



THE COMPLETE HIPAA SECURITY POLICIES



IT Security Policy and Procedures Manual

TABLE OF CONTENTS

1	INTRODUCTION.....	1
1.1	GENERAL.....	1
1.2	OBJECTIVE.....	1
1.3	SCOPE.....	2
1.4	APPLICABILITY.....	2
1.5	SPPM ORGANIZATION AND CONTENT.....	2
2	SECURITY ORGANIZATION.....	8
2.1	IT MISSION.....	8
2.2	ROLES AND RESPONSIBILITIES.....	8
2.2.1	<i>Data Owners</i>	8
2.2.2	<i>Director of Information Systems</i>	9
2.2.3	<i>Security Focal Point (SFP)</i>	9
2.2.4	<i>System/Network Administrators</i>	10
2.2.5	<i>Department Managers</i>	10
2.2.6	<i>Supervisors</i>	11
2.2.7	<i>Authorized Users</i>	11
2.2.8	<i>Information Security Management Committee</i>	11
3	POLICIES AND PROCEDURES.....	9
3.1	SUBJECT AREA: LOGICAL SECURITY.....	10
3.1.1	<i>Software Security</i>	11
3.1.1.1	<i>Overview</i>	11
3.1.1.2	<i>Security Software Design</i>	11
3.1.1.3	<i>Software Copyright</i>	11
3.1.1.4	<i>Guidelines on Anti-Virus Process</i>	12
3.1.1.5	<i>Software Development</i>	13
3.1.1.6	<i>Security in the System Development Life Cycle Process</i>	13
3.1.1.7	<i>Probing/Exploiting Security Controls</i>	14
3.1.2	<i>Change Control</i>	15
3.1.2.1	<i>Overview</i>	15
3.1.2.2	<i>Software Changes/Configuration Management</i>	15
3.1.3	<i>Data/Media Security</i>	16
3.1.3.1	<i>Overview</i>	16
3.1.3.1	<i>Formal Mechanism for Processing Records</i>	16
3.1.3.2	<i>Data Classification</i>	16

3.1.3.2.1 Confidential Patient Classification in Meditech	17
3.1.3.3 External Markings	18
3.1.3.4 Printing/Display	18
3.1.3.5 Reproduction	18
3.1.3.6 Storage	18
3.1.3.7 Disposal/Destruction/Re-use	18
3.1.3.8 Shipping and Manual Handling	19
3.1.3.9 Facsimile Transmission	19
3.1.3.10 Data Authentication	20
3.1.3.11 Data Integrity	20
3.1.3.12 Message Authentication	20
3.1.3.13 Electronic Transmission (E-mail, File Transfer Protocol (FTP), etc.)	21
3.1.3.14 Wireless Communication Policy	21
3.1.3.15 Business Associate Contracts and Agreements	21
3.1.4 <i>Telecommunications Security</i>	22
3.1.4.1 Overview	22
3.1.4.2 Telecommunications Changes/Configuration Management	22
3.1.4.3 Dial-Up Controls	22
3.1.4.3.1 Requesting Dial-Up Access Procedure	23
3.1.4.3.2 Virtual Private Network	24
3.1.4.4 Encryption	25
3.1.4.5 Internet (Firewalls)	26
3.1.5 <i>Workstation Security</i>	27
3.1.5.1 Overview	27
3.1.5.2 Mandatory Protection for all Workstations	27
3.1.5.2.1 Protection for Sensitive Workstations	27
3.1.5.2.2 Resident Protection from Malicious Software	27
3.1.5.2.3 Erasure of Restricted/Confidential Information	27
3.1.5.2.4 Workstations Equipped with Modems	28
3.1.5.2.5 Unattended Workstation Processing	28
3.1.5.2.6 Supplemental Encryption	28
3.1.5.2.7 Authorized Applications	28
3.1.6 <i>System Certification and Sever Policy</i>	28
3.2 SUBJECT AREA: MANAGERIAL SECURITY	30
3.2.1 <i>Administrative Security</i>	31
3.2.1.1 Overview	31
3.2.1.2 Access Control and Accountability	31
3.2.1.2.1 Individual Access Authorization	31
3.2.1.2.1.1 Physicians and Physicians' Office Staff Meditech Access	32
3.2.1.2.1.2 Sealed Patient EMR Routine	33
3.2.1.2.2 Individual Access Authorization for Contractors	33
3.2.1.2.3 Individual Access Termination	35
3.2.1.2.4 Individual Accountability	36
3.2.1.2.5 Communication Link Control	36
3.2.1.2.6 Dial-Up Access Control	36
3.2.1.2.7 Individual Access Transfer/Modification	37
3.2.1.3 Userids/Passwords	38
3.2.1.3.1 Password Protection	38
3.2.1.3.2 Password Non-Display	39
3.2.1.3.3 Password Selection Standard	39
3.2.1.3.4 Password Change Policy	39
3.2.1.3.5 Change of Default Passwords	40
3.2.1.3.6 Control of Password Assignment	40
3.2.1.3.7 Password/Userid Lockout	40
3.2.1.3.8 Password History	40
3.2.1.3.9 Minimum Password Age	40
3.2.1.3.10 Concurrent Connections	40
3.2.1.3.11 Emergency Access	40
3.2.1.3.12 Application Development Standards	40
3.2.1.3.13 Use of Passwords and Passphrases for Remote Access	41
3.2.1.3.14 Data Base Password Policy	41
3.2.1.3.15 Computer Password Confidentiality	43

3.2.1.4	Host Environment	45
3.2.1.5	Network Environment	45
3.2.1.5.1	Access to Shared File Storage Areas (Directories)	45
3.2.1.6	Supervisor Capabilities	45
3.2.1.7	Privileges	45
3.2.2	<i>Procedural Security</i>	46
3.2.2.1	Overview	46
3.2.2.2	Separation of Duties	46
3.2.2.3	Individual Accountability	46
3.2.2.4	Output Distribution Controls	46
3.2.2.5	Audit Capabilities	46
3.2.2.5.1	Audit Trails	47
3.2.2.5.2	Investigative Support	48
3.2.2.5.3	Review/Retention Schedule	48
3.2.2.5.4	HIPAA Documentation Retention Schedule	48
3.2.2.6	Security Violations	48
3.2.2.6.1	Reporting Violations	48
3.2.2.6.2	Sanctions for Non-Compliance	48
3.2.2.6.3	Responding to Reports of Security Incidents	52
3.2.2.7	Risk Management	53
3.2.2.7.1	Risk Management Process	53
3.2.2.7.2	Risk Analysis	53
3.2.2.7.3	Security Alerts	54
3.2.2.7.4	Security Testing	55
3.2.2.8	Personnel Security	55
3.2.2.8.1	Employee Termination/Transfer Controls	55
3.2.2.8.2	Agreement	55
3.2.2.9	Data Privacy	55
3.2.2.10	User Verification	56
3.2.3	<i>Internet and Electronic Mail Acceptable Use</i>	57
3.2.3.1	Overview	57
3.2.3.2	Employee Responsibilities	57
3.2.3.3	Department Responsibilities	58
3.2.3.4	Unacceptable Uses	58
3.2.3.5	Forwarded Email	60
3.2.4	<i>Monitoring</i>	60
3.2.5	<i>Requesting an Internet Site be Unblocked</i>	60
3.2.6	<i>Downloading from the Internet</i>	61
3.2.7	<i>Privacy and Confidentiality</i>	61
3.2.8	<i>Posting Information to hospital's Intranet/Internet Home Page</i>	61
3.2.9	<i>Contract or Vendor Electronic Exchange of Data</i>	61
3.2.10	<i>Responsible Use of Information Technology Systems and Applications</i>	61
3.2.11	<i>IS Department Help Desk</i>	62
3.3	SUBJECT AREA: PHYSICAL SECURITY	65
3.3.1	<i>Physical Access Control</i>	66
3.3.1.1	Overview	66
3.3.1.2	Fauquier Hospital Employee Identification Proximity Cards	66
3.3.1.2.1	Procedure to Obtain Employee Identification Proximity Card	66
3.3.1.2.2	Lost Identification Proximity Card	67
3.3.1.3	Contractor Identification Proximity Cards	67
3.3.1.3.1	Procedure to Obtain Contractor Identification Proximity Card	67
3.3.1.3.2	Procedures for Visiting Contractors Accessing Facilities	67
3.3.1.4	Building Access to the Hospital Facility	68
3.3.1.4.1	Employee Access Procedures	68
3.3.1.4.2	Access Procedures for Non-Hospital Employees	68
3.3.1.4.3	Visitors	68
3.3.1.4.4	Access Not Otherwise Covered	68
3.3.1.4.5	Contingency Operations	69
3.3.1.5	Facility Construction (Environmental Controls)	69
3.3.1.5.1	Electrical	69
3.3.1.5.2	Heat	69

3.3.1.5.3 Humidity.....	69
3.3.1.5.4 Water.....	69
3.3.1.5.5 Dirt and Dust.....	69
3.3.1.5.6 Maintenance Documentation.....	70
3.3.1.6 Hardware Security.....	70
3.3.1.6.1 Inventory.....	70
3.3.1.6.2 Rooms and Cabinets to Protect Equipment.....	70
3.3.1.6.3 Workstation and Terminal Control.....	70
3.3.1.6.4 Access Key Control.....	71
3.3.1.6.5 Portable Equipment Control.....	71
3.3.1.6.6 Hardware Changes/Configuration Management.....	71
3.3.1.6.7 Theft Protection.....	71
3.3.1.6.8 Router Security.....	71
3.3.1.7 Facility Security Plan.....	72
3.4 SUBJECT AREA: CONTINGENCY PLANNING.....	73
3.4.1 Backup Procedures.....	74
3.4.1.1 Overview.....	74
3.4.1.2 Data Backup.....	74
3.4.1.3 Alternate Data Backup.....	77
3.4.1.4 Emergency Response/Recovery Procedures.....	77
3.4.1.5 Emergency Mode Operation Plan.....	77
3.4.1.6 Contingency Plan Maintenance and Exercising.....	77
3.4.1.7 Applications and Data Criticality Analysis.....	78
3.4.1.8 Responsibilities.....	78
3.5 SUBJECT AREA: SECURITY AWARENESS PROGRAM.....	79
3.5.1 Security Awareness.....	80
3.5.1.1 Establishing a Security Awareness Program.....	80
3.5.1.2 Initial Security Awareness Training.....	80
3.5.1.3 Periodic Security Awareness Training.....	81
3.5.1.4 Record.....	81
APPENDIX A – INFORMATION SENSITIVITY POLICY AND DATA CLASSIFICATION.....	1
INTEGRITY.....	6
APPENDIX B – ACKNOWLEDGEMENT OF CONFIDENTIALITY FORM.....	1
APPENDIX C – ACKNOWLEDGMENT OF RESPONSIBILITY FOR BUILDING ACCESS FORM.....	1
APPENDIX D – REMOTE ACCESS FORM.....	1
APPENDIX E – VENDOR ACKNOWLEDGEMENT FORM.....	1
APPENDIX F – DEPARTING EMPLOYEE CHECKLIST FORM.....	1
MANAGER/SUPERVISOR SIGNATURE:.....	2
APPENDIX G – GENERAL INCIDENT RESPONSE INSTRUCTIONS.....	1
GENERAL RESPONSE PROCEDURES.....	2
<i>Keep a Log Book.....</i>	2
<i>Inform the Appropriate People.....</i>	3
<i>Release of Information.....</i>	3
RESPONSE TO UNAUTHORIZED PASSWORD DISCLOSURE.....	3
APPENDIX H – HIPAA POLICY MATRIX.....	1
APPENDIX I – SYSTEM CONFIGURATION AND SERVER SECURITY POLICY.....	1
APPENDIX J – PROCEDURES FOR CONFIDENTIAL PATIENT CLASSIFICATION IN MEDITECH.....	1
APPENDIX K – SEALED PATIENT EMR ROUTINE AND PROCEDURES.....	1
APPENDIX L – DATA OWNER’S ACCOUNTABILITY AND RESPONSIBILITY PROCEDURES	

AND RECOMMENDATIONS.....1
APPENDIX M – INFORMATION SYSTEMS DEPARTMENT HELP DESK PROCEDURES.....1
APPENDIX N – WIRELESS COMMUNICATION POLICY1
APPENDIX O – RESPONSIBLE USE OF INFORMATION TECHNOLOGY SYSTEMS AND APPLICATIONS.....1