

**Supplement to the Guidelines for
Academic Medical Centers on Security
and Privacy**

May 2001

Version 1.0

Contents

Introduction.....	3
Purpose.....	4
Sample Contracts and Policies.....	5
Privacy Addendum.....	6
Privacy Breach Flowchart.....	10
Chain Of Trust Agreement.....	11
Appendix A (Authorized Personnel to Access Data)	19
Appendix B (Confidentiality of Patient Information).....	20
Appendix C (Confidentiality Statement)	27
Information Security Policies and Standards.....	29
Responsibilities of Authorized Data Users	47
Responsibilities of Data Managers	51
Responsibilities of Department Directors.....	56
Information Management Policy: Sharing Data with External Entities	59
Information Management Policy	63
Information Management Policy: Need to Know	82
Information Management Policy: Legally Restricted Information.....	85
Job Descriptions.....	86
Information Security Officer.....	87
Chief Security Officer (CSO) (Sample #1).....	91
Chief Information Security Officer (CSO) (Sample #2).....	95
Corporate Privacy Officer.....	97
Information Security Officer.....	98

Introduction

This Supplement to the Guidelines for Academic Medical Centers on Security and Privacy is a collection of useful documents from organizations implementing Security and Privacy practices. The majority of these documents were contributed by participants in the workshop series that produced the Guidelines for Academic Medical Centers on Security and Privacy. Workshop participants reviewed many documents, and those selected for this supplement were deemed useful references for organizations deploying security and privacy compliance programs.

SAMPLE DOCUMENT

Purpose

The purpose of this Supplement to the Guidelines for Academic Medical Centers on Security and Privacy is to provide examples of policies and procedures for organizations deploying operational security and privacy compliance programs. These examples serve as a suggestion of what other organizations have found useful and might prove beneficial to organizations starting with a blank page. In addition, several documents that articulate HIPAA security and privacy issues of the higher education community have been included for reference.

The template format of the guideline document facilitates ease of use and cross-reference to various HIPAA regulations. The decision was made to place these other useful reference materials into a supplement of the Guidelines for Academic Medical Centers on Security and Privacy, instead of interrupting the easy reference template format of the document.

SAMPLE DOCUMENT

Sample Contracts and Policies

The documents included in this Supplement to the Guidelines for Academic Medical Centers on Security and Privacy are not meant to be used as a replacement for good organizational practices and documentation. Organizations are encouraged to consult legal council for determining appropriate format and content for their particular circumstance. Legal statues vary from state to state. This supplement is meant to serve as a starting point as organizations develop documentation and policy appropriate for its particular circumstance.

Privacy Addendum

PRIVACY ADDENDUM

Note: This addendum is provided for illustration only and may not include all of the provisions required for compliance with the Privacy Standards. It may also be necessary to add or modify certain provisions to comply with applicable state law. This addendum is a practice aid and should not be considered legal advice.

1. OBLIGATIONS OF VENDOR

Section 1. **Use of Protected Health Information.** Vendor shall not and shall ensure that its directors, officers, employees contractors and agents, do not use Protected Health Information received from the Covered Entity in any manner that would constitute a violation of the Privacy Standards if used by the Covered Entity, except that Vendor may use Protected Health Information (i) for Vendor's proper management and administrative services, or (ii) to carry out the legal responsibilities of Vendor.

Section 2. **Disclosure of Protected Health Information.** Vendor shall not and shall ensure that its directors, officers, employees, contractors and agents do not disclose Protected Health Information received from the Covered Entity in any manner that would constitute a violation of the Privacy Standards if disclosed by the Covered Entity, except that Vendor may disclose Protected Health Information in a manner permitted pursuant to this Agreement or as required by law. To the extent Vendor discloses Protected Health Information to a third party, Vendor must obtain, prior to making any such disclosure, (a) reasonable assurances from such third party that such Protected Health Information will be held confidential as provided pursuant to this Agreement and only disclosed as required by law or for the purposes for which it was disclosed to such third party, and (b) an agreement from such third party to immediately notify Vendor of any breaches of the confidentiality of the Protected Health Information, to the extent it has obtained knowledge of such breach.

Section 3. **Safeguards Against Misuse of Information.** Vendor agrees that it will implement all appropriate safeguards to prevent the use or disclosure of Protected Health Information other than pursuant to the terms and conditions of this Agreement.

Section 4. **Reporting of Disclosures of Protected Health Information.** Vendor shall, within five (5) days of becoming aware of a disclosure of Protected Health Information in violation of this Agreement by Vendor, its officers, directors, employees, contractors or agents or by a third party to which Vendor disclosed Protected Health Information pursuant to Section 2 of this Addendum, report any such disclosure to the Covered Entity.

Section 5. **Agreements by Third Parties.** Vendor shall enter into an agreement with any agent or subcontractor that will have access to Protected Health Information that is received from, or created or received by Vendor on behalf of the Covered Entity pursuant to which such agent or subcontractor agrees to be bound by the same restrictions, terms and conditions that apply to Vendor pursuant to this Agreement with respect to such Protected Health Information.

SAMPLE DOCUMENT

Section 6. **Access to Information.** Within five (5) days of a request by the Covered Entity for access to Protected Health Information about an individual contained in a Designated Record Set, Vendor shall make available to the Covered Entity such Protected Health Information for so long as such information is maintained in the Designated Record Set. In the event any individual requests access to Protected Health Information directly from Vendor, Vendor shall within two (2) days forward such request to the Covered Entity. Any denials of access to the Protected Health Information requested shall be the responsibility of the Covered Entity.

Section 7. **Availability of Protected Health Information for Amendment.** Within ten (10) days of receipt of a request from the Covered Entity for the amendment of an individual's Protected Health Information or a record regarding an individual contained in a Designated Record Set (for so long as the Protected Health Information is maintained in the Designated Record Set), Vendor shall provide such information to the Covered Entity for amendment and incorporate any such amendments in the Protected Health Information as required by 45 C.F.R. §164.526.

Section 8. **Accounting of Disclosures.** Within ten (10) days of notice by the Covered Entity to Vendor that it has received a request for an accounting of disclosures of Protected Health Information regarding an individual during the six (6) years prior to the date on which the accounting was requested, Vendor shall make available to the Covered Entity such information as is in Vendor's possession and is required for the Covered Entity to make the accounting required by 45 C.F.R. §164.528. At a minimum, Vendor shall provide the Covered Entity with the following information: (i) the date of the disclosure, (ii) the name of the entity or person who received the Protected Health Information, and if known, the address of such entity or person, (iii) a brief description of the Protected Health Information disclosed, and (iv) a brief statement of the purpose of such disclosure which includes an explanation of the basis for such disclosure. In the event the request for an accounting is delivered directly to Vendor, Vendor shall within two (2) days forward such request to the Covered Entity. It shall be the Covered Entity's responsibility to prepare and deliver any such accounting requested. Vendor hereby agrees to implement an appropriate recordkeeping process to enable it to comply with the requirements of this Section.

Section 9. **Availability of Books and Records.** Vendor hereby agrees to make its internal practices, books and records relating to the use and disclosure of Protected Health Information received from, or created or received by Vendor on behalf of, the Covered Entity

Copyright 2001 American Health Lawyers Association, Washington, D.C.

Reprint permission granted.

Further reprint requests should be directed to

American Health Lawyers Association

1025 Connecticut Avenue, N.W., Suite 600

Washington, D.C. 20036

(202) 833-1100

For more information on Health Lawyers content, visit us at www.healthlawyers.org.

These materials were developed by Marilyn Lamar (mlamar@mwe.com) and McDermott, Will & Emery

SAMPLE DOCUMENT

available to the Secretary for purposes of determining the Covered Entity's and Vendor's compliance with the Privacy Standards.

II. DEFINITIONS FOR USE IN THIS ADDENDUM

"Data Aggregation" shall mean, with respect to Protected Health Information created or received by Vendor in its capacity as the business associate of the Covered Entity, the combining of such Protected Health Information by Vendor with the Protected Health Information received by Vendor in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

"Designated Record Set" shall mean a group of records maintained by or for the Covered Entity that is (i) the medical records and billing records about individuals maintained by or for the Covered Entity, (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for the Covered Entity to make decisions about individuals. As used herein the term "Record" means any item, collection, or grouping of information that includes Protected Health Information and is maintained, collected, used, or disseminated by or for the Covered Entity.

"Electronic Media" shall mean the mode of electronic transmissions. It includes the Internet, extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, private networks, and those transmissions that are physically moved from one location to another using magnetic tape, disk, or compact disk media.

"Individually Identifiable Health Information" shall mean information that is a subset of health information, including demographic information collected from an individual, and

(i) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(ii) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) identifies the individual, or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Copyright 2001 American Health Lawyers Association, Washington, D.C.

Reprint permission granted.

Further reprint requests should be directed to

American Health Lawyers Association

1025 Connecticut Avenue, N.W., Suite 600

Washington, D.C. 20036

(202) 833-1100

For more information on Health Lawyers content, visit us at www.healthlawyers.org.

These materials were developed by Marilyn Lamar (mlamar@mwe.com) and McDermott, Will & Emery

SAMPLE DOCUMENT

"Privacy Standards" shall mean the Standard for Privacy of Individually Identifiable Health Information, 45 C.F.R. Parts 160 and 164.

"Protected Health Information" shall mean Individually Identifiable Health Information that is (i) transmitted by electronic media, (ii) maintained in any medium constituting Electronic Media; or (iii) transmitted or maintained in any other form or medium. "Protected Health Information" shall not include (i) education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. §1232g and (ii) records described in 20 U. S.C. §1232g(a)(4)(B)(iv).

"Secretary" shall mean the Secretary of the Department of Health and Human Services.

Copyright 2001 American Health Lawyers Association, Washington, D.C.

Reprint permission granted.

Further reprint requests should be directed to

American Health Lawyers Association

1025 Connecticut Avenue, N.W., Suite 600

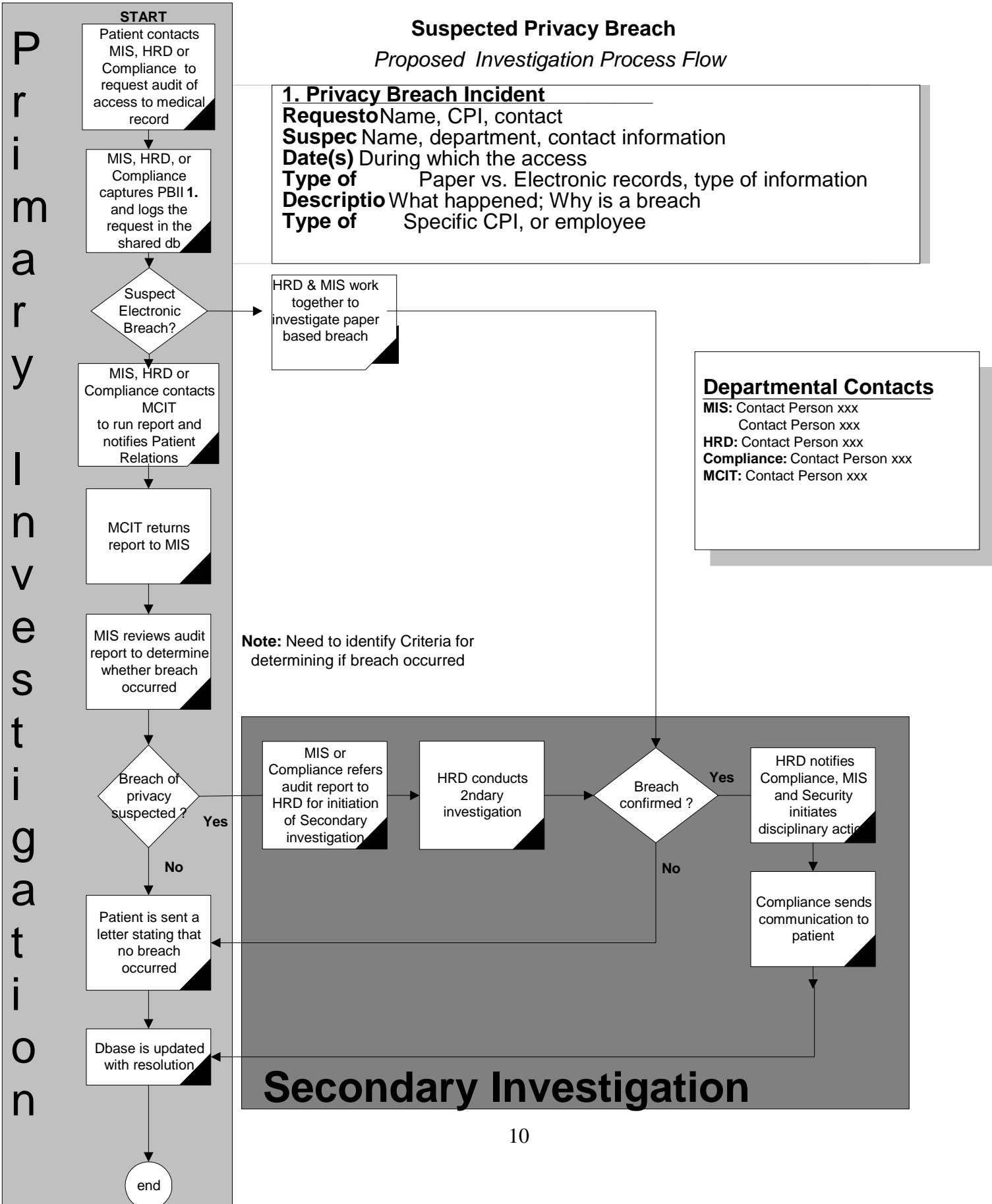
Washington, D.C. 20036

(202) 833-1100

For more information on Health Lawyers content, visit us at www.healthlawyers.org.

These materials were developed by Marilyn Lamar (mlamar@mwe.com) and McDermott, Will & Emery

Privacy Breach Flowchart



SAMPLE DOCUMENT

Chain Of Trust Agreement

CHAIN OF TRUST AGREEMENT FOR TRANSMISSION OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION IN ELECTRONIC FORM

This Agreement, is entered into by and between ORGANIZATION, located at _____, and _____ (PARTNER), located at _____.

WHEREAS, it is of benefit for PARTNER to be able to access individually identifiable health information held by ORGANIZATION,

WHEREAS, ORGANIZATION has an obligation to ensure the confidentiality of individually identifiable health information in its care, and further to ensure that it only makes such data available to parties which have an acceptable need to access such data, and

WHEREAS, PARTNER has a need to access specified individually identifiable health information held by ORGANIZATION,

NOW THEREFORE, in consideration of covenants and conditions set forth in this Agreement, the parties agree as follows:

SECTION I Definitions

- 1.1 AUDIT refers to a formal review and identification of access to an information asset by an individual, organization, or application process.

- 1.2 AUTHENTICATION is the process by which a user (or application process) identifies herself or himself to an information system or resource. The user is required to provide at least one (often a combination) of the following unique elements:
 - 1.2.1 Something that the user knows (such as a password or a personal identification number);
 - 1.2.2 Something that the user has in his/her possession (such as a token or access card);
 - 1.2.3 Something that is a characteristic or an expression of the user's physical being (such as finger or voice prints).

- 1.3 DATA refers to individually identifiable health information, physician information and other proprietary information that has been identified as appropriate for sharing between ORGANIZATION and PARTNER.

SAMPLE DOCUMENT

1.4 ENCRYPTION refers to the reversible conversion of readable information into an unreadable, protected form so that only a recipient who has the appropriate “key” can convert the information back into its original readable form.

1.5 INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION means any information held by ORGANIZATION including elements that allow unique identification of an individual, specifically demographic information such as name, address, social security number, date of birth, sex, etc. Individually identifiable health information includes but is not limited to the following examples if they contain such data elements:

- (a) Patient information generated, collected, maintained, or distributed by ORGANIZATION including transferred (medical) records, and all correspondence;
- (b) Information entrusted by a patients or research subject to an employee, trainee, student, volunteer, vendor, consultant, or member of the faculty or clinical staff;
- (c) Any knowledge a ORGANIZATION employee, trainee, student, volunteer, vendor, consultant, or member of the faculty or clinical staff has regarding a patient;
- (d) Research information collected, generated, maintained, or disseminated by ORGANIZATION which identifies individual or when combined with other data can lead to the identification of an individual;
- (e) Personnel information collected, maintained, or generated by ORGANIZATION that identifies current or past employees other than that information which is made available under Federal or State law, statute, or regulation, or under University policy;
- (f) Academic information collected, maintained, or generated by ORGANIZATION that identifies current or past students.

SECTION II Rights and Duties of ORGANIZATION

2.1 ORGANIZATION agrees to treat security, personnel, and policy information disclosed to it by PARTNER under this Agreement as confidential.

2.2 ORGANIZATION agrees to provide PARTNER with ORGANIZATION policies on confidentiality and data security as well confidentiality statements attesting to the PARTNER’s knowledge of compliance with these policies.

2.3 ORGANIZATION will provide to PARTNER with individually identifiable health information in the form of _____, including but not limited to microfiche, magnetic tape, disk, and by electronic transmission.

SAMPLE DOCUMENT

2.4 ORGANIZATION will determine if PARTNER's security measures are sufficient to protect DATA and recommend changes before releasing DATA.

2.5 ORGANIZATION agrees to designate a point of contact for PARTNER.

SECTION III Rights and Duties of PARTNER

3.1 PARTNER understands that the information it will receive is confidential and PARTNER agrees to maintain and protect the confidentiality of all information it has access to as a result of this Agreement, Section 8.1.

3.2 PARTNER agrees to disclose the security measures it uses to protect the DATA, which must meet applicable professional standards.

3.3 PARTNER agrees to provide the names and job titles of all its personnel who are given access to the DATA, and its disciplinary procedures regarding breaches of computer security and confidentiality, to ORGANIZATION upon request. PARTNER agrees to update Appendix A with every addition or deletion of any staff member to have access to DATA.

3.4 PARTNER agrees to distribute ORGANIZATION Confidentiality and Data Security Policies to employees with access to individually identifiable health information, Appendix B, and require that each employee with access to ORGANIZATION DATA sign confidentiality statements attesting to his/her knowledge and compliance with those policies, Appendix C.

3.5 PARTNER agrees to retain copies of each employee's confidentiality statement attesting to his/her knowledge and compliance with the ORGANIZATION Confidentiality and Data Security Policies and present these statements to ORGANIZATION upon request.

3.6 PARTNER agrees to (_____) information provided by ORGANIZATION to the form of including but not limited to microfiche, magnetic tape, disk, and by electronic transmission.

3.7 PARTNER agrees to report breaches of security to ORGANIZATION as soon as possible in order to minimize damages.

SECTION IV Systems Operations

4.1 Each party, at its own expense and at its own site, shall provide and maintain the equipment, software services and testing services necessary to effectively convert,

SAMPLE DOCUMENT

process or interchange DATA in the form of including but not limited to microfiche, magnetic tape, disk, and by electronic transmission and ensure the integrity of all DATA converted, processed or interchanged.

- 4.2 PARTNER shall allow ORGANIZATION or its designee to review PARTNER's security of external DATA within normal business hours.
- 4.3 PARTNER agrees to designate a point of contact for ORGANIZATION.
- 4.4 PARTNER agrees to receive written permission from ORGANIZATION before outsourcing any work identified in this Agreement to a subcontractor.
- 4.5 PARTNER agrees to ensure that subcontractor will maintain the security and confidentiality provisions of this Agreement.
- 4.6 PARTNER agrees not to copy the individually identifiable health information in any media, except that necessary to complete the process of transferring the DATA in the form of including but not limited to microfiche, magnetic tape, disk, and by electronic transmission.

SECTION V Ownership

- 5.1 ORGANIZATION is the guardian of all DATA rights and information contained within the records shared with PARTNER. Each individual about whom information is shared with PARTNER is the owner of all DATA rights and information that is being shared.
- 5.2 PARTNER covenants not to enter into any agreement allowing any other party to view or extract DATA in any form from all information placed in PARTNER's care, without the written consent of ORGANIZATION.

SECTION VI Compensation

- 6.1 ORGANIZATION agrees to compensate PARTNER in accordance with the terms of the RFP.

SECTION VII Term and Termination

- 7.1 The term of this Agreement shall be for a period of _____, commencing on _____, 1999.
- 7.2 This Agreement may be renewed for an additional year by written notice of renewal signed by both parties.

SAMPLE DOCUMENT

- 7.3 The procedures for termination of this Agreement, for any reason, will be as follows:
- a) PARTNER will return all DATA, regardless of media, to ORGANIZATION.
 - b) PARTNER agrees to destroy any and all copies in any medium, physical or electronic, that were created to transfer the DATA including but not limited to magnetic tape, microfiche and electronic transfer so that none of the individually identifiable health information, physician information and other proprietary information can be retrieved or replicated.
 - c) PARTNER shall make available to ORGANIZATION all services necessary for an orderly transfer of PARTNER's obligations under this Agreement at the time of termination of the Agreement.
- 7.5 This Agreement shall immediately terminate, at the option of ORGANIZATION, if:
- a) Any petition in bankruptcy is filed by or concerning PARTNER. In no event shall this Agreement become an asset in any such proceeding nor shall ORGANIZATION or the University of ORGANIZATION be bound by this Agreement, after any act of bankruptcy by PARTNER. Any delay by the University or ORGANIZATION in the exercise of this right to terminate this provision shall not diminish or waive this right.
 - b) Any breach of confidentiality.

Section VIII Other Important Provisions

- 8.1 Confidentiality. PARTNER understands the, <Name of State> and Federal laws on confidentiality of medical records and other individually identifiable health information and shall ensure that its staff is properly trained in the handling of medical records and other individually identifiable health information under State and Federal law and the ORGANIZATION policies.
- 8.1.1 PARTNER understands that individually identifiable health information may only be released by authorized ORGANIZATION employees, in accordance with the terms of this Agreement.
- 8.1.2 PARTNER shall ensure that the individually identifiable health information that is released to PARTNER will be kept confidential and will not be used by PARTNER or its agents, representatives, or employees in any manner whatsoever other than as agreed.
- 8.1.3 PARTNER shall be responsible for any breach of confidentiality by its agents, representatives, or employees, and shall indemnify the University for all payments, legal fees and costs incurred by such breach.

SAMPLE DOCUMENT

8.1.4 In the event of such a breach, PARTNER will immediately notify ORGANIZATION of the specifics.

8.1.5 PARTNER and its officers, employees and agents understand that confidentiality shall survive the terms of this agreement.

8.2 Security. Each party shall use those security procedures, which are specified, in Section III to ensure that all transmissions of DATA are authorized and to protect ORGANIZATION medical records and DATA from improper access. When information must travel across lines of communication where both ends are not under the control of the Regents of the University of <Name>, PARTNER agrees to use, at a minimum, strong authentication and encryption to protect the DATA.

a) PARTNER will use security/access software and/or procedures sufficient to reasonably ensure that all transmissions of DATA are authorized and to protect the DATA from unauthorized access.

b) PARTNER will safeguard the DATA from tampering and unauthorized disclosures. This protection must extend beyond the initial information obtained from ORGANIZATION to any databases or collections of DATA containing information derived from the DATA. This provision shall be in force even if DATA are made anonymous by removing any identifying information. PARTNER shall maintain the confidentiality of passwords and other codes required for accessing this information.

c) PARTNER may not sell, release, or otherwise furnish such information to any third parties without the written approval of ORGANIZATION.

d) Access is limited to authorized personnel as specified in Appendix A and referenced in Section 3.3.

e) The list of authorized personnel in Appendix A may be amended from time to time with the permission of ORGANIZATION.

8.3 Notices. All payments, notices and formal communications required or permitted under this Agreement shall be made in writing and shall be deemed to be duly given if sent by first class mail, postage prepaid, return receipt requested, addressed as appropriate as follows:

PARTNER: _____ **ORGANIZATION:** _____

8.4 Assignment. In no event shall either party assign any of its rights, powers, duties or obligations under this Agreement without the prior written consent of the other party;

SAMPLE DOCUMENT

provided, however, that ORGANIZATION and PARTNER may assign all or part of this Agreement to its successor, affiliates, and assigns. This Agreement shall be binding upon and inure to the benefit of ORGANIZATION and PARTNER's successors, affiliates, and assigns.

- 8.5 Severability. If any provision of this Agreement is held invalid by a court of competent jurisdiction, such provision shall be deemed modified to eliminate the invalid element, and as so modified, such provision shall be deemed a part of this Agreement. If it is not possible to modify any such provision to eliminate the invalid element, such provision shall be deemed eliminated from this Agreement. The invalidity of any provision of this Agreement shall not affect the force and effect of the remaining provisions.
- 8.6 Governing Law. This Agreement shall be governed by and interpreted in accordance with the laws of the State of ORGANIZATION .
- 8.7 Enforceability. This Agreement shall be enforceable only by the parties hereto and their successors in interest by assignment. No other person shall have the right to enforce any of the provisions contained herein nor is this Agreement intended to create any third-party beneficiary rights.
- 8.8 Amendments. This Agreement may not be revoked, altered, changed, modified, amended or discharged except in writing. No waiver of one or more of the provisions of this Agreement or failure to enforce the Agreement by either of the parties hereto shall be construed as a waiver of any subsequent rights. Only the signatories to this Agreement, or their successors, may revoke, alter, change, modify, amend, or discharge this Agreement.
- 8.9 Prior Agreements, Modifications. This Agreement, together with any attachments, exhibits or appendices, constitutes the entire agreement between the parties regarding its subject matter and shall supersede all prior agreements, promises, negotiations, and representations, oral or otherwise with respect to this subject matter.
- 8.10 Indemnification. PARTNER agrees to indemnify and hold harmless the Regents of the University of <State>, its governing board, from and against any and all claims, costs, losses, damages, liabilities, expenses, demands, and judgments, including litigation expenses and attorney's fees, which may arise from PARTNER'S performance under this Agreement or negligent acts or omissions of its subcontractors, agents, or employees.
- 8.11 Liquidated Damages. PARTNER agrees that ORGANIZATION would be substantially and irretrievably damaged by PARTNER sharing any of the individually identifiable health information, in any form, provided to PARTNER with any other party. PARTNER shall be personally responsible to pay ORGANIZATION the amount of \$50,000.00 in liquidated damages per occurrence should the PARTNER or any of its subcontractors, agents or employees intentionally or accidentally make available any DATA to another party.

SAMPLE DOCUMENT

8.12 Injunction. ORGANIZATION shall be entitled to obtain an injunction against PARTNER in a court of competent jurisdiction should PARTNER share the individually identifiable health information, in any form, provided to PARTNER with any other party. PARTNER shall be responsible for payment of ORGANIZATION legal fees and costs associated with obtaining such injunction.

8.14 Insurance. PARTNER agrees to maintain, at all times relevant to this Agreement, insurance in a form and in limits acceptable to the University. Required are: commercial general liability insurance, including contractual liability, with limits not less than \$2 million per occurrence and \$3 million annual aggregate and errors & omissions insurance with limits not less than \$2 million per occurrence and \$3 million annual aggregate. Evidence of such insurance shall be provided to ORGANIZATION upon request and 30 days prior written notice of a reduction in stated limits or cancellation of stated insurance will be provided to ORGANIZATION.

IN WITNESS WHEREOF, THIS AGREEMENT IS EXECUTED by the parties, by their duly authorized representatives as of _____ day of _____, 1999.

REGENTS OF THE UNIVERSITY

PARTNER NAME:

OF <State>

By: _____

By: _____

Title: _____

Title: _____

SAMPLE DOCUMENT

Appendix A

Authorized Personnel to Access Data

This list may be amended from time to time with the permission of ORGANIZATION.

<u>Name</u>	<u>Position</u>	Date Educated In Laws and <u>ORGANIZATION Policies</u>	Date Confidentiality Statement <u>Signed</u>	Date Access <u>Provided</u>	Date Access <u>Terminated</u>
-------------	-----------------	---	---	--	--

SAMPLE DOCUMENT

Appendix B

UNIVERSITY OF ORGANIZATION HOSPITAL AND HEALTH CENTERS

Confidentiality of Patient Information

ORGANIZATION Policy # _____
Confidentiality of Patient Information

Date of Issue _____ Revised: _____

I. POLICY STATEMENT

It shall be the policy of the University of ORGANIZATION Hospitals and Health Centers that all information regarding care of the individual patient be maintained as confidential information. Patient care information is the property of the patient; ORGANIZATION is the steward or caretaker of that information and the owner of the medium of storage.

II. POLICY PURPOSE

The purpose of this policy is to protect the patient, the clinical team, and the University of ORGANIZATION Hospitals and Health Centers from inappropriate dissemination of information regarding care of individual and collective patients. This policy applies to all clinical staff, employees, vendors, volunteers, students and others who are members of the University of ORGANIZATION Hospitals and Health Centers, and refers to all information resources, whether verbal, printed, or electronic, and whether individually controlled, shared, stand alone or networked. Proper handling of external requests for patient information is addressed in Policy _____. This policy also provides guidelines and examples on employee access to patient identifiable information to ensure confidentiality and integrity of patient information.

III. DEFINITIONS

Aggregate Data: A collection of patient care or clinical information which does not reveal the identity of individual patients.

Central Repository of Patient Information: A physical archive or storage area where one or more of the several components of patient information are permanently maintained.

Clinical Staff: Attending, courtesy, honorary, and visiting physicians, house officers and fellows, special purpose trainee staff members and nurses having practice privileges for the diagnosis and treatment of patients at the University of ORGANIZATION Hospitals and Health Centers.

SAMPLE DOCUMENT

Confidential Information: All of the following are considered confidential:

Patient information collected by the University of ORGANIZATION Hospitals and Health Centers (e.g. transferred medical records, correspondence, telephone calls, etc.); or

Patient information generated by the University of ORGANIZATION Hospitals and Health Centers; or

Information entrusted by the patient to an employee, trainee, student, volunteer or member of the clinical staff; or

Any knowledge the employee, trainee, student, volunteer or clinical staff member has regarding the patient.

Data Steward: Individual or department having access to patient information and having capability of providing for storage or transfer of patient information subject to this policy.

Due Care: That degree of care which other prudent, competent, persons providing patient services would exercise in similar circumstances.

Employee: For the purposes of this policy, any individual providing service to the University of ORGANIZATION Hospitals and Health Centers who receives compensation from the University of ORGANIZATION for that service.

Inappropriate Dissemination: Seeking access to and/or disclosing confidential information, regardless of intent, in verbal, written or electronic form:

To individuals not involved in the care and treatment of that the University of ORGANIZATION Hospitals and Health Centers patient; or

To individuals who are involved with or know the patient but have no need to know the information; or

In a setting where that information could be overheard by individuals who have no need to know (e.g., in elevators, lobbies, waiting rooms, hallways, dining rooms, etc.); or

In a setting where information can be read or transferred from an unattended computer monitor; or

Through sharing another person's electronic password.

Need to Know: Necessary to fulfill the mission or charge of the University of ORGANIZATION Hospitals and Health Centers and its clinical staff, employees, trainees, students, volunteers, or vendors to provide quality patient care, education and research. See Exhibit - "Need to Know" for further discussion and examples of this definition.

SAMPLE DOCUMENT

Patient Information: All information, data and/or knowledge relating to the care of a the University of ORGANIZATION Hospitals and Health Centers patient, including but not limited to:

The medical record, including data recorded on paper, on microfilm, or in a computer data base; or

Pictorial, graphic, or multimedia representations (e.g. photographs, x-ray films ECG tracings, videotape); or

Tissue specimens obtained for histological examination; or

Administrative data, such as the data included in the University of ORGANIZATION Hospitals and Health Centers census system, registration system, clinic scheduling system, laboratory system and the billing system; or

Business or Financial Records.

Trainee: Any individual involved, directly or indirectly, in the provision of patient care, one aspect of which is to further that individual's knowledge. Includes house officers, medical students, nursing students, and other health care professions students. A trainee may or may not receive financial compensation from the University of ORGANIZATION.

Vendor: Any individual or organization that sells or otherwise provides a good or service to the University of ORGANIZATION Hospitals and Health Centers.

Volunteer: Any individual providing a service to the University of ORGANIZATION Hospitals and Health Centers, coordinated through the Director of Volunteers in each corporate area, who receives no financial compensation from the University of ORGANIZATION for that service.

IV. POLICY STANDARDS

A. In order to ensure confidentiality, patient information collected and/or generated within the University of ORGANIZATION Hospitals and Health Centers shall be maintained in such a manner that access to it is restricted to those with a need to know, and release of it is restricted to those with a legal right to know, as mandated by State and Federal laws.

B. It shall be the responsibility of management in each department to determine what information its members need access to in order to complete their job functions. Viewing or obtaining information not needed for job completion, regardless of the medium of storage, constitutes disclosure of that information. It shall be the responsibility of department management to monitor and discipline members in all matters of information security.

SAMPLE DOCUMENT

- C. It shall be the responsibility of management staff in each department to inform their employees of this policy, and to develop and maintain, if appropriate, data confidentiality policies specific to their department which are consistent with this policy. To assure knowledge of these policies, it shall be the responsibility of the department supervisors to assure that current policies are addressed at departmental staff meetings periodically. In addition, these policies shall be referred to and addressed in each orientation program and shall be included in any orientation "information packet" provided for new employees, trainees, volunteers, vendors, and clinical staff.
- D. It shall be the responsibility of respective data stewards to maintain secure access to their electronic data and to provide such information in response to questions regarding potential breach of confidentiality. To the extent technologically possible, audit trails shall be maintained of access to both aggregate and patient-identifiable electronic data.
- E. It shall be the responsibility of respective data stewards to maintain a list of all people granted access to electronic databases under their stewardship. Access shall not be granted to employees who do not have an up-to-date, signed confidentiality statement on file (see Appendix C).
- F. In order to help ensure that only those employees with a need to know patient identifiable information are granted access to such information, data stewards will, on an annual basis, review who has access to patient identifiable information in central repositories of patient information under their purview.
- G. Hard copy printouts of aggregate and patient-identifiable electronic data will be stored in a secure area and maintained in a confidential manner as is currently required of paper medical records.
- H. Every clinical staff member, employee, trainee, student, vendor, and volunteer at the University of ORGANIZATION Hospitals and Health Centers shall be responsible for maintaining confidentiality of all information entrusted to them.
- I. Every employee is expected to exercise due care in any discussion or use of patient information.
- J. Confidentiality statements attesting that the employee is aware of and understands the confidentiality policy, shall be signed at the beginning of employment and shall be reviewed and signed and/or documented annually by all employees and clinical staff of the University of ORGANIZATION Hospitals and Health Centers who have access to patient identifiable information.
- K. The University of ORGANIZATION Hospitals and Health Centers characterizes as unethical and unacceptable any activity through which an individual:

SAMPLE DOCUMENT

1. Voluntarily allows or participates in inappropriate dissemination of confidential patient information; or
2. Interferes with the intended use of the information resources; or
3. Without authorization, destroys, alters, dismantles, disfigures, prevents rightful access to or otherwise interferes with the integrity of patient information and/or information resources; or
4. Without authorization invades the privacy of individuals or entities that are creators, authors, users, or subjects of the information resources.

L. Infractions of this confidentiality policy shall be subject to the disciplinary action of the University of ORGANIZATION Hospitals and Health Centers, up to and including dismissal and/or loss of privileges. Invasion of another person's right to privacy can have legal consequences in addition to disciplinary action from the University of ORGANIZATION Hospitals and Health Centers.

M. Requests for access to patient identifiable data needed for research purposes must be accompanied by IRB approval.

N. Communication regarding confidentiality policies and monitoring of these policies for medical staff shall be channeled through the Clinical Affairs Office.

V. PROCEDURE ACTIONS

None

VI. NEED TO KNOW

Definition: Necessary to fulfill the mission or charge of the University of ORGANIZATION Hospitals and Health Centers and its clinical staff, employees, trainees, students, volunteers or vendors to provide quality patient care, education and research.

Following are examples where employees have a need to know patient identifiable information to complete their assigned job functions, as well as examples where employees do not have a need to know such information. These lists are intended to be examples only, and are not intended to be complete representations of situations where employees have a need to know patient identifiable information. Per the University of ORGANIZATION Hospitals and Health Centers policy, specific access to patient identifiable information is under the discretion of departmental management.

Examples of appropriate uses of patient identifiable information where employees have a need to know:

SAMPLE DOCUMENT

Rendering care to specific patients.

Billing and collecting for services rendered to specific patients.

Financial analysis to assess the business impact of patient care, including but not limited to analysis of specific cases to assess impact of clinical practice redesign or in response to research requests, and analysis of situations where it is necessary to join records from more than one system (for example, Vendor1 and Vendor2) together in order to analyze the full impact of that care.

Performing reimbursement analysis on specific patients.

Provision of educational materials for patients, given at the direction of their treating physician.

Fund raising activities done at the request of a physician who has knowledge of the patient's or family's desire to donate to the University.

Examples of inappropriate use of patient identifiable information:

Mass mailing fund raising solicitations to patients with specific medical conditions, without the express approval of the Dean of the Medical School.

Informing others that employees, relatives, famous people, etc. are patients in the hospital.

Use of personal medical information in making employment decisions.

Use of employee's personal medical information to see if the employee was really out sick, had a doctor's appointment, had a worker's compensation injury, etc.

Employee access to or request for patient information of a relative or another University of ORGANIZATION Hospitals and Health Centers employee, unless:

The request or access is made on behalf of an inpatient unit or an outpatient clinic and the information is needed to provide patient care during a verified clinic appointment or inpatient hospitalization;

The request or access is made for the purpose of carrying out medical research and the need for the patient information is verified as consonant with the goals of that research;

The request or access is made by Financial Services for billing and collection purposes.

VII. REFERENCES

SAMPLE DOCUMENT

SAMPLE DOCUMENT

Appendix C

UNIVERSITY OF ORGANIZATION HEALTH SYSTEM

Confidentiality Statement

In consideration of the University of ORGANIZATION Health System (ORGANIZATION) agreeing to provide certain confidential information to _____ Company and its employees, _____ Company and each employee provided with confidential information agree to abide by the terms of this statement.

- A. Patient care information, whether in written, unwritten, or electronic computer system form, may be accessed only by ORGANIZATION employees or contracted personnel who need that information to perform their job or contractual responsibilities. Patient care information may only be released to individuals outside the health system by authorized ORGANIZATION employees.
- B. I understand that this information belongs to the patient and I am only the caretaker and must guard the information appropriately. This includes, but is not limited to, keeping patient information secure, private, and out of public viewing, protecting computerized data by logging off when leaving a work station, and keeping information secure by not discussing patient-specific issues in public areas such as elevators, etc.
- C. Contracted personnel may only access data necessary to perform their contracted responsibilities. Contracted personnel agree not to disclose, communicate, or use any patient care information in any manner whatsoever other than in the provision of contracted services and, even within the scope of those services, must limit dissemination to those who have signed confidentiality agreements and have a need to know.
- D. Contracted personnel agree not to copy or download this confidential information. If for some reason confidential information must be copied, the contracted personnel must obtain permission from ORGANIZATION employee and must return such information to ORGANIZATION immediately after completion of that particular activity.
- E. The confidentiality of this information survives the termination of your contracted personnel status.
- F. I understand that if I do not keep patient information confidential, or if I allow or participate in the inappropriate dissemination of or access to patient care information, my employer will be sanctioned \$50,000 per infraction and criminal offenses will be reported to the appropriate authorities.

(Note: often the vendors would like to remove F)

SAMPLE DOCUMENT

G. Contracted personnel agrees to comply with all state and federal laws applicable to the use of this confidential patient information.

My signature attests to the fact that I have read, understand and agree to abide by the terms of this statement and the University of ORGANIZATION Health System's policies on confidentiality of patient care information (policy # 03-07-015).

Name: _____ Contracting company: _____

Signature: _____

Date: _____

Information Security Policies and Standards

I. Information security

Information vital to the entity will be protected from unauthorized access, modification, disclosure or destruction. An information security program will exist to protect the interests of our patients and of the entity.

II. Security administration

A group will exist to develop and maintain an information security program for the entity. This group will oversee standards, promote awareness, and monitor the program to validate its effectiveness.

A. Standard: applicability and exceptions

Each practice site may add to, but not detract from, these policies and standards. Any exceptions to these standards must be requested in writing and submitted to the Information Security Subcommittee.

B. Standards: Roles

1. The information security officer is responsible for implementing and monitoring a consistent data security program. The Information Security Subcommittee will monitor this responsibility. The information security officer will:

- Coordinate the development and maintenance of information security policy and standards
- Coordinate information security activities with Security, Internal Audit Services, Information Services and Treasury Services
- Monitor security activities and oversee the application of specified security standards
- Assist data stewards in assessing their data for classification and advise them of available controls
- Implement an information security awareness program
- Provide consulting services for information security throughout the entity

2. The steward is responsible for a particular set of information and for implementing information security policy and standards. The steward will:

- Assume responsibility for information
- Recommend appropriate business use of information
- Authorize information access and assign administrative responsibility
- Communicate control and protection requirements to administrators and users
- Monitor compliance and periodically review requirements for information protection

SAMPLE DOCUMENT

- Review security violations and follow reporting procedures
3. The system administrator is responsible for operation and maintenance of information processing services. The administrator implements information security policy and standards, and will:
 - Administer steward-specified business and information protection controls
 - Administer access control
 - Provide backup and recovery of information
 - Detect and respond to violations and weaknesses
 - Monitor compliance with information security standards
 4. The Information Security Subcommittee is comprised of members from the group practices and acts as a council for information security for all entity subdivisions.
 5. Internal Audit proactively reviews systems and services for compliance with information security standards, other internal standards and the requirements of external regulatory bodies.

C. Standard: information assessment

Stewards will assess risks and threats to information under their purview and accordingly classify their information as *public*, *internal*, or *confidential*. Recommendations for handling information are outlined in the table below:

Information Classification

	Public	Internal	Confidential
Label	None	None	Mark "Confidential"
Access	No controls	No controls	Discretionary
Storage	No controls	Store out of sight of non-ORGANIZATION persons	Lock up
Communication	No controls	No controls	Confidential envelope; Secure transmission
Destruction	No controls	No controls	Shred paper Overwrite media

D. Standard: training and awareness

Each site will assign responsibility for information security awareness and training.

Guidelines:

1. Human Resources will describe data security to all new employees.
2. Awareness programs will provide instruction on good security practices.

SAMPLE DOCUMENT

3. The ORGANIZATION will support specific technical and management training for system administrators and users as needed.

E. Standard: violations

Any deviation from the information security policies and standards is a violation. Everyone must report instances of noncompliance. Violations will be reviewed for appropriate disciplinary action in accordance with Human Resources policy and procedures. Corrective action may include termination of employment or criminal prosecution.

Guidelines:

1. The information security officer, Human Resources and an appropriate level of department management will review standards violations and recommend corrective or disciplinary action.
2. Users should report security violations to a supervisor, system administrator, data steward, the Security Section, the information security officer or Internal Audit Services, as appropriate.

F. Standards: computer crime

1. Computer crimes violate state and federal law. They include but are not limited to: unauthorized disclosure, modification or destruction of data, programs, or hardware; denial of computer services; theft of computer services; illegal copying of software; invasion of privacy; theft of hardware, software, peripherals, data, or printouts; misuse of communication networks; promulgation of malicious software such as viruses; and breach of contract. Perpetrators may be prosecuted under state or federal law, held civilly liable for their actions, or both.
2. The entity must comply with license agreements for copyrighted software and documentation.
3. Licensed software must not be reverse engineered or copied unless the license agreement specifically provides for it.
4. Copyrighted software must not be loaded or used on systems for which it is not licensed. This includes employee-owned home computers and other personal digital devices used for the business.

G. Standard: exceptions to standards

All exceptions to these standards are to be requested in writing and approved by the Information Security Subcommittee.

H. Standards: ORGANIZATION systems administered by contractors

1. Contracts for system and/or application management must include security, confidentiality and non-disclosure clauses. These clauses must specify adherence to the *Information Security Policies and Standards*. The XXX's information security officer or designee will assess the contractor's security posture. This assessment may include a site visit.

SAMPLE DOCUMENT

2. Oversight of contractor operations is the responsibility of entity staff. On-site information stewards and system administrators must be identified to oversee administrative duties performed by non-entity personnel and compliance with security policies and standards. The entity system administrator must have a working knowledge of the system or application and possess a level of administrative privilege equal or higher than that of the contractor. The must carefully consider several administrative aspects and ensure that checks and balances are in place to control and monitor contractor activities:
 - A. Secure authentication of contractors is required. This may include multiple levels of authentication such as at a remote access server or firewall *and* at host levels. Authentication may involve secure tokens, username/password combinations, and public/private key combinations. Device-to-device or firewall-to-firewall authentication is acceptable provided contractor demonstrates individual accountability for access to the ORGANIZATION systems and applications. This may be verified on-site at the contractor's place of business.
 - B. Authorization of contractors is required. The entity must limit contractor access to systems, services and information on a discretionary basis. Contractor user accounts must not allow more system or network privileges than necessary to meet contract requirements.
 - C. Logging and auditing system accesses and activity is required. The entity's administrators and contractors are jointly responsible for auditing system access and activity and will routinely examine the logs for adherence to standards and authorized activities. Contractors cannot have the ability to delete or alter system log files. System audit logs should be retained for at least 6 months.
3. Operating systems employed must provide a reasonable level of integrity. Use of newer operating system versions or the application of patches to fix known bugs and vulnerabilities is highly recommended. Information Security provides a vulnerability scanning service, which can identify operating system security weaknesses and other areas of concern.
4. System or application access by contractor personnel must be closely controlled. The access method must not provide functionality beyond that which is required for contract performance.
5. Secure communications with contractors who provide service from remote locations is necessary to preclude technical compromise of information and systems. The entity's technical staff will work with contractors to employ standard, secure methods whenever possible.

SAMPLE DOCUMENT

III. Standards for information use

Standards will be established for ethical use of information to protect the interests of the patients and to prevent misuse of information vital to the entity.

A. Standard: misuse of resources

Any action or misuse of information that harms the resources of the institution or adversely affects other individuals is prohibited.

Guideline: Use of the entity network, computers, Internet link, dial-in services and information resources is primarily for the entity's business-related activity or for personal professional development. Limited personal use is acceptable but discretion is necessary to ensure that individuals do not degrade the entity's public image through their activities, adversely affect the availability of network resources, or disrespect the rights of others.

B. Standard: authorized usage

Users must not attempt to gain physical or logical access to info or systems for which they are not authorized.

C. Standard: connection to the network

Users must not connect unauthorized devices to the entity network.

Guideline: Networks will evaluate requests to attach devices to the network.

D. Standard: medical information

Users must hold confidential all medical information. [Reference local policy that addresses access to medical information.]

IV. Information access control

Physical and electronic access to sensitive information and computing resources is controlled. The level of control will depend on user need and the level of risk and exposure to loss or compromise. Electronic access is controlled through identification and authentication. Users are responsible and accountable for access under their personal identifiers.

A. Standards: access to computing facilities and equipment

1. The level of physical access control for any area that contains *confidential* information is determined by the level of risk and exposure.

Guidelines:

1. Access control lists should be maintained to include ongoing review and update.
2. An administrative determination of trustworthiness should be made prior to allowing individual access to sensitive areas. This normally includes reference and records checks.

SAMPLE DOCUMENT

3. Maintenance personnel should be escorted and supervised by knowledgeable persons.
 4. System administrators should provide initial and ongoing security awareness training for those assigned to sensitive areas.
 5. The Information Security Subcommittee or its delegate will review and approve the placement of, and physical access to, devices located in any authorized off-campus sites.
2. Highly sensitive areas, such as data centers, server areas and communications facilities will have separate control systems to limit access. [Reference local standards regarding lock location and installation.]
3. Security precautions for personal computers, software, documentation and diskettes will be determined by the risk of loss or damage. Available precautions include equipment enclosures, lockable power switches, equipment identification and fasteners to secure the equipment.

Guidelines:

1. The senior manager of the area will specify the physical access controls based on information security and lock placement standards.
2. Persons granted access to areas or information are responsible for their actions. Additionally, they are responsible for the actions of others that are, in turn, allowed access.

B. Standard: media and hardcopy protection and transportation

Electronic media and hardcopy that contains *confidential* information must have access controls during transportation and disposal.

Guidelines

1. Printed versions (hardcopy) of *confidential* information should not be copied indiscriminately or left unattended and open to compromise.
2. Media containing *confidential* information should be placed in confidential envelopes and hand-carried by employees, transported by General Service couriers or sent through an approved outside carrier. These outside carriers may include, but are not limited to, the U.S. Postal Service, Federal Express and the United Parcel Service.
3. *Restricted* media in transit on campus may be transported by employees in any containers deemed appropriate. Reasonable care should be used and media should be secured when left unattended.
4. Magnetic media containing *internal* or *confidential* information that is released from the entity should first be processed to purge any information residing on that media.
5. Degaussing and overwriting are acceptable methods of purging information from magnetic media.
6. Responsible personnel should authorize the shipping and receiving of magnetic media and maintain appropriate records.
7. *Confidential* information in hardcopy format should be disposed of properly. This may include shredding finely enough to ensure that the information is unrecoverable.

SAMPLE DOCUMENT

C. Standards: information access controls

1. Access to the network and the Internet will be controlled. Each user will be uniquely identified, and an accepted process will authenticate identity. Processes for verification may include unique tokens, card keys, biometric readers, or individual passwords. Passwords and tokens are the individual's responsibility and will not be shared.

Guidelines

1. All network access should be controlled through individual identification and authentication.
 2. Each user should have a unique identification code.
 3. Each user's identity should be authenticated through an acceptable verification process. Acceptable processes include individual passwords, unique tokens such as cards with magnetic stripes, or biometrics.
 4. Passwords are the individual's responsibility and users should not share them.
 5. Users should be able to select and change their own passwords.
 6. Passwords should be changed at least every ninety days. Permanent passwords are discouraged.
 7. Passwords should be at least six characters long and not easily guessed or found in a dictionary. Use of numeric digits and non-alphanumeric characters in passwords is encouraged for protection of *confidential* information.
 8. Users should not write down passwords, store them on hard copy or store them locally on workstations and laptop computers.
2. System administrators must periodically review user privileges and remove or inactivate accounts when access is no longer required.

Guideline: Stewards and system administrators should determine the necessity of changing locks and recovering card keys, tokens and other access control devices when users terminate employment or when work assignments change.

3. System administrators must implement discretionary access controls. Each user may have access to all systems, services and information necessary to accomplish assigned tasks.
4. System administrators must implement inactivity time-outs, where technically feasible, for terminals and workstations that access *confidential* information.

Guideline: Implementation procedures are developed at the local and business unit levels. Stewards should specify time-out intervals based on business needs and amount of risk and exposure.

5. System Administrators must be able to audit access and access attempts to *confidential* information. Audits will be conducted when unauthorized accesses and attempts are identified. Audit records shall be kept at least six months, and administrators shall periodically review the audit records for evidence of violations or system misuse.

SAMPLE DOCUMENT

D. Standards: generic access to data

1. Generic access to information stored in databases is allowed only for non-interactive tasks. A non-interactive task is one that is scheduled to run automatically or one that is triggered by a series of events. A user does not directly initiate the task, nor is a user the direct recipient of the information.
2. Requests for generic access to information stored in databases are made to the database administrators. If the request meets standards, the database administrator will establish an account. If the request is not within the scope of the standards, the requestor may ask the Information Security Subcommittee for a variance. The subcommittee will render a decision and notify both the requestor and the database administrator.
3. Generic accounts and passwords are, in general, subject to standards and guidelines that pertain to individual user accounts. One exception is password expiration. Generic account passwords will expire every 180 days and application administrators will be notified of the expiration and will be prompted to change it. Application administrators will have 7 calendar days to comply prior to revocation of access. There will be no exceptions to the expiration requirement.
4. Generic account passwords must be protected from unauthorized disclosure. Hard coded passwords that reside on the client machine or in an application must be afforded reasonable protection commensurate with risk and available platform or application security features.
5. Information access via generic accounts must be limited to the maximum practical extent and functionality must be limited to the specific task required.

V. Communication security

Information transmitted outside the organization requires protection. Methods employed will depend upon information sensitivity, technical risks and threats, external regulations and available communication security controls.

A. Standard: internal transmission

Technical security features for systems and services vary. Stewards, system administrators and developers must consider these variances when they transmit *confidential* information internally from one system or service to another.

SAMPLE DOCUMENT

B. Standards: release of information that individually identifies patients

1. Information that identifies individual patients will not be released to any outside organization or individual except for patient care, legal, or reimbursement purposes.

Guideline: Patient-identifying information includes names, addresses, clinic numbers, Social Security numbers and any other information that uniquely identifies individuals. The fact that information released does not specifically identify individuals *as* patients is immaterial.

2. Release of information for patient care will occur only in accordance with each site's medical information access policy and the *Information Security Policies and Standards*.

Guideline: *Release* is the physical movement or electronic transmission of information outside the physical boundaries of the entity or the institutional network and supporting infrastructure that connects entity subdivisions.

3. The policies and standards cited in the *Information Security Policies and Standards* booklet will apply to all entity subdivisions.

4. Exceptions to information release standards must be consistent with state and federal laws and regulations and approved by the Information Security Subcommittee, Information Infrastructure Policy Committee and the Executive Committee.

Guideline: Project proposals and draft contracts for service must accurately identify the sources and flow of information, how it is stored and used, and detail security controls. Only endorsed standards exceptions are forwarded for consideration.

E. Standards: external transmission and access

1. The steward and appropriate policy setting groups make the business decisions regarding appropriateness of external transmission and access. Each group practice will provide guidance to system administrators concerning the provision of these services. Risk and countermeasure information is available from the Information Security Officer.

Guideline: Stewards must understand the risks of transmitting *confidential* information via the public switched telephone system and should employ technical security services, such as encryption, where feasible.

2. The Information Security Subcommittee or its delegate will review and approve technical security mechanisms and services for remote access and external transmission.

SAMPLE DOCUMENT

Guidelines:

1. Dial-up access should occur through a technical security service such as Remote Authentication Dial-In User Service (RADIUS).
2. If a secure, institutionally supported service is not used, an employee must enable and disable the modem and supervise its use. Modems should not be left unattended in answer mode.

D. Standards: electronic mail

1. The entity owns the electronic mail service, and considers electronic mail private, direct communication between sender and recipient. However, employees cannot expect absolute confidentiality. The contents will not be monitored, observed, viewed, displayed or reproduced in any form by anyone other than the sender or recipient unless specifically authorized by an officer of the entity, a law enforcement representative or the Information Security Officer.
2. Electronic mail is considered official correspondence of the entity, and users must avoid the inclusion of inappropriate or derogatory language in their messages. Electronic mail is maintained in computer systems and on backup media for varying lengths of time and may be recovered subsequent to deletion. The messages may be disclosed in the same manner as paper records. Reasons for recovery of electronic mail messages may include legal discovery, external investigations by law enforcement personnel and internal security investigations.
3. Work-related mail is forwarded to the most appropriate employee in the case of employment termination or when an employee is absent for an extended period of time. A recipient may designate another employee to receive and read work-related mail for business reasons. Personal messages are forwarded to the intended recipient. If that is not possible, they are destroyed. Messages are not examined further than is necessary to determine the category into which they fall.

E. Standards: e-mail host security

1. Hosts that run e-mail routing applications must support and employ security functions such as authentication and logging at the system and e-mail application administrative levels.

Guideline: Most single user PC-based operating systems, such as Windows 95, do not provide acceptable security functionality. E-mail hosts must run on operating systems capable of identification, authentication and other security functions such as logging and discretionary access controls. Examples of such operating systems are Windows NT, Unix and VMS. Administrators must employ these security features to prevent and detect unauthorized access to system and application administrative accounts.

SAMPLE DOCUMENT

2. Administrators must actively manage e-mail hosts to minimize security risk.

Guidelines: Operating system security vulnerabilities exist and are well documented. Tools exist to assist administrators evaluate risk and correct vulnerabilities. Information sources, such as the National Security Agency's Computer Emergency Response Team (CERT), publish threat information and prescribe technical courses of action to neutralize those threats. The persons, groups or departments that own and operate systems are ultimately responsible for security. System administrators will actively monitor authoritative security sources, perform risk assessments and employ available countermeasures as risks and threats are identified. Specific security guidance includes:

- Hosts should preferably run the most current version of e-mail routing applications. Minimally, the routing software used must incorporate applicable security patches.
- E-mail gateways/mailers must not automatically execute attachments or message bodies, such as those found in Multipurpose Internet Mail Extensions (MIME), ActiveX, SML or Java.
- Administrators of E-mail routers that perform some non-MIME auto-execute functions such as "vacation," must configure their systems to automatically invoke programs deemed secure and/or required for the business function of the system.

3. E-mail hosts and e-mail users must be Internet "good neighbors."

Guidelines: Administrators who configure e-mail hosts as relay hosts must take measures to detect and prevent delivery of unsolicited broadcast E-mail, or "spam," by watching for messages coming to their machines from non-entity sites that are destined for other non-entity sites. Spammers sometimes attempt to hide their tracks by bouncing e-mail off intermediate sites to obscure the source.

Senders of e-mail may not hide or disguise the origin of their messages for illicit or illegal purposes. Forging or altering e-mail messages to impersonate other individuals or entities is forbidden. Violators are subject to corrective action.

4. No employee may automatically forward mail outside of the entity.

Guidelines: For security reasons, it is inappropriate for users to indiscriminately route all incoming email from entity-designated email account to an account outside the intranet, without specific permission from the Information Security Subcommittee. Only under exceptional circumstances will such permission be granted. Terminated employees, with supervisory approval, may have all email routed from their internal email in-box to an Internet email account for up to six (6) months as a courtesy.

SAMPLE DOCUMENT

F. Standards: Internet

1. Use of the Internet via the network must be primarily for business or professional development. Limited personal use is acceptable but discretion is necessary to ensure that individuals do not degrade the entity's public image through their activities or adversely affect the availability of network resources. Use of the Internet via the network for personal business is not permitted. [Cross-references: 1. local Human Resources policy on computer and Internet use; 2. policy on web usage and content filtering]

Guideline: Internet access should be limited to those with business need.

2. All access and communication to or from the Internet must occur through an actively managed Internet firewall service.

3. Internet services available via the internal network will be limited to those required for business or professional development.

4. Access via Internet to the internal network must be approved by the Information Security Officer or designate. External organizations must have contractual agreements with the entity that address information security, confidentiality and nondisclosure. Access methods must employ strong authentication and encryption. Access must be limited to the minimum systems and services required, and activity must be logged.

5. Internet access by non-entity persons (i.e. patients and guests) via network services is not allowed. Non-networked systems with dialup service to commercial Internet service providers is the preferred method of providing Internet access to non-entity persons.

VI. Information integrity controls

Vital information must remain consistent, complete and accurate. Serious errors and unauthorized or inappropriate duplications, omissions and intentional alterations will be investigated.

A. Standard: separation of duties and functions

Where feasible, responsibilities of application programmer, system programmer, system administrator and database administrator must not overlap.

B. Standard: application software

Only tested and controlled software should be installed on networked systems. Use of unevaluated and untested software outside an application development environment is prohibited.

C. Standard: change controls

Change control management must exist for software development.

SAMPLE DOCUMENT

Guideline: Revision procedures should be designed to minimize the likelihood of information loss or corruption.

D. Standards: anti-virus controls

1. All systems connected to the network will have virus protection.

Guideline: Controls may include real-time or periodic scans. System Administrators are responsible for oversight and implementation of these procedures. A consistent approach will be employed across the entity.

2. Information Services will maintain and update a list of approved software for virus protection.

3. Where technically feasible, users will employ approved anti-virus software.

Guideline: An entity-wide educational and technical approach will exist to raise user awareness of virus hazards in the computing environment and to detect and purge viruses.

4. Where necessary, the entity will provide and help maintain anti-virus software on networked personal systems.

Guidelines:

1. To the extent practical, users are responsible for the integrity of their personally owned devices used for remote access.
2. Users will employ adequate anti-virus software that is updated regularly via central security control, as practical, or via manual download.
3. The entity should provide anti-virus software protection, where necessary, for personally owned systems used for remote access.

VII. Preventive measures, backup and recovery

Processes are necessary to prevent loss of vital information, to provide backup and recovery, and provide continuous operation consistent with the business needs of the entity.

A. Standard: prevention

Frequent testing of preventive methods as they apply to fire, utility services and other environmental hazards must occur.

SAMPLE DOCUMENT

Guideline: Combustibles should not be stored in data centers, network hub rooms, network points of presence, or other areas critical to the computing base.

B. Standard: backup

All information must have sufficient backup and be recoverable.

Guidelines:

1. Multiple levels of backup and storage should be used for critical information.
2. Backup should provide for the loss of multiple cycles.
3. Users of personal computers and other personal digital devices are responsible for backup and recovery of locally stored information.
4. Files and programs should be properly labeled and indexed to facilitate recovery.
5. Alternate fire zone storage facilities should be used for media containing vital data that, if lost or destroyed, would be difficult to recreate.
6. Alternate fire zone storage facilities should be used for files containing patient care programs, program changes, or data that could be used to reconstruct essential systems in the event of a disaster.
7. Backup and recovery procedures should be tested.

C. Standard: emergency mode of operation

Alternate modes of operation, that may include manual methods, must exist to ensure continuity of critical services in the event a natural disaster, fire, or act of vandalism or terrorism occur.

D. Standards: disaster recovery planning

1. All data centers and computerized systems critical to the ORGANIZATION must have written and operationally tested disaster recovery plans.
2. Information stewards will prioritize the recovery of applications and associated databases to ensure critical services are recoverable in a timely fashion.

Guidelines:

1. Information processing management will maintain teams to execute recovery procedures for data centers, systems, networks and databases.
2. The disaster plan should include procedures to facilitate an immediate, planned response to emergency situations.
3. All areas of data processing are required to maintain recovery documentation consisting of a system recovery overview, systems chart and job-level recovery documentation.
4. Recovery procedures should address computers, peripheral equipment, environmental systems, supplies and anything else essential to the data processing operation.
5. Stewards, system administrators and users should all be involved in disaster recovery planning.
6. Specific personnel should be assigned recovery tasks. Each person should have an alternate. Recovery plans must allow alternate personnel to access the necessary instructions and procedures to accomplish recovery tasks.

SAMPLE DOCUMENT

7. Testing of recovery plans should be an ongoing activity. All activity during a test must be recorded and reviewed for the purpose of improving the plans. Tests should include alternate site processing where applicable.

Corrective Action

Purpose

This policy sets forth a set of guidelines for the Corrective Action process to be followed when an employee has performance, attendance or behavior problems that interfere with work, patient care or operations of the entity.

Policy

Corrective Action should be used to correct inappropriate behavior. Supervisors are responsible for accurate and timely documentation of inappropriate behaviors or performance issues.

Corrective Action should be used consistently.

Supervisors should identify and inform employees of:

- What is expected behavior and the performance standards of their job
- When they are not meeting these expectations
- What must be done to correct the inappropriate behavior and an improvement plan with a time line for its accomplishment
- Consequences if improvement does not occur

The corrective action process is meant to assist employees in recognizing the seriousness of their behavior and encouraging their commitment to changing these behaviors. In many situations, informal counseling may be utilized by the supervisor to resolve issues prior to the formal corrective action process.

An informal counseling is used by management as a reminder to employees of policies and practices. Supervisors can utilize informal counseling to explain the performance expectations of the job to the employee who is not meeting the performance standards or job requirements. Notes of an informal counseling should be retained by the supervisor and may be referenced at a later time. Supervisors may choose to have the employee acknowledge the informal counseling session in writing by initialing the note.

Supervisors must complete a corrective action form after each formal step of the process. Employees will be asked to sign this form indicating that they have had an opportunity to review it. If an employee elects not to sign, this should be noted on the form. Employees should be given a copy. The Corrective Action Conference form is sent to Human Resources, where it will be placed in the employee's file. If the documentation regarding discipline is not related to Equal Employment Opportunity legislation, including Sexual Harassment, it will be removed two years after the date of the incident, unless a related offense is repeated during this time.

In some cases, an immediate suspension pending an investigation is appropriate. There may be situations where an employee may be terminated without progressing through the steps outlined

SAMPLE DOCUMENT

in this policy. Some steps can be repeated or omitted if the facts of the situation warrant it. Human Resources may be contacted as a resource for any issues that arise.

Procedure

Informal Counseling Session

This step should be used before proceeding to the following formal documentation stages.

Step 1 - Supervisor's Conference (may coordinate with Human Resources)

This step serves as a reminder to the employee as to the behavior that is expected of them. The goal of the meeting is to ensure that there is both understanding and commitment by the employee to correct the inappropriate behavior.

Step 2 - Written Warning (encouraged to coordinate with Human Resources)

During this meeting, the supervisor should stress the seriousness of this action and what is expected behavior. The employee should be informed that should similar behavior reoccur, he/she will face additional disciplinary action up to and including termination of employment from the Clinic.

Step 3 - Suspension Without Pay (required to coordinate with Human Resources)

As with all previous steps, the problem should be identified along with an indication of what is the expected behavior. (Be sure that this is clear to the employee.)

Any previous incidents of similar nature resulting in discipline should be reviewed along with the conclusions reached at those meetings. The employee must realize that a suspension without pay normally is a "last chance" and that future incidents of a similar or related nature will likely result in termination of employment from the entity.

Step 4 - Termination (required to coordinate with Human Resources)

Termination of employment by its very nature is the most severe form of discipline that can be imposed. The facts surrounding the rule infraction or unacceptable behavior must be investigated before a termination proceeding is finalized.

Process to Appeal Corrective Action

Employees who wish to appeal disciplinary action, may use the appeals procedure. For more information, contact the Employee Service Center.

Guidelines for Corrective Action

The following are meant to give assistance to supervisors in assessing the seriousness of an offense, provide consistency, and establish the appropriate discipline.

These are not work rules. They are guidelines only.

To ensure the fair interpretation of the following guidelines, supervisors should review each situation for the following:

- Is the "rule" necessary for the orderly, effective, and safe operation of the entity?

SAMPLE DOCUMENT

- Was the employee informed of the "rule" or work expectation; did he/she understand the expectation?
- Has the "rule" been applied equally? Each case is unique; therefore, equally does not mean rigid enforcement of "rules". Consider the specifics of each incident (i.e., theft of a 5-cent item would not necessarily be a Group III offense although "theft" is listed under Group III).

Group I

The following behaviors are usually subjected to all four steps of the Corrective Action process beginning with the supervisor's conference. Repeated offenses may be followed by a documented written warning, suspension and ultimately termination:

1. Reporting to work in improper attire or failure to maintain a clean, neat appearance
2. Loitering, neglecting work or loafing during working hours
3. Interference with work of other employees
4. Horseplay or disorderly conduct
5. Disregard for safety rules or safety practices
6. Careless operation and/or use of property which results in its damage
7. Creating or contributing to unsanitary conditions
8. Unauthorized posting, removal or defacing of notices, signs or writing in any form on any Clinic bulletin boards
9. Distribution of literature and/or solicitation of employees, patients and the public on company time, unless prior permission is received from Administration
10. Stopping work before specified stopping time
11. Being out of the department or assigned working areas during working hours without permission of a supervisor, except for the use of the rest rooms
12. Rude or discourteous behavior
13. Excessive tardiness
14. Excessive absences from work
15. Not meeting work and/or job performance standards
16. Smoking on company property and/or chewing tobacco (refer to Smoking/Tobacco Products policy)
17. Unauthorized use and/or misuse of the telephone
18. Unauthorized overtime

Group II

These offenses may begin with a written warning. Repeated offenses or more serious incidents may result in suspension or termination:

1. Accepting gratuities or tips from patients, their relatives, visitors or vendors
2. Sleeping or appearing to be asleep while on duty
3. Threatening, intimidating or coercing patients, fellow employees, or visitors on premises at anytime for any reason
4. Harassment of employees, visitors, or patients based on equal employment opportunity protected categories
5. Use of obscene or abusive language or gestures
6. Deliberate falsification of timekeeping record or other data related to work assignments

SAMPLE DOCUMENT

Group III

Incidents in Group III are very severe infractions of company policies and may result in a suspension or termination.

1. Refusal to carry out instructions of supervisory personnel pertaining to work
2. Deliberate slowdown in regards to work
3. Deliberate refusal to complete work shift without approval of immediate supervisor
4. Immoral or indecent conduct on company property
5. Possession of marijuana, alcoholic beverage, and/or illegal drugs on company property
6. Reporting for work with the odor of alcohol on one's breath, or appearing to be under the influence of alcoholic beverages, marijuana, or any drug that impairs judgment or work performance
7. Willfully falsifying application for employment or other data requested by company
8. Defacing or intentional destruction in any manner of company property, the property of fellow employees, patients, or visitors
9. Theft of company, other employees', patients' or visitors' property
10. Fighting, agitating a fight, or attempting bodily harm or injury to anyone on company property
11. Bringing a firearm or dangerous weapon onto company property
12. Breach of ethics concerning confidentiality of employee or patient information

SAMPLE DOCUMENT

Responsibilities of Authorized Data Users

University of ORGANIZATION Health System Role and Responsibilities of Authorized Data Users

I. POLICY STATEMENT

It shall be the policy of the University of ORGANIZATION Health System to capture, share, secure, maintain, and enhance the value of ORGANIZATION health information assets in all mediums through appropriate information management policies and actions that meet applicable Federal, State, regulatory, or contractual requirements and support the ORGANIZATION mission, vision, and values. Furthermore it shall be the policy of ORGANIZATION to support and adhere to the rights and responsibilities of patients as specified in the State of ORGANIZATION Public Health and Mental Health Codes.

This policy applies to all clinical staff, employees, vendors, volunteers, students, and others as appropriate (including external data users granted direct access to ORGANIZATION health information resources through an Information Sharing Agreement). Every ORGANIZATION Authorized Data User has a responsibility, as they perform their job activities, to ensure that ORGANIZATION data assets are protected.

II. POLICY PURPOSE

The purpose of this policy is to inform Data Users of their specific role and responsibilities regarding ORGANIZATION data security.

III. DEFINITIONS

SAMPLE DOCUMENT

NOTE: Definitions of terms used in this policy are found in ORGANIZATION Policy #####, "Information Management Policy" and should be downloaded for use with this policy.

IV. STANDARDS

- A. All persons with access to ORGANIZATION health information assets may only have such access on a need to know basis and must be approved and verified as Authorized Data Users at regular intervals (but no less than annually) by his or her department's Departmental Director (or Delegated Access Coordinator).
- B. An Authorized Data User who finds that he or she has retained or been inadvertently granted additional access beyond that appropriate to his or her current role should report this to his or her current Departmental Director (or Delegated Access Coordinator).
- C. It is the responsibility of every Authorized Data User to maintain confidentiality of ORGANIZATION health information assets even if technical security mechanisms fail or are absent. A lack of security measures to protect the confidentiality of information does not imply that such information is public.
- D. All Authorized Data Users shall be formally charged with the responsibility and obligation to:
 - 1. seek access to data only through the Authorization and Access Control process
 - 2. access only that data which they have a need to know
 - 3. disseminate data to others only when appropriate
 - 4. protect the confidentiality and integrity of ORGANIZATION health information assets
- E. Internal Authorized Data Users shall have this responsibility and obligation specified through their supervisor as part of the conditions of their ORGANIZATION employment.

SAMPLE DOCUMENT

- F. External Authorized Data Users shall have this responsibility and obligation specified through Information Sharing Agreement(s) with the ORGANIZATION .
- G. ORGANIZATION supervisors shall verify that potential Authorized Data Users have attested to ORGANIZATION Policy ##### “ORGANIZATION Information/Computer Security Management” and ORGANIZATION Policy ##### “Confidentiality of Patient Information” and that potential Authorized Data Users have received appropriate education and training before access to ORGANIZATION information is granted.
- H. Authorized Data Users should be aware that records of data access by users are, where technologically practical, a capability of all ORGANIZATION health information assets subject to this policy and that, from time to time or as indicated by events and circumstances, such access audits may be conducted.
- I. If an Authorized Data User elects to place individually identifiable health information onto personally-owned media or storage devices (e.g. PDAs, floppy disks, case logs, note cards), he or she is responsible for ensuring that its security, confidentiality, and integrity are maintained according to this policy, and he/she is individually responsible for any breaches that occur as a result of his/her actions.
- J. Authorized Data Users who access data for which they do not have a need to know or data outside that granted by the AAC process may lose their access privileges.
- K. Authorized Data Users who commit breaches of confidentiality under this policy are also subject to appropriate disciplinary action up to and including discharge or termination of contract/relationship.
- L. Each clinical staff member, employee, trainee, student, vendor, volunteer, or contractor, or other affiliate of the ORGANIZATION with access to ORGANIZATION health information

SAMPLE DOCUMENT

is subject to and has the responsibilities outlined in this policy as well as those outlined in their organization's policy on confidentiality of information (e.g. UMHHC policy #03-07-015 “Confidentiality of Patient Information.”) For external entities, this is covered by the Information Sharing Agreement, see ORGANIZATION Policy XX-XX-XXXX "Sharing ORGANIZATION Data with External Entities."

M. Authorized Data Users should be aware that in order to protect the individually identifiable health information entrusted to ORGANIZATION , all directed communication/ solicitations must adhere to ORGANIZATION Policy #XX-XX-XXX “Directed Communication/Solicitations” .

V. EXHIBITS -

1. Need to Know
2. Legally Restricted Information

VI. REFERENCES

1. ORGANIZATION Policy # ### “Information Management Policy”
2. ORGANIZATION Policy # ### “Role and Responsibilities of ORGANIZATION Data Managers”
3. ORGANIZATION Policy # ### “Confidentiality of Patient Information”
4. ORGANIZATION Policy # ### “Directed Communication/Solicitations”

AUTHOR: ORGANIZATION Information Security Committee

Responsibilities of Data Managers

**University of ORGANIZATION Health System
Role and Responsibilities of ORGANIZATION
Data Managers**

I. POLICY STATEMENT

It shall be the policy of the University of ORGANIZATION Health System (ORGANIZATION) to capture, share, secure, maintain, and enhance the value of ORGANIZATION health information assets in all mediums through appropriate information management policies and actions that meet applicable Federal, State, regulatory, or contractual requirements and support the ORGANIZATION mission, vision, and values. Furthermore it shall be the policy of ORGANIZATION to support and adhere to the rights and responsibilities of patients as specified in the State of ORGANIZATION Public Health and Mental Health Codes.

As custodians of individually identifiable health data, ORGANIZATION Data Managers have a vital role to play in protecting ORGANIZATION data assets.

II. POLICY PURPOSE

The purpose of this policy is to inform ORGANIZATION Data Managers of their specific role and responsibilities regarding the handling of ORGANIZATION data assets.

III. DEFINITIONS

NOTE: Definitions of terms used in this policy are found in ORGANIZATION Policy XX-XX-XXXX 1, "Information Management Policy" and should be downloaded for use with this policy.

SAMPLE DOCUMENT

IV. STANDARDS

- A. Data Managers for each ORGANIZATION health information asset are appointed by the Data Steward (or Business Owner), or as specified in Standard B.
- B. If any ORGANIZATION staff member chooses to maintain a database containing individually identifiable health information generated in the course of performing professional responsibilities, he/she will be responsible as Data Manager for that database and must follow all applicable rules.
- C. The Data Manager is accountable for ensuring that any and all applicable ORGANIZATION policies are fully executed for the data asset(s) for which he or she is responsible.
- D. Data Managers must register all ORGANIZATION health information assets containing individually identifiable health information in any medium for which they are responsible in the Authorized Access Database.
- E. Individuals have the right to correct inaccurate individually identifiable health information. The appropriate process for validating and processing such corrections is determined individually by each organization, and specified in that organization's policies (see, e.g., Medical Information Services Policy ###, "Medical Record Amendment;" policy _____). Each Data Manager is responsible for ensuring that validated correction requests relevant to ORGANIZATION data assets under his/her control are implemented.
- F. Data Managers asked to make their data available for solicitation purposes should be aware that in order to protect the individually identifiable health information entrusted to ORGANIZATION , all directed communication/solicitations shall adhere to ORGANIZATION Policy #XX-XX-XXX "Directed Communication/Solicitations" (under development).

SAMPLE DOCUMENT

- G. Data Managers and Data Administrators may go to the ORGANIZATION Information Security Committee (security oversight entity) for assistance with interpretation of existing policy, cataloging of information assets and individually identifiable health information, monitoring and tracking violations and appeals, identifying areas of risk, and defining security controls. The ISC shall evaluate and certify that appropriate security systems and measures are implemented.
- H. Data Managers are the custodians, not the owners, of the data for which they are responsible. Individually identifiable health information is the property of the individual to whom the information pertains and the ORGANIZATION is the steward of that information and the owner of the storage medium.
- I. The Data Manager for a ORGANIZATION health information asset is responsible for working with Department Directors (or their Delegated Access Coordinators) to provide their departmental staff with appropriate levels of access to the data according to the staff's need to know. In the event of a dispute, the ISC will resolve appeals.
- J. Data Managers shall ensure that System Administrators under their supervision maintain ongoing internal audit processes (to the extent technologically practical) which record system activity such as log-ins, file accesses, and security incidents. To the extent technologically practical, for systems containing individually identifiable health information, an audit trail must be implemented so that a list can be obtained of users who have accessed an individual's records or of records accessed by a specific user.
- K. If the Data Manager is responsible for individually identifiable health information that is subject to additional specific legal restrictions, that information shall also be subject to the additional safeguards and processes as specified in Exhibit 2, "Legally Restricted

SAMPLE DOCUMENT

Information,” and the Data Manager is responsible for ensuring that those measures are in effect.

- L. Data Managers shall not permit external data users to access ORGANIZATION data assets unless the external users have completed an Information Sharing Agreement with ORGANIZATION , as described in ORGANIZATION Policy xxx, "Sharing ORGANIZATION Data with External Entities."
- M. Data Managers should be aware that there may be cases in which a state, federal, or regulatory agency requires that access be granted to it under law or regulation. In such cases, to the extent possible, an Information Sharing Agreement meeting the criteria listed in ORGANIZATION Policy xxx, "Sharing ORGANIZATION Data with External Entities," shall be negotiated between ORGANIZATION and the agency before access is granted to the ORGANIZATION data assets.
- N. To the extent that a Data Manager is also a Data User, or otherwise comes into contact with individually identifiable health information, he or she has the additional responsibilities outlined in ORGANIZATION Policy xxx, "Role and Responsibilities of Authorized Data Users".

V. EXHIBITS -

- 1. Need to Know
- 2. Legally Restricted Information

VI. REFERENCES

- 1. ORGANIZATION Policy # ### “Information Management Policy”

SAMPLE DOCUMENT

2. ORGANIZATION Policy # ### “Role and Responsibilities of Authorized Data Users”
3. ORGANIZATION Policy ##### “Sharing ORGANIZATION Data with External Entities”
4. ORGANIZATION Policy #XX-XX-XXX “Directed Communication/Solicitations”

AUTHOR: ORGANIZATION Information Security Committee

SAMPLE DOCUMENT

Responsibilities of Department Directors

University of ORGANIZATION Health System ### Information Access: Responsibilities of Department Directors or Delegated Access Coordinators

I. POLICY STATEMENT

It shall be the policy of the University of ORGANIZATION Health System (ORGANIZATION) to capture, share, secure, maintain, and enhance the value of ORGANIZATION health information assets in all mediums through appropriate information management policies and actions that meet applicable Federal, State, regulatory, or contractual requirements and support the ORGANIZATION mission, vision, and values. Furthermore it shall be the policy of ORGANIZATION to support and adhere to the rights and responsibilities of patients as specified in the State of ORGANIZATION Public Health and Mental Health Codes.

As the link between departmental users and the Authorization and Authentication Process, Departmental Directors (or their Delegated Access Coordinators) have a vital role to play in ensuring that information gets to those who have a need to know, while remaining protected from those who do not.

II. POLICY PURPOSE

The purpose of this policy is to inform Departmental Directors (or their Delegated Access Coordinators) of their specific role and responsibilities regarding ORGANIZATION data security.

III. DEFINITIONS

SAMPLE DOCUMENT

NOTE: Definitions of terms used in this policy are found in ORGANIZATION Policy ###, "Information Management Policy" and should be downloaded for use with this policy.

IV. STANDARDS

- A. Department Directors may, if they choose, appoint a Delegated Access Coordinator to execute their responsibilities under this policy. Delegated Access Coordinators for external entities are specified by the appropriate Information Sharing Agreement.
- B. Departmental Directors (or their Delegated Access Coordinators) are responsible for defining, in consultation with the appropriate Data Managers, departmental access profiles for members of their department/unit by listing roles within the department and the appropriate level of access for individuals in those roles based on their need to know. In the event of a dispute, the ISC will resolve appeals.
- C. All persons with access to ORGANIZATION health information assets may only have such access on a need to know basis and must be approved and verified as Authorized Data Users at regular intervals (but no less than annually) by the appropriate Departmental Directors (or Delegated Access Coordinator).
- D. The Departmental Director (or Delegated Access Coordinator) for a department shall be responsible for communicating changes in job status to the manager of the Authorized Access Database in a timely fashion so it is updated to reflect changes in that department's Authorized Data Users' job status and need to know. (See ORGANIZATION Policy ####, "Assignment and Retrieval of ORGANIZATION Information Technology Access and ORGANIZATION Property.")

SAMPLE DOCUMENT

- E. To the extent that an Departmental Directors (or Delegated Access Coordinator) is also a Data User, he or she has the additional responsibilities outlined in ORGANIZATION Policy ###, "Role and Responsibilities of Authorized Data Users".

V. EXHIBITS -

1. Need to Know

VI. REFERENCES

1. ORGANIZATION Policy ##### "Information Management Policy"
2. ORGANIZATION Policy #####, "Assignment and Retrieval of ORGANIZATION Information Technology Access and ORGANIZATION Property"
3. ORGANIZATION Policy ##### "Role and Responsibilities of Authorized Data Users"

AUTHOR: ORGANIZATION Information Security Committee

SAMPLE DOCUMENT

Information Management Policy: Sharing Data with External Entities

University of ORGANIZATION Health System ##### Sharing ORGANIZATION Data with External Entities

I. POLICY STATEMENT

It shall be the policy of the University of ORGANIZATION Health System (ORGANIZATION) to capture, share, secure, maintain, and enhance the value of ORGANIZATION health information assets in all mediums through appropriate information management policies and actions that meet applicable Federal, State, regulatory, or contractual requirements and support the ORGANIZATION mission, vision, and values. Furthermore it shall be the policy of ORGANIZATION to support and adhere to the rights and responsibilities of patients as specified in the State of ORGANIZATION Public Health and Mental Health Codes.

It is the responsibility of the ORGANIZATION to ensure that these principles and policies are upheld even when individually identifiable health information in the custody of ORGANIZATION needs to be shared with other entities. Sharing of data shall be done by requiring potential data sharing partners to execute an information sharing agreement which obliges them to handle the data in a manner consistent with ORGANIZATION policies and procedures.

II. POLICY PURPOSE

The purpose of this policy is to inform ORGANIZATION personnel of the procedures that must be followed if individually identifiable health information is to be shared with an external entity.

SAMPLE DOCUMENT

III. DEFINITIONS

NOTE: Definitions of terms used in this policy are found in ORGANIZATION Policy ####, "Information Management Policy" and should be downloaded for use with this policy.

IV. STANDARDS

A. External data users must not be permitted to access ORGANIZATION data assets unless the external users have completed an Information Sharing Agreement with ORGANIZATION that establishes at least the following:

1. Identification of the external party's Delegated Access Coordinator(s) and a representative from ORGANIZATION to communicate with them regarding the data sharing, and the procedures that will be used to authenticate and authorize external data users.
2. The external entity's intended use(s) of the data.
3. The method used to identify which individuals' information will be shared.
4. The method the external users will use to access the data.
5. The scope of access that will be permitted.
6. Descriptions of audit reports that will be required, including
 - a. what they will cover
 - b. who is responsible for generating them
 - c. how often they are to be generated (biannually at a minimum, or as necessary)
7. The procedures that will be used for reporting and responding to security breaches, including the external entity's responsibility to report security breaches

SAMPLE DOCUMENT

affecting the shared data to ORGANIZATION and what steps the external entity will take to enforce its policies.

8. Demonstration that the potential Authorized External Data User will maintain the data with security at a level compliant with HIPAA and any applicable professional standards.

If any external personnel are to be granted accounts on ORGANIZATION health information resources (e.g., via Electronic Health Record accounts), the agreement *must* also include:

9. A provision specifying that any and all external personnel granted accounts on ORGANIZATION health information resources are subject to the ORGANIZATION Confidentiality and Data Security Policies and requiring that they individually sign statements attesting to their knowledge of and compliance with those policies.

The agreement *may*, if appropriate, also include the following elements:

10. Access by the ORGANIZATION unit or its designee on a regular basis to audit the security of the external data user.
11. Fees, if any, and assignment of responsibility for costs incurred in sharing the data.
12. Damages for breaches of the agreement.
13. Indemnification between the parties.

- B. There may be cases in which a state, federal, or regulatory agency requires that access be granted to it under law or regulation. In such cases, to the extent possible, an Information Sharing Agreement meeting the criteria above shall be negotiated between

SAMPLE DOCUMENT

ORGANIZATION and the agency before access is granted to the ORGANIZATION data assets.

- C. All Information Sharing Agreements must be approved by the Office of the Vice President and General Counsel — Health System.

V. EXHIBITS -

VI. REFERENCES

1. ORGANIZATION Policy ##### “Information Management Policy”

AUTHOR: ORGANIZATION Information Security Committee

SAMPLE DOCUMENT

Information Management Policy

University of ORGANIZATION Health System #### Information Management Policy

I. POLICY STATEMENT

It shall be the policy of the University of ORGANIZATION Health System (ORGANIZATION) to capture, share, secure, maintain, and enhance the value of ORGANIZATION health information assets in all mediums through appropriate information management policies and actions that meet applicable Federal, State, regulatory, or contractual requirements and support the ORGANIZATION mission, vision, and values. Furthermore it shall be the policy of ORGANIZATION to support and adhere to the rights and responsibilities of patients as specified in the State of ORGANIZATION Public Health and Mental Health Codes.

II. POLICY PURPOSE

The purpose of this policy is to identify and disseminate the ORGANIZATION framework and principles for information management that guide our institutional actions and operations in protecting, generating, and sharing individually identifiable health information in support of the ORGANIZATION mission, vision, and values.

III. DEFINITIONS

Access - The ability of a data user or application process to read, write, modify, or communicate information or otherwise make use of an information asset.

SAMPLE DOCUMENT

Access Profile - A list of the applications and/or databases a user (or application process) is permitted to access, and the access levels granted in each of those applications and/or databases.

Account Administration - The process by which authorized data users are assigned accounts (sign-ons) to ORGANIZATION health information assets using the access controls (profiles) prepared by Data Managers.

Account Administrator - The individual acting at the direction of the Data Manager who implements controls on access to information assets by applying formal guidelines and practices to functions such as assigning user access codes, revoking user access privileges, and setting file protection parameters. (The roles of account and system administrator may be combined for smaller databases.)

Audit - A formal review and identification of access to an information asset by an individual, organization, or application process.

Authentication - The process by which a user (or application process) identifies her or himself to an information system or resource. The user is required to provide at least one (often a combination) of the following unique elements:

1. Something that the user knows (such as a password or a personal identification number);
2. Something that the user has in her possession (such as a token or access card);
3. Something that is a characteristic or an expression of the user's physical being (such as finger or voice prints).

SAMPLE DOCUMENT

Authorization - Documented approval to access ORGANIZATION health information assets based on the user's need to know.

Authorization and Access Control (AAC) Process - The process in which Departmental Directors request access for members of their department based on those members' roles and their role-based need to know, and Data Managers ensure that the needed access to applications is made available.

Authorized Access Database (AAD) - The centralized repository of information about all ORGANIZATION Authorized Data Users, under the responsibility of one administrator. The Authorized Access Database must include at a minimum:

1. User name and a unique identifier
2. User login ID
3. Date access last changed, and start and stop date for authorized use of an account and/or application
4. User's Departmental Director or Delegated Access Coordinator
5. Application ID for each application
6. User's authorized access profile for each application

Authorized Data User (ADU) - Individuals who have been granted authorization through the Authorization and Access Process to access specific ORGANIZATION health information assets in the performance of their assigned duties or in fulfillment of their role in the

SAMPLE DOCUMENT

ORGANIZATION community. Authorized Data Users include, but are not limited to, faculty and staff members, employees, trainees, students, vendors, volunteers, contractors, and other affiliates of the ORGANIZATION as well as external users who have been granted accounts on ORGANIZATION health information assets under the terms of an information sharing agreement. For detailed information, see ORGANIZATION Policy ####, "Role and Responsibilities of Authorized Data Users."

Business Owner - The senior ORGANIZATION official (and his/her staff) having policy-level responsibility for managing a segment of the ORGANIZATION information assets by the Data Steward, e.g. Departmental Chairs, Directors of Units. (The Business Owner has the role of Delegated Data Steward, as described in University of ORGANIZATION, Data Administration Guidelines for Institutional Data Resources.

Certification - Evaluation of the computer system(s), storage media, network(s), information transmissions, operating systems, and applications design supporting the ORGANIZATION health information assets which confirms that the appropriate security measures have been implemented in accordance with ORGANIZATION policies.

Consent - the voluntary agreement of an informed and competent individual or their legal guardian for a given action relative to the individual (including the release of information). See individual entity policies..

SAMPLE DOCUMENT

Contingency Plan - a routinely updated plan for responding to an emergency. At a minimum, it must include a data backup and disaster recovery plan.

Data Manager - ORGANIZATION Official and their staff who have been given operational-level responsibility for the capture, maintenance, and dissemination of specific data by the appropriate Data Steward or Business Owner (Delegated Data Steward). For detailed information, see ORGANIZATION Policy #####, "Role and Responsibilities of ORGANIZATION Data Managers."

Data Steward - the ORGANIZATION Executive Officer having policy-level responsibility for managing a segment of the ORGANIZATION information resource as designated by the Regental by-laws. For the University of ORGANIZATION Health System, the official data steward is the Executive Vice President for Medical Affairs.

Delegated Access Coordinator - An individual within a department or external entity designated by the Department Director (or Information Sharing Agreement, in the case of external entities) to:

1. Define, in consultation with the appropriate Data Managers, departmental access profiles for members of their department/unit by listing roles within the department and the appropriate level of access for individuals in those roles based on their need to know.
2. Notify the AAD Administrator when personnel status changes require access changes (e.g. hiring, termination, suspension, transfer).

SAMPLE DOCUMENT

For detailed information, see ORGANIZATION Policy #####, "Information Access: Responsibilities of Department Directors or Delegated Access Coordinators."

Directed Communication/Solicitations - the use of individually identifiable health information to promote fund raising, educational opportunities, special research or clinical activities, new forms of treatment, or notification of ORGANIZATION events. Contact with a patient to discuss or provide information related to the above activities is not considered directed communication/solicitations if the inquiry is initiated by the patient. See ORGANIZATION Policy #XX-XX-XXX "Directed Communication/Solicitations".

Disclosure - The release of information to third parties about an individual which requires the individual's consent or release due to a legal or regulatory requirement.

Encryption - The reversible conversion of readable information into an unreadable protected form so that only a recipient who has the appropriate "key" can convert the information back into its original readable form.

Health Information Asset - Any individually identifiable health information, in any form, on any medium.

Health Insurance Portability and Accountability Act (HIPAA) - Federal statute requiring, among other things, the adoption of standards for the security and privacy of individually identifiable health information.

SAMPLE DOCUMENT

Individually Identifiable Health Information - any information, including demographic and/or scheduling information collected about an individual, that-

- a. Is created or received by a health care provider, health plan, employer, or health care clearinghouse or any employee of the above; and
- b. Relates to the past, present or future physical and/or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and
 - (i) Identifies the individual, or
 - (ii) With respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

All of the following are considered by ORGANIZATION to fall into this category:

- Patient information collected by the University of ORGANIZATION Hospitals and Health Centers and Medical School or member information collected (e.g. transferred medical records, correspondence, telephone calls, e-mail, etc.); **or**
- Patient information generated by the University of ORGANIZATION Hospitals and Health Centers and Medical School or member information generated; **or**
- Information entrusted by the individual to a clinical staff member, employee, vendor, volunteer, student or other affiliate of ORGANIZATION; **or**
- Any knowledge a clinical staff member, employee, vendor, volunteer, student or other affiliate of ORGANIZATION gains in the course of fulfillment of his or her appointed role in the ORGANIZATION regarding the individual; **or**

SAMPLE DOCUMENT

- Research information collected, generated, maintained or disseminated by the ORGANIZATION that identifies individuals, or when combined with other data can reasonably lead to the identification of individuals.

Information asset - any data in any form on any media.

Information Security Committee (security oversight entity) - that ORGANIZATION entity documented as formally assigned the responsibility for defining procedures to assure the security, integrity, and confidentiality of ORGANIZATION health information assets. This responsibility includes but is not limited to the oversight of:

- the use of security measures to protect data.
- the conduct of personnel in relation to the protection of data.
- the coordination of the AAC process and procedures with other operational entities necessary to provide for the security, integrity, and confidentiality of ORGANIZATION health information assets.

Membership of the ISC shall, at a minimum, include representatives from Medical Information Services, ORGANIZATION Legal Office, Finance, the Medical Center Human Resources Department, the Office of Clinical Affairs, the Institutional Review Board, the Compliance Committee, the ORGANIZATION Medical School, the House Officers' Association, and relevant information technology organizations.

Information Sharing Agreement - (Also known as, and referred to in HIPAA as, a "Chain of Trust Agreement.") A contract entered into by two parties in which they agree to exchange data

SAMPLE DOCUMENT

while maintaining its security and confidentiality. Part of administrative procedures to guard data integrity, confidentiality and availability. For a description of the factors that must be present in an information sharing agreement between ORGANIZATION and any external entity seeking access to ORGANIZATION health information assets, see ORGANIZATION Policy ####, "Sharing ORGANIZATION Data with External Entities."

Legally Restricted Information - individually identifiable health information for which disclosure is specifically subject to additional legal requirements imposed by statute or administrative rule.

Need to know - The principle that states that a user should access only the specific information necessary to complete his or her assigned job functions.

This principle is applied in two main contexts:

1. Departmental Directors (or their Delegated Access Coordinators) apply this principle in determining the appropriate level of access to databases and/or applications needed by people in different roles in their department (see ORGANIZATION Policy ####, "Information Access: Responsibilities of Department Directors or Delegated Access Coordinators").
2. Authorized Data Users apply the principle every time they decide whether to access a specific individual's record or not, even if they have been granted full access to the application in which the record resides (see ORGANIZATION Policy ####, "Role and Responsibilities of Authorized Data Users"). Once access to a database and/or application has been authorized, the authorized data user is still obligated to assess the appropriateness of each specific access on a need to know basis.

SAMPLE DOCUMENT

See Exhibit 1 - "Need to Know" for further discussion and examples of this definition.

System Administrator - the individual responsible for the functions of installing, maintaining, and operating hardware and software platforms (system environments). (The roles of system and account administrator may be combined for smaller databases.)

IV. POLICY STANDARDS

General Standards:

- A. All persons with access to ORGANIZATION health information assets may only have such access on a need to know basis and must be approved and verified as Authorized Data Users at regular intervals (but no less than annually) by the appropriate Departmental Director (or Delegated Access Coordinator).
- B. It is the responsibility of every Authorized Data User to maintain confidentiality of ORGANIZATION health information assets even if technical security mechanisms fail or are absent. A lack of security measures to protect the confidentiality of information does not imply that such information is public.
- C. Each clinical staff member, employee, trainee, student, vendor, volunteer, or contractor, or other affiliate of the ORGANIZATION with access to ORGANIZATION health information is subject to and has the responsibilities outlined in this policy as well as those outlined in their organization's policy on confidentiality of information . For external entities, this is covered by the Information Sharing Agreement, see ORGANIZATION Policy ##### "Sharing ORGANIZATION Data with External Entities."

SAMPLE DOCUMENT

- D. Individually identifiable health information is the property of the individual to whom the information pertains and the ORGANIZATION is the steward of that information and the owner of the storage medium.
- E. If an Authorized Data User elects to place individually identifiable health information onto personally-owned media or storage devices (e.g. PDAs, floppy disks, case logs, note cards), he or she is responsible for ensuring that its security, confidentiality, and integrity are maintained according to this policy, and he/she is individually responsible for any breaches that occur as a result of his/her actions.
- F. A person must be identified by the Data Steward (or Business Owner) as the Data Manager for each ORGANIZATION health information asset.
- G. The ORGANIZATION Information Security Committee (security oversight entity) shall provide assistance to the ORGANIZATION community on interpretation of existing policy, cataloging of ORGANIZATION health information assets and individually identifiable health information, monitoring and tracking violations and appeals, identifying areas of risk, defining security controls, and maintaining the AAD in collaboration with other departments that hold information about individuals' job status and access privileges.
- H. All ORGANIZATION health information assets containing individually identifiable health information in any medium must be registered by the appropriate Data Manager in the Authorized Access Database.
- I. If any ORGANIZATION staff member chooses to maintain a database containing individually identifiable health information generated in the course of performing professional responsibilities, he/she will be responsible as Data Manager for that database and must follow all applicable rules.

SAMPLE DOCUMENT

- J. Individuals have the right to correct inaccurate individually identifiable health information. The appropriate process for validating and processing such corrections is determined individually by each organization, and specified in that organization's policies (see, e.g., Medical Information Services Policy #####, "Medical Record Amendment;" policy _____). Each Data Manager is responsible for ensuring that validated correction requests relevant to ORGANIZATION data assets under his/her control are implemented.
- K. In order to protect the individually identifiable health information entrusted to ORGANIZATION, all directed communication/solicitations shall adhere to ORGANIZATION Policy #XX-XX-XXX "Directed Communication/Solicitations".
- L. ORGANIZATION (through the ISC) shall create, administer and oversee policies to ensure the prevention, detection, containment and correction of breaches of security, integrity, and confidentiality.
- M. ORGANIZATION, through the Information Security Committee, shall evaluate and certify that appropriate security systems and measures are implemented. For external entities, this is part of the Information Sharing Agreement.
- N. The security management process shall be the responsibility of the Business Owner, according to the guidelines set by the ISC, and must include, at a minimum, the implementation of:
1. Risk analysis, based on information asset contents and user population, to determine the likely occurrence and severity of loss of potential incidents.
 2. Risk management including formal, documented procedures for monitoring, detection, auditing, reporting, and responding to breaches of security, integrity, and confidentiality.

SAMPLE DOCUMENT

3. A disciplinary process including procedures for the potential discipline, up to and including dismissal, for misuse, misappropriation of data, or acts of omission or commission which result in breaches of security, integrity, or confidentiality.
- O. The prevention of access to ORGANIZATION health information assets by unauthorized or untrained personnel shall be addressed by personnel security policies, including provisions that:
1. Ensure that all personnel with access or potential access to ORGANIZATION health information assets have gone through personnel clearance procedures — they have been screened, are specifically authorized for that access, are trained in relevant ORGANIZATION confidentiality policies, and have attested knowledge of and compliance with those policies.
 2. Ensure that operating and maintenance personnel are given the access necessary for them to perform their system maintenance responsibilities without compromising individually identifiable health information.
 3. Ensure that personnel performing maintenance activities related to ORGANIZATION health information assets are supervised by authorized, knowledgeable persons.
 4. Require maintenance of records of those granted physical access to ORGANIZATION health information assets.
 5. Employ personnel security policy/procedures.
 6. Ensure that system users, including technical maintenance personnel, are trained in system security.
- P. The security management process shall be the responsibility of the Business Owner, according to the guidelines set by the ISC, and must include, at a minimum, formal,

SAMPLE DOCUMENT

documented policies and procedures to limit physical access while ensuring that properly authorized access is allowed, including contingency planning for how security is to be maintained in the event of an emergency. These controls shall include, but not be limited to:

1. Applications and data criticality analysis.
 2. A data backup plan.
 3. Disaster recovery.
 4. Emergency mode operation.
 5. Equipment control (into and out of site) including workstation and laptop computers.
 6. A facility security plan coordinated with Hospital Security Services and/or any other relevant security organizations.
 7. Procedures for verifying access authorizations prior to physical access.
 8. Maintenance records.
 9. Need-to-know procedures for personnel access.
 10. Sign-in for visitors and escort, if appropriate.
 11. Testing and revision.
- Q. To ensure that appropriate access control of ORGANIZATION health information assets are in place and to fulfill the obligation to keep information timely, accurate, complete, and confidential, all information systems and application programs must adhere to the following principles:
1. Data Stewards, Business Owners, Data Managers, Account and System Administrators are accountable for ensuring that the information security policies are fully executed.
 2. Information systems and application programs must provide a mechanism to control authentication, authorization, and audit.

SAMPLE DOCUMENT

3. All members of the ORGANIZATION “community” shall be assigned a unique ORGANIZATION name identifier. The user assigned a specified account shall be the sole user of that account and its associated identification methods; they shall not be shared. Identification methods include, but are not limited to, login names or IDs, password and pass phrases, digital certificates and signatures, PIN, tokens, smart card, biometrics (voice and finger printing), and other forms of personal identification.
4. Authentication shall include establishment of criteria for account eligibility, creation, maintenance, and expiration.
5. When passwords are used as an authentication mechanism, a password shall be present, be of a minimal length, be changeable by the end user, be encrypted, be non-reusable (uniqueness) and have a timed forced renewal.
6. Intruder detection and lockout (maximal limit of 3-5 attempts with a 15-30 minute timeout upon violation) shall be set on for the account.
7. Electronic communication of and exchange of health information that occurs over open networks such as the Internet must include strong authentication, adequate encryption, and effective administration of keys and passwords for encryption.
8. Applications shall provide an automatic logoff/lockout after a specified period of inactivity of interaction with that application; a user shall re-authenticate to gain access to the application. The period of inactivity shall be long enough to provide for continuous user interaction with the application, yet short enough not to permit access to a possibly unattended session (no longer than 7 minutes).

SAMPLE DOCUMENT

9. One authoritative source shall hold the identifications for ORGANIZATION users, information systems, applications, and their processes. This authoritative source shall include the identification information of application processes which access ORGANIZATION health information assets for purposes of capturing, providing, and/or receiving information.
- R. External data users shall have access to ORGANIZATION health information assets only upon the completion of an Information Sharing Agreement with ORGANIZATION, as described in ORGANIZATION Policy #####, "Sharing Information with External Entities."
- S. There may be cases in which a state, federal, or regulatory agency requires that it be granted access to ORGANIZATION health information assets under law or regulation. In such cases, to the extent possible, an Information Sharing Agreement meeting the criteria listed in ORGANIZATION Policy #####, "Sharing Information with External Entities," shall be negotiated between ORGANIZATION and the agency before access is granted to the ORGANIZATION data assets.
- T. Individually identifiable health information that is subject to additional specific legal restrictions shall be subject to the additional safeguards and processes specified in Exhibit 2 "Legally Restricted Information". Requests for access to information that is Legally Restricted must be processed in accordance with release of information procedures as specified by the Medical Information Services Department, or other relevant organization (*see, e.g. [policy cites]*).
- U. All data users shall receive education on the expectations, knowledge, and skills related to information security prior to being given access to ORGANIZATION health information assets. ORGANIZATION supervisors shall verify that potential Authorized Data Users

SAMPLE DOCUMENT

under their supervision have received security education and attested to ORGANIZATION Policy ##### “Role and Responsibilities of Authorized Data Users” and ORGANIZATION Policy ##### “Confidentiality” before access to ORGANIZATION information is granted, and that they have attested to the Confidentiality policy on an annual basis.

- V. To the extent technologically practical, system administrators shall maintain ongoing internal audit processes which record system activity such as log-ins, file accesses, and security incidents.
- W. To the extent that an audit trail shows access to an individual's individually identifiable health information, it shall be made accessible to that individual at the individual's request in the event that questions arise about improper access to his or her records.
- X. All Authorized Data Users, both internal and external, shall be made aware, as a part of the AAC process and the supervisory educational process, that records of data access by users are a capability of all ORGANIZATION health information assets subject to this policy (to the extent technologically practical) and that, from time to time or as indicated by events and circumstances, such access audits may be conducted.
- Y. Should evidence of data access outside that granted through the AAC process be discovered it may result in revocation of access rights.
- Z. Breaches of confidentiality under this policy are subject to appropriate disciplinary action up to and including discharge or termination of contract/relationship.

V. EXHIBITS -

SAMPLE DOCUMENT

1. Need to Know
2. Legally Restricted Information

VI. REFERENCES

1. ORGANIZATION Policy ##### "Assignment and Retrieval of ORGANIZATION Information Technology Access and ORGANIZATION Property"
2. ORGANIZATION Policy ##### "Role and Responsibilities of ORGANIZATION Data Managers"
3. ORGANIZATION Policy ##### "Information Access: Responsibilities of Department Directors or Delegated Access Coordinators"
4. ORGANIZATION Policy ##### "Role and Responsibilities of Authorized Data Users"
5. ORGANIZATION Policy ##### "Sharing ORGANIZATION Data with External Entities"
6. ORGANIZATION Policy ##### "Confidentiality of Patient Information"
7. ORGANIZATION Policy #XX-XX-XXX "Directed Communication/Solicitations"
8. Medical Information Services Policy #####, "Medical Record Amendment"
9. SPG 601.12, The University of ORGANIZATION Policy on Institutional Data Resource Management.
10. University of ORGANIZATION, Data Administration Guidelines for Institutional Data Resources.
11. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191 (1996).

SAMPLE DOCUMENT

AUTHOR: ORGANIZATION Information Security Committee

SAMPLE DOCUMENT

Information Management Policy: Need to Know

ORGANIZATION, Health Centers, and Medical School

EXHIBIT 1

Policy ##### Information Management

NEED TO KNOW

Definition: **Need to know** - the principle that states that a user should access only the specific information necessary to perform a particular function in the exercise of his/her appointed duties. Once access to an application is authorized, the authorized data user is still obligated to assess the appropriateness of each specific access on a need to know basis.

Following are examples where employees have a need to know individually identifiable health information to complete their assigned job functions, as well as examples where employees do not have a need to know such information. These lists are intended to be examples only, and are not intended to be complete representations of situations where employees have a need to know individually identifiable health information. Per the ORGANIZATION policy, specific access to individually identifiable health information is under the discretion of departmental management.

Examples of appropriate uses of individually identifiable health information where employees have a need to know:

Rendering direct clinical care to specific patients (including diagnosis, procedural support, and progress assessment).

Disease management and prevention activities such as immunization verification, screening for candidacy for specialized treatment programs or potential preventative interventions.

At the request of the patient. (Exception: friends or relatives are not permitted access without a form signed by the patient authorizing release of the information.)

Administrative support activities including but not necessarily limited to appointment and scheduling coordination, pre-arrival requirements, complying with third party requirements, follow-up coordination, billing and collecting for services rendered to specific patients, and maintenance of the medical record and/or health information medium.

Financial analysis to assess the business impact of patient care, including but not limited to analysis of specific cases to assess impact of clinical practice redesign or in response to research requests, and analysis of situations where it is necessary to join records from more than one system (for example, Vendor X and Vendor Y) together in order to analyze the full impact of that care.

SAMPLE DOCUMENT

Performing reimbursement analysis on specific patients.

Performing activities in the course of development/fund raising, ORGANIZATION strategic planning, ORGANIZATION legal defense, or follow-up on a compliance complaint.

IRB approved research.

Educational or teaching purposes or instructional requirement criteria.

Performing quality assurance and/or regulatory compliance activities.

Provision of educational materials for patients, given at the direction of their treating physician.

Fund raising activities done at the request of a physician who has knowledge of the patient's or family's desire to donate to the University.

Examples specifically relevant:

Administrative activities including enrollment, claims payment, coordination of benefits, customer service, HEDIS reporting, data quality investigation, and quality improvement of administrative services.

Utilization management activities for the purpose of assessing the appropriateness and efficiency of the health services used to treat a member or group of members, and for determining the contributing causes underlying certain financial results.

Case management activities, including identification of members with a specific type or extent of health problems and provision of case management interventions.

Health promotion or wellness activities to assess, improve, and monitor the health and risk status of members.

Examples of **inappropriate use** of patient identifiable information:

Mass mailing fund raising solicitations to patients with specific medical conditions, without the express approval of the Dean of the Medical School.

Informing others that employees, relatives, famous people, etc. are patients in the hospital.

Use of personal medical information in making employment decisions.

SAMPLE DOCUMENT

Use of employee's personal medical information to see if the employee was really out sick, had a doctor's appointment, had a worker's compensation injury, etc.

Accessing information about a friend, relative, or family member without a signed authorization for release.

Employee access to or request for patient information of a relative or another University of ORGANIZATION Hospitals and Health Centers and Medical School employee, unless:

The request or access is made on behalf of an inpatient unit or an outpatient clinic and the information is needed to provide patient care during a verified clinic appointment or inpatient hospitalization;

The request or access is made for the purpose of carrying out medical research and the need for the patient information is verified as consonant with the goals of that research;

The request or access is made by Financial Services for billing and collection purposes.

SAMPLE DOCUMENT

Information Management Policy: Legally Restricted Information

ORGANIZATION, Health Centers, and Medical School

EXHIBIT 2

Policy ##### Information Management

LEGALLY RESTRICTED INFORMATION

Definition: **Legally Restricted Information** - individually identifiable health information whose disclosure is specifically subject to additional legal requirements imposed by statute or administrative rule.

Examples of legally restricted information are:

substance abuse treatment records,

sexual abuse treatment records,

mental health treatment records,

certain diagnostic categories such as HIV/AIDS

adolescent health information related to pregnancy, birth control, and/or sexually transmitted diseases

SAMPLE DOCUMENT

Job Descriptions

The sample job descriptions included in this Supplement to the Guidelines for Academic Medical Centers on Security and Privacy are not meant to be use as a replacement for good organizational practices and documentation. Organizations are encouraged to work with legal council and human resource staff to determine appropriate format and content for their particular circumstance. This supplement is meant to serve as a starting point for organizations developing or updating security and privacy officer roles.

SAMPLE DOCUMENT

Information Security Officer

Organizational Relationships: The position reports to an administrator within the Department of Facilities and Systems Support Services.

Position Overview: Implements and supports information security initiatives throughout ORGANIZATION . Acts as a focus and resource for ORGANIZATION information security matters. Works with those in corresponding roles at the ORGANIZATION group practices and at ORGANIZATION Health System sites. Takes direction from the Information Security Subcommittee and Department of Facilities and Systems Support Services Administration. Investigates and recommends secure solutions that implement information security policy and standards. Coordinates Office of Information Security activities and manages staff. Oversees, implements and monitors the National Industrial Security Program and special security requirements levied by the Department of Defense and intelligence community agencies.

Education/Experience/Job Specifications: A four-year college degree is required. A Certified Information Systems Security Professional rating is desired. At least ten years of information security work experience is required with both public and private sector experience preferred. The ability to work effectively in a collegiate, consensus driven organization is required, as are demonstrated personnel and information security program management skills. A working knowledge of all aspects of information security is essential, as is the ability to apply this knowledge in an open network environment.

SAMPLE DOCUMENT

1. Job Specific Competency: <i>Provides ORGANIZATION information security oversight.</i>			
Performance Expectations/Accountabilities	AE	NI	NA
a) Maintains current and appropriate body of knowledge necessary to perform the information security management function.			
b) Effectively applies information security management knowledge to enhance the security of the open network and associated systems and services.			
c) Maintains working knowledge of external legislative and regulatory initiatives. Interprets and translates requirements for implementation.			
d) Develops appropriate information security policies, standards, guidelines and procedures.			
e) Works effectively with other ORGANIZATION information security personnel and the committee process.			
f) Provides meaningful input, prepares effective presentations and communicates information security objectives.			
g) Participates in short and long term planning.			
h) Monitors Information Security Program compliance and effectiveness.			

SAMPLE DOCUMENT

2. Job Specific Competency: <i>Provides ORGANIZATION information security oversight.</i>			
Performance Expectations/Accountabilities	AE	NI	NA
a) Works with committees and management professionals to accomplish information security goals.			
b) Coordinates and prioritizes activities of the Office of Information Security in support of the mission.			
c) Acts as a resource for matters of information security. Provides pertinent and useful information.			
d) Oversees and conducts information security reviews and liaison visits to ORGANIZATION Health System practices. Makes recommendations and reports to Regional Practice Administration.			
e) Coordinates and performs reviews of contracts, projects and proposals. Assists information technology proponents with standards compliance.			
f) Conducts investigations of information security violations and computer crimes. Works effectively with management and external law enforcement to resolve these instances.			
g) Reviews instances of noncompliance and works effectively and tactfully to correct deficiencies.			

SAMPLE DOCUMENT

3. Job Specific Competency: <i>Manages Office of Information Security personnel.</i>			
Performance Expectations/Accountabilities	AE	NI	NA
a) Determines positions and personnel necessary to accomplish information security goals. Requests positions, screens personnel and takes the lead in the interviewing and hiring process.			
b) Develops meaningful job descriptions. Communicates expectations and actively coaches personnel for success.			
c) Prioritizes and assigns tasks. Reviews work performed. Challenges staff to better themselves and advance the level of service provided.			
d) Provides meaningful feedback to staff on an ongoing basis and formally appraises performance annually.			

SAMPLE DOCUMENT

Chief Security Officer (CSO) (Sample #1)

Organizational Relationships: The position reports to [administrator, CIO, vice president, etc.]

Position Overview: Implements and supports information security initiatives throughout the organization. Acts as a focus and resource for information security matters. Works with those in corresponding roles at other organizational entities. Takes direction from the oversight committee and organization administration. Investigates and recommends secure solutions that implement information security policy and standards. Coordinates Office of Information Security activities and manages staff. Oversees, implements and monitors any special security requirements levied by government agencies in the performance of funded research, clinical trials and other activities.

Education/Experience/Job Specifications: A four-year college degree is required. A Certified Information Systems Security Professional rating is desired. At least ten years of information security work experience is required with both public and private sector experience preferred. The ability to work effectively in a collegiate, consensus driven organization is required, as are demonstrated personnel and information security program management skills. A working knowledge of all aspects of information security is essential, as is the ability to apply this knowledge in an open network environment.

SAMPLE DOCUMENT

2. Job Specific Competency: <i>Provides information security oversight for greater Academic Medical Center.</i>			
Performance Expectations/Accountabilities	AE	NI	NA
i) Maintains current and appropriate body of knowledge necessary to perform the information security management function.			
j) Effectively applies information security management knowledge to enhance the security of the open network and associated systems and services.			
k) Maintains working knowledge of external legislative and regulatory initiatives. Interprets and translates requirements for implementation.			
l) Develops appropriate information security policies, standards, guidelines and procedures.			
m) Works effectively with other entity information security personnel and the committee process.			
n) Provides meaningful input, prepares effective presentations and communicates information security objectives.			
o) Participates in short and long term planning.			
p) Monitors Information Security Program compliance and effectiveness.			

SAMPLE DOCUMENT

2. Job Specific Competency: <i>Provides information security oversight for local entities [if so structured].</i>			
Performance Expectations/Accountabilities	AE	NI	NA
h) Works with committees and management professionals to accomplish information security goals.			
i) Coordinates and prioritizes activities of the Office of Information Security in support of the mission.			
j) Acts as a resource for matters of information security. Provides pertinent and useful information.			
k) Oversees and conducts information security reviews and liaison visits to regional practices. Makes recommendations and reports to Regional Practice Administration.			
l) Coordinates and performs reviews of contracts, projects and proposals. Assists information technology proponents with standards compliance.			
m) Conducts investigations of information security violations and computer crimes. Works effectively with management and external law enforcement to resolve these instances.			
n) Reviews instances of noncompliance and works effectively and tactfully to correct deficiencies.			

SAMPLE DOCUMENT

3. Job Specific Competency: <i>Manages Office of Information Security personnel.</i>			
Performance Expectations/Accountabilities	AE	NI	NA
e) Determines positions and personnel necessary to accomplish information security goals. Requests positions, screens personnel and takes the lead in the interviewing and hiring process.			
f) Develops meaningful job descriptions. Communicates expectations and actively coaches personnel for success.			
g) Prioritizes and assigns tasks. Reviews work performed. Challenges staff to better themselves and advance the level of service provided.			
h) Provides meaningful feedback to staff on an ongoing basis and formally appraises performance annually.			

SAMPLE DOCUMENT

Chief Information Security Officer (CSO) (Sample #2)

This position is a senior level manager responsible for championing institutional security awareness, security policy and procedure development, and working to ensure compliance with internal and external standards related to information security. The CSO would report to the ORGANIZATION Deputy Corporate Compliance Officer.

Duties and Responsibilities

- Chair the ORGANIZATION Information Security and Privacy Committee (ISPC) in its policy development effort to maintain the security and integrity of ORGANIZATION information assets in compliance with state and federal laws, and accreditation standards.
- Provide project management and operational responsibility for the administration, coordination and implementation of information security policies and procedures across the Health System including the Hospitals and Health Centers, Medical School.
- Perform periodic information security risk assessments including disaster recovery and contingency planning, and coordinate internal audits to ensure that appropriate access to ORGANIZATION information assets is maintained.
- Serve as a central repository for information security-related issues and performance indicators. Develop, implement, and administer a coordinated process for response to such issues.
- Function when necessary as an approval authority for platform and/or application security and coordinate efforts to educate the ORGANIZATION community in good information security practices.
- Maintain a broad understanding of federal and state laws relating to information security and privacy, security policies, industry best practices, exposures, and their application to the ORGANIZATION information technology environment.
- Make recommendations for short and long-range security planning in response to future systems, new technology, and new organizational challenges.
- Act as an advocate for security and privacy on internal and external committees as necessary.
- Develop, maintain and administer the security budget required to fulfill ORGANIZATION information security expectations.

Minimum Qualifications

- Bachelor's degree in Computer Science or related field or equivalent experience.
- Five or more years of experience in information security.
- Eight or more years of experience in information technology.
- In-depth understanding of network and system security technology and practices across all major-computing areas (mainframe, client/server, PC/LAN, telephony) with a special emphasis on Internet related technology.

SAMPLE DOCUMENT

- Demonstrated effectiveness with consensus building, policy development and verbal and written communication skills.
- Clear ability to explain information technology concepts to audiences outside the field.

Preferred Qualifications

- Specific experiences in the health care industry.
- Extensive familiarity with health care relevant legislation and standards for the protection of health information and patient privacy.
- Demonstrated successful project management expertise.
- Professional certification, e.g. CISSP, CISA.
- Experience with student record/higher education laws.



Corporate Privacy Officer

The Corporate Privacy Officer oversees the development and implementation of corporate-wide privacy principles, policies and practices. The Corporate Privacy Officer is responsible for coordinating all corporate activities with privacy implications, as well as monitoring all of the organization's services and systems to assure meaningful privacy practices. The Corporate Privacy Officer also advocates and protects patient privacy by serving as a key privacy advisor for patients, handling disputes and managing patient requests regarding their medical record.

Requirements:

- Coordinates corporate privacy activities which include overseeing the establishment, implementation and adherence to corporate policies on patient privacy, confidentiality and release of patient information
- Reviews new or revised government healthcare laws and regulations pertaining to patient privacy to determine if new policies or modifications of current policies are needed
- Conducts privacy risk assessments and internal privacy audits
- Manages patient privacy-disputes and requests for changes to their medical record
- Increases the public's awareness of the organization's efforts to preserve patient privacy
- Oversees the development and delivery of privacy training and awareness.
- Works closely with Health Information Management, Information Technology and Marketing departments
- Ensures that record custodians correctly protect and archive patient information
- Ensures that the organization's privacy protections keep pace with technological advances
- Participates in outside healthcare organizations for keeping updated on privacy developments and "best practices" for patient privacy
- Reports to the organization's executive officers on emerging legislation/regulations and how the company is currently dealing with privacy issues

General Skills:

- Good verbal and written communication skills
- A high level of integrity and trust
- Knowledge and understanding of technology-related law and public policy experience, clinical research and related issues

Professional Certifications or Experience:

- Registered Health Information Administrator (RHIA)

This position description is intended to describe the general requirements for this position. It is not meant to an exhaustive statement of duties, responsibilities and requirements.



Information Security Officer

The Information Security Officer designs, develops and implements security changes and enhancements to the Information Technology (IT) computing environments. The Information Security Officer is responsible for determining appropriate security measures and creating policies and procedures that monitor and control access to system resources and data. The Information Security Officer will update security standards as necessary and is responsible for the prevention, detection, containment and correction of security breaches.

Requirements:

- Oversees the establishment, implementation and adherence to policies and procedures that guide and support the provision of information security services
- Conducts risk assessments and risk analysis to help the organization develop security standards and procedures that support strategic, tactical and operational objectives on a cost-effective basis
- Makes recommendations on appropriate personnel, physical and technical security controls
- Manages the Information Security Incident Reporting program to ensure the prevention, detection, containment and correction of security breaches
- Participates in resolving problems with security violations
- Responsible for the content (and in some cases the delivery) of information security seminars and training classes
- Coordinates the communication of information security awareness to all members of the organization
- Certifies that IT systems meet predetermined security requirements
- Strives to maintain high system availability
- Works with vendors, IT associates, and user departments to enhance information security

General Skills:

- Good verbal and written communication skills
- A high level of integrity and trust
- Knowledge of security hardware and software products that comply with current industry standards.
- Knowledge and understanding of technology-related state and federal regulations

Professional Certifications:

- Certified Information Systems Security Professional (CISSP®)

Or

- Certified Information Systems Auditor (CISA®)

This position description is intended to describe the general requirements for this position. It is not meant to be an exhaustive statement of duties, responsibilities and requirements.