITATIONS..... 83

6.03 GROUP HEALTH PLAN AMENDMENTS..... 84

A. CITATIONS..... 85

6.04 DOCUMENTATION..... 86

A. TIME LIMIT 86

B. AVAILABILITY..... 86

C. UPDATES 86

D. CITATIONS..... 86

7. APPENDICES..... 87

7.01 E-PHI ACCESS CONTROL CHECKLIST..... 88

7.02 E-PHI BACKUP CHECKLIST 89

7.03 BUSINESS ASSOCIATE CONTRACTS 90

A. BUSINESS ASSOCIATE CONTRACT TRACKER..... 90

B. SAMPLE BUSINESS ASSOCIATE CONTRACT..... 91

7.04 COVERED PLANS..... 94

A. LIST OF COVERED PLANS..... 94

B. SAMPLE PLAN AMENDMENT..... 95

7.05 SECURITY OFFICIAL..... 96

A. SECURITY OFFICIAL CONTACT INFORMATION..... 96

THE FOLLOWING PERSON IS DESIGNATED AS THE SECURITY OFFICIAL: 96

B. SECURITY OFFICIAL JOB DESCRIPTION..... 97

7.06 RISK ANALYSIS RESULTS 99

8. DEFINITIONS..... 100

9. KEY RESOURCES..... 103

9.01 SECURITY RULE..... 104

9.02 OTHER RESOURCES..... 153

A. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)..... 153

B. THE SANS INSTITUTE..... 153

C. ISO 17799:2000..... 153

D. BS 7799-2:2002..... 153

E. FEDERAL INFORMATION SYSTEMS AUDIT MANUAL (FISCAM)..... 153

F. CORPORATE GOVERNANCE TASK FORCE REPORT: A CALL TO ACTION (APRIL 2004)..... 153

G. OCTAVE IMPLEMENTATION GUIDE..... 153

MERCER

Human Resource Consulting

GRIST InDepth: Different strokes for different folks – HIPAA security compliance for various plan designs

*By Tami Simon, Barbara McGeoch, and Judy Bauserman of the Washington Resource Group
October 4, 2004*

In This Article

[Summary](#) | [Background](#) | [Types of HIPAA security obligations](#) | [Decision tree overview](#) | [HIPAA Security Decision Tree](#) | [Fully insured plans](#) | [Self-funded plans](#)

Summary

Employers that sponsor group health plans may have to undertake certain activities on behalf of their plans to comply with the HIPAA security rules. Those activities will differ among employers, depending on the funding and administrative structures of their plans and on whether the plan sponsor transmits or stores electronic protected health information, or e-PHI. In this article summarizing sponsor obligations, we find that in general, those with fully insured plans have fewer obligations than self-funded plans. And plan sponsors that limit the e-PHI they receive and maintain – either by restricting the amount they require or by transmitting and storing the information in non-electronic form – will have fewer obligations. Plans must comply with the security rules by April 21, 2005 – 2006 for small plans – and employers need to find out what they must do and give themselves enough lead time to address any deficiencies.

GRIST is prepared by the Washington Resource Group and the Information Research Center of Mercer Human Resource Consulting. For more information, contact the InfoServices team at 202 263 3950. Copyright © 2004.

WRG only: #20040294

MERCER

Human Resource Consulting

GRIST InDepth: HIPAA electronic security rule compliance for employer group health plans

By Judy Bauserman, Barbara McGeoch, Mark Hamelburg and Tami Simon of the Washington Resource Group

July 24, 2003

In This Article

[Summary](#) | [Overview of the security requirements](#) | [Actions a plan sponsor must take on behalf of its plans](#) | [Security infrastructure](#) | [Business associate requirements](#) | [Securing employer systems](#) | [Next steps](#) | [Appendix A: Group health plan security requirements](#) | [Appendix B: Security standards](#)

Summary

The HIPAA security rules require group health plans to safeguard electronic protected health information (e-PHI). Employers that sponsor group health plans may have to undertake certain compliance activities on behalf of their plans. And some employers may have to bring their own electronic systems into compliance with the rules. Compliance is not required until April 21, 2005 (or 2006 for small plans), but lengthy lead times to budget for and possibly implement technology systems changes mean employers should start compliance efforts now. This article outlines the obligations imposed on group health plans and the responsibility employers have with respect to the plans they sponsor.

GRIST is prepared by the Washington Resource Group and the Information Research Center of Mercer Human Resource Consulting. For more information, contact the InfoServices team at 202 263 3950. Copyright © 2003.

WRG only: #20030192