HIPAA & California State Patient Confidentiality Laws

Staff Training

Arrowhead Regional Medical Center

HIPAA PRIVACY & SECURITY

HIPAA & California State Patient Confidentiality Laws
Staff Training

Arrowhead Regional Medical Center

Instructions

Please read through this handbook and the attached policies and complete the acknowledgement form on the last page and return it to you department chairperson or manager. Thank you.

Introduction

This handbook provides a general overview of the federal and state regulations which protect patient privacy and Arrowhead Regional Medical Center's policies and procedures which staff must follow while working for or on behalf of the medical center.

Protection of patient confidentiality is a very important subject which requires the training of all staff that provide patient care or deal with patient information. Federal and state laws require that health care providers, including hospitals and affiliated medical staff, implement safeguards which provide for the privacy and security of patient information. HIPAA and California state law both require reporting of breaches of a patient's privacy in certain circumstances. Employees & providers that fail to comply with HIPAA and state law are subject to fines and penalties and criminal prosecution in certain circumstances. By following state and federal laws and ARMC policies health care providers can reduce or eliminate the legal and financial liability associated with non-compliance and provide a safe and private environment for the patient which promotes patient care in providing quality health care to the community.

California Anti-Snooping Laws

It is critical that all ARMC employees understand that it is against the law to look at a patient's medical records out of curiosity or without a business need to know. California passed two new laws, AB211 and SB541, effective January 1, 2009, which are intended to prevent healthcare providers and other staff and employees from "snooping" into the medical records of patients. The laws also require that facilities report any breaches of patient confidentiality to the patient and to the California Department of Public Health (CDPH).

Kaiser Permanente Snooping Incident

In January 2009, Nadya Suleman, (Octomom) gave birth to her octuplets at Kaiser Permanente. Kaiser advised staff not to look at this patient's records out of curiosity or without a legitimate business reason. Even after training, 23 people (including 2 physicians) still looked at her records electronically out of curiosity. Kaiser fired 15 people and disciplined the rest. The CDPH still fined Kaiser for each person that accessed the patient's records. Kaiser was fined $250,000 for failing to prevent the unauthorized access to the patient's records. Those individuals who are licensed by the state may face additional fines and disciplinary action against their licenses.

HIPAA Overview

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law which sets forth requirements for health care providers to protect the privacy of patient information in all forms by limiting the use and disclosure of such information and requiring implementation of safeguards to protect the information from inappropriate access, use or disclosure.

HIPAA Privacy and Security Rules

The HIPAA Privacy and Security Rules are federal regulations that require health care providers to put in place certain safeguards which protect the privacy and security of patient information in all forms. The Privacy Rule and the Security Rule work together to limit the use and disclosure of patient information without the patient's authorization and require safeguards to protect the confidentiality, integrity and availability of a patient's information stored in electronic form.

The HIPAA Privacy and Security Rules cover certain patient information created, used or disclosed by Covered Entities (CE's). A CE is a health care provider, such as a physician or hospital, which bills for health care electronically; a health plan or a clearinghouse. Other providers of health care may include clinics, laboratories, pharmacies, and home-health agencies.

The Privacy Rule

The Privacy Rule took effect in 2003. The Rule established requirements for safeguarding patient information by requiring that CE's limit their use and disclosure of patient information and secure that information in all forms; paper, oral and electronic. The Privacy Rule also established certain patient rights which allow the patient to see and get copies of records, request amendments for their records if they believe there to be an error in them, request restrictions on the use and disclosure of their records and to file a complaint when they feel that their privacy has been violated.

Privacy Notice

The Privacy Rule established a requirement for CE's to notify the public of the CE's privacy practices (how the CE uses and discloses patient information) and the patients rights. These practices are summarized and provided to the public in the Notice of Privacy Practices. (Also known as the Privacy Notice.) The ARMC Privacy Notice is provided to the patient when the patient signs the consent for treatment. The Privacy Notice is also available on the ARMC website at www.arrowheadmedcenter.org.

Penalties

The penalties for violations of the HIPAA Privacy & Security rules range from $50,000 to $250,000 (and up to 10 years in prison) against an individual who knowingly and in violation of HIPAA obtains, uses or discloses a patient's protected health information. Organizations may also be fined for non-compliance depending upon the level of non-compliance. Fines for organizations can range up to 1.5 million dollars.

Business Associates

HIPAA also impacts the Business Associates (BA) of a CE. BA's are defined as those who conduct business for or on behalf of a CE and who create, use or disclose patient information in order to perform these services. Before BA's can perform these functions for a CE, the CE must receive written assurance from the BA that the BA will protect the patient information and comply with the provisions of the Privacy and Security Rules. This assurance is normally documented and executed in a contract defined under HIPAA as a Business Associate Agreement (BAA).

Protected Health Information

What is Protected Health Information? When we speak of patient information, we're talking about what HIPAA calls, "Protected Health Information" or PHI. PHI is any health information that could identify a particular person. The person could be living or deceased. The information could be about the past, present or future health of a person. The information could be written on paper, displayed or stored in computer, or it could be spoken. Examples include patient charts, reports, x-rays, billing systems, nursing notes, conversations about patients and patient rounds sheets. All research records involving patients must also be protected.

Use and Disclosure of PHI

Covered Entities may use or disclose PHI for their own treatment, payment or health care operations activities (often referred to as TPO in the regulations). We "use" health information in our hospital and clinics. We "disclose" or release health information when we give it to another entity to use. HIPAA permits the use and disclosure of PHI for three primary purposes without having to obtain a patient's written authorization.

Treatment

Treatment is generally anything to do with the provision, coordination or management of health care and related services by one or more health care providers. Treatment might include consultation between one physician and another, or referral from one health care provider to another. Consultation regarding treatment, diagnosis or referral is permitted for general health care providers without an authorization; however, special confidentiality laws governing substance abuse treatment programs require an authorization from the patient before providers from those treatment programs may speak with health care providers outside of the program.

Payment

This generally refers to any movement of money in relation to an individual's health care. It refers to the collection of premiums and the determination of responsibility for coverage and benefits. It refers also to the reimbursement of health care providers. And it refers to the collection of payments due to a health plan under a reinsurance contract.

Health Care Operations

This can include any activity involving administrative, financial, legal and quality improvement activities; business planning activities; training, teaching; accreditation, credentialing, licensing, competence, performance activities; fraud, abuse or compliance activities.

Use of PHI for Training or Education

Prior to using any patient information for training or educational purposes, you must obtain the permission of your department chair or manager. Use of PHI for such purposes must be limited and all direct identifiers must be removed from the information prior to use. Use of PHI for educational or training purposes is covered further in ARMC policies section 1000. No patient identifiable information or reports containing information from any ARMC generated medical records may be used for posting to any website or used for external training. All patient identifiers and ARMC identifying information (such as the name of the medical center and any doctor's names) must be redacted from the information and permission obtained from your supervisor prior to use or disclosure. If you have any questions contact the Hospital Privacy & Security Officer at 909-580-3287.

Incidental Disclosures

The HIPAA Rules were written with the understanding that despite having safeguards in place, in certain circumstances, others may overhear information about another patient within the healthcare setting. These types of disclosures are allowable under HIPAA as incidental disclosures. For example, a doctor or nurse enters a patient's room and pulls the curtain to examine the patient. The doctor or nurse used reasonable precautions such as speaking in a low voice and pulling the privacy curtain closed. However, the room is a semi-private room and the other patient overhears the conversation. Since reasonable precautions were followed this would not be considered a HIPAA violation. Calling out a patient's name in a waiting room is acceptable also. An example of a violation which is not considered an incidental disclosure would be when two doctors are discussing a patient outside of the healthcare setting such as in an elevator and another patient overhears the conversation.

Patient Authorization Requirements

When there is a request to use or disclose patient information for purposes other than treatment, payment or healthcare operations, or as specifically permitted by the Privacy Rule or required by law, then a valid authorization from the patient must be obtained in writing prior to the use or disclosure being made. The authorization must be specific and include what information is being requested, to whom the information is to be given, the purpose of the request and an expiration date. An example of when an authorization would be required includes providing information to an attorney or prior to allowing media to interview a patient or prior to providing any patient-specific information to the media. ARMC uses an official valid authorization form which complies with both federal and state law (located in ARMC tools under Authorization Form).

Minimum Necessary

HIPAA established the Minimum Necessary rule in order to limit the access to, use and disclosure of PHI to the minimum amount necessary in order to conduct business for purposes other than treatment of the patient. Under the Minimum Necessary rule, medical staff must limit their use or disclosure of patient information to the minimum necessary amount when the use is not for treatment. Further, if a member of the workforce, employee or provider does not have a business need to know, then they must not access, view, use or disclose patient information.

If it's not part of your job, it's not part of your business! If not involved in their care, NO ONE is allowed to look up any information on strangers, friends, family members, or even themselves!

Reasonable Safeguards

Verbal Information

Be careful when talking to or about patients when you are within earshot of others. Always check with the patient first before discussing their care in front of other people. Never assume that it is okay with the patient. Speak with a quiet voice or move to a more private place. Avoid using patient names or other identifiers when speaking about patients with other care providers if possible. Don't disclose patient information to others unless it is necessary for patient care.

Be careful when leaving messages for a patient on an answering machine. You can't be sure who might overhear it. Leave only the name of the facility and a return phone number if possible.

Printed Information

Printed patient information takes on many forms. Information about a patient may be in the form of hand written notes, printed computer information such as reports or lab results, information on a prescription, patient round sheets, a printed fax or other documents. Proper steps to protect printed information include locking file cabinets, offices or other doors or areas where printed information may be stored, and securing printers and other devices that produce printed information. Always dispose of printed information in confidential shred bins. Never place patient information in the trash. Be especially careful when carrying patient information around in your pockets as it may fall out and inadvertently breach the patient's privacy. This type of breach may then be reportable to the state CDPH.

Electronic Information

Patient information stored electronically includes information stored on computer systems, hard drives, PDA's, cell phones, email, CDROM's, memory sticks, flash drives and any other device capable of storing data in an electronic format. Patient information in electronic form is covered by the HIPAA Privacy Rule and the HIPAA Security Rule. The Security Rule requires that information stored electronically be protected from anything that would be a threat to the confidentiality, integrity and availability of that information. The Rule also requires that ARMC have in place certain Administrative, Technical and Physical safeguards.

Examples of these types of safeguards include requiring that all staff have a unique user ID and password in order to access patient information on computers. Users are to log off of computers promptly when completed with work or lock the computer before leaving it unattended. Never store patient identifiable information on a device that has no security or access controls. Never remove or transfer electronic patient information out of the medical center or store it on home computers or post to a personal or unauthorized website.

Inappropriate Access

All staff must protect patient information from all threats of loss or unauthorized disclosure. Further staff must not try to access, use or disclose information about a patient unless they have a legitimate business need to look at such information. *In other words, do not look at a patient's medical information just because you are curious or concerned about them.* This is considered a breach of the patient's privacy and must be reported. ARMC routinely audits access to it's systems to ensure that users are not accessing information inappropriately.

Sanctions

HIPAA requires that ARMC sanction staff for violations as part of complying with HIPAA. Most policy violations related to privacy and/or security incidents are also violations of state and/or federal law and must therefore be appropriately reported and investigated by the Hospital Privacy and Security Officer. Individuals may be found liable for damages resulting from disclosure of patient medical, financial or even demographic information and may be subject to civil lawsuits and/or criminal prosecution in some circumstances. It is important to understand that violations or non-compliance may result in more than just disciplinary action. Under the law, when a violation occurs, the individuals name must be provided to the CDPH. The CDPH can then forward the violators name to the licensing agency for further fines and disciplinary action against the license of the individual. Also, certain HIPAA violations can subject the individual to prosecution under federal law by the Department of Justice resulting in fines and or imprisonment. (See ARMC Policy 700.06)

Case Scenarios

Situation #1

Consider the example of a patient in the waiting room. His physician is discussing his cancer condition with him and a nurse, and everyone in the waiting room can hear the conversation.

What could have been done differently to protect this patient's privacy?

- The physician should have tried to find a private room or area where details could not be overheard. Even when the patient's name is not specifically used in conversation, remember that details about his condition can be identifying factors in certain circumstances. This patient would be embarrassed and could file a complaint against the physician in which case the possible breach of privacy would have to be investigated and possibly reported to the state.

Situation #2

You are a healthcare provider. Your friend's spouse is in the hospital after an accident. Your friend asks you to review what treatment has been provided to the spouse and see if you concur. You are not part of the patient's treatment team. What are you able to do under current state and federal laws?

- If you access the person's chart so that you can communicate with your friend about the patient's condition you would be in violation of ARMC policy and state and federal law. Remember, it is wrong to access the patient's chart just so you can help out a friend.
- The correct response would be for you to advise your friend that you can only look at the medical record if you are treating the patient.

Situation #3

You are in the ER examining a 6-year-old boy and observe cigarette burns on the arms and hands of the boy. What does HIPAA require you to do?

- In this particular case HIPAA permits the disclosure of the patient's information because the report is required by law. Patient safety is involved, and when federal or state law require that you report the situation to the proper authorities the disclosure is permitted by HIPAA without requiring you to obtain authorization from the patient or the parents prior to disclosure.

ARMC Administrative Operations Policies Overview

Arrowhead Regional Medical Center has many policies that cover patient privacy and the protection of confidential information. ARMC Administrative policies 1000.07 Uses and Disclosures of Protected Health Information and 700.01 Information Security – General Requirements are attached to this handbook for you to review. (*The full list of policies can be located in ARMC Tools under the policies-privacy and policies-security folders*.)

Contact and Resource Information

If you have any questions or concerns or need to report a situation of possible non-compliance please contact the Hospital Compliance Department at 909-580-3170 or the Hospital Privacy & Security Officer at 909-580-3287. You can find out more information about HIPAA at the Office for Civil Rights website at www.hhs.gov/ocr/privacy/index.html.

ARROWHEAD REGIONAL MEDICAL CENTER
Administrative Operations Manual

SECTION: **INFORMATION MANAGEMENT** **SUB SECTION:** **INFORMATION SECURITY**

SUBJECT: **INFORMATION SECURITY – GENERAL REQUIREMENTS**

APPROVED BY: ____
Chief Executive Officer

_

POLICY

It is the policy of Arrowhead Regional Medical Center (ARMC) to protect the Confidentiality, Integrity and Availability (CIA) of information it collects, maintains, uses, or transmits; whether written, spoken, recorded electronically or printed and to assure that such information is readily available for patient care and business operations. Federal and state laws govern the protection of certain non-public "sensitive" information, including health, employment and financial information. ARMC utilizes various administrative, physical and technical safeguards to fulfill these requirements. All staff has a responsibility to understand and utilize these safeguards and protect all information systems, personnel, and data at all times. Workforce members, (employees, contracted service providers, medical corporations, volunteers, students, physicians and others granted authorized access to ARMC facilities or resources), other authorized users and all departments are responsible for knowledge of and compliance with this and related privacy & security policies.

AMPLIFICATION

ARMC is increasingly dependent upon computer systems for storage, processing, and transmission of information in order to provide quality healthcare to the community and perform business operations. This dependence, along with changes in state and federal regulations, requires implementation of enhanced safeguards to ensure such information is protected from loss, theft or damage. All information and information systems must be identified, categorized and protected in accordance with policy. Taken as a whole, these policies provide a framework for information security by requiring that these protections be implemented, maintained, monitored and enforced. Individual departments may need to develop or modify existing policies either to comply with these policy requirements or to enhance or clarify system or area specific issues. Such policies may be more restrictive but must not conflict with the requirements established herein.

1. **APPLICABILITY**

   This policy applies to:

   A. ARMC workforce members (regular employees, per-diem contract staff, contract service providers, volunteers, students, resident physicians, attending staff, physicians), Organized Health care Arrangement (OHCA) participants, medical corporations and Family Health Centers (FHCs) and others granted authorized access to ARMC facilities or resources.

   B. Clinical information generated in the context of patient care, including, for example, laboratory data, radiology results, results of other tests and procedures, and the dictated and written notes detailing patient histories and physical examination findings. Such patient-related data may be available electronically, or in written form in standard medical records and patient charts. It may be available for individual patients or for groups of patients. Such information may reside in large central computer databases, or on stand-alone workstations, diagnostic equipment or handheld technology devices.

   C. Employment information collected and maintained by the Human Resources department, the various graduate programs, and Medical Staff data. The regulations of the Family Educational Rights and Privacy Act of 1974 as amended (i.e., FERPA) will be applied to employee information.

   D. Business operations and support functions information such as accounting, payroll, personnel, purchasing, and other activities related to the management of ARMC are also covered. Additionally, this policy applies to library information, research information, and to external and user-specific data files related to ARMC work.

   E. Information systems and technology devices used to process, store, and transmit information.

F. All hardware and/or software of any kind, including in-house developed programs.

2. **PROCUREMENT AND ACQUISITION REQUIREMENTS - INFORMATION SYSTEMS/TECHNOLOGY**

Information systems and/or technology devices including desktop, laptop and server computers, handheld computing devices, peripheral equipment, storage media, and the like, must, as part of the procurement/acquisition process, have a privacy/security risk assessment completed in order to address any privacy and/or security issues and to meet minimum safeguard requirements as defined by this and related privacy and security policies and Information Management requirements.

All information technology and systems purchased after the effective date of this policy must comply with this and related privacy and security policies. Existing systems must be brought into compliance to the greatest extent possible pursuant to a completed system/application/area privacy/security risk assessment. (See APP 700.02 Security Management and Evaluation Process for risk assessment and management requirements.)

3. **PERSONAL HARDWARE/SOFTWARE USE**

No personal hardware, technology devices or software are allowed to be used or installed for any reason whether for personal or business operations or patient care or be connected in any way to the ARMC computer systems or network or be used for storage of ARMC information without prior written authorization from the Hospital Privacy and Security Officer and Director of Information Management, even if not connected to the ARMC network or computer systems.

Only ARMC-owned or controlled technology devices, computers and equipment are allowed to be connected to the network or used for storage of ARMC information or be operated within ARMC or it's facilities after approval and/or installation by Information Management.

Using personal computers (i.e. a home computer) to connect to ARMC network resources remotely via the Email web interface is not considered "connecting" to the ARMC network, however, users granted this access must do so only in accordance with these and related privacy and security policies. Remotely accessing and downloading confidential or restricted ARMC information from the ARMC network is prohibited without prior approval.

4. **NO EXPECTATION OF PRIVACY**

Users of ARMC computer systems and facilities have no expectation of privacy in anything they create, store, send or receive on ARMC computer systems. All information generated on ARMC computers or network systems is considered the property of ARMC and therefore, open to view and/or monitoring by authorized personnel as designated by the Hospital Privacy & Security Officer and the Director of Information Management. Oversight of all monitoring functions for investigational purposes is the responsibility of the Hospital Privacy & Security Officer or Chief Compliance Officer.

5. **GENERAL SAFEGUARD REQUIREMENTS**

Privacy and security are inseparably linked. You cannot have privacy without some form of security. Therefore, the establishment of certain safeguards or protections is required to protect information and privacy. Information security is most easily broken down into three areas that must be protected. These three areas are information Confidentiality, Integrity and Availability or **CIA**.

A. **Confidentiality** is the property that data or information is not made available or disclosed to unauthorized persons or processes

B. **Integrity** is the property that data or information has not been altered or destroyed in an unauthorized manner

C. **Availability** is the property that data or information is accessible and usable upon demand by an authorized person

The level of protection required to safeguard information CIA is determined through a process called "risk assessment". Risk assessments inventory what you have to protect, why you have to protect it and how well you are protecting it. Compliance with the safeguard and protection requirements is then achieved through integration of such into existing policies, systems, processes and functions, thereby incorporating security into existing business infrastructure.

6. **The Two-Key Rule**

To facilitate the implementation of the above protections, the "two-key rule" is used. In general, the two-key rule states that confidential, restricted or critical information must be protected by requiring that it takes two keys to access it. A key can be an actual physical key or a technical key such as requiring a user ID and password. A key can also be a policy that requires the continual presence of a staff member who escorts patients to and from care areas, etc. Using this basic rule of thumb will help staff understand how to protect information and systems.

7. **INFORMATION SECURITY CLASSIFICATION**

Information, as hereinafter defined, in all its forms and throughout its life cycle will be protected in a manner consistent with its <u>sensitivity</u> and <u>criticality</u> (value) to ARMC and its support functions, research activities, educational and instructional programs, and health care delivery services. This protection includes an appropriate level of physical and electronic security for the networks, facilities, equipment and software used to process, store, and transmit information. Generally, all ARMC information and systems require some level of protection.

Information used in conducting ARMC business requires that adequate controls protect that information from accidental or deliberate disclosure, damage, misuse, or loss. Users must have a business “need-to-know” and authorization prior to being allowed to access information. Users have the responsibility to inspect and classify all information and follow the guidelines for that classification. Further, all systems, as defined below, must be classified in order to apply appropriate security measures which are consistent with the information it contains.

Information classification is used to promote proper controls for safeguarding information. The classification assigned and the related controls applied are dependent on the sensitivity of the information. Information should be classified according to the most sensitive detail it includes. The content of the information, not its format, is the basis of classification. Formats may include paper, electronic, audio, video, or graphics.

Information belongs in a classification depending on the extent of possible damage or assumed liability or risk resulting from unauthorized access or loss of the information’s confidentiality, integrity or availability.

8. **The following categories are to be used to classify information.**

A. **ORGANIZATIONAL**

Organizational information represents data that is generally considered public. It is accessible in read-only status to maintain its integrity. Access to organizational information is available only to authorized users.

Examples of information in the ORGANIZATIONAL classification

- library resources
- materials protected by copyright laws
- phone directories and information made available to the public by ARMC

B. **INTERNAL**

Information in this classification is restricted to staff of ARMC. It cannot be used in reports distributed to people outside of ARMC without the issuer’s authorization. When used in internal reports or memorandums, it may be labeled “INTERNAL USE ONLY” (IUO will suffice for brevity). Any information not specifically labeled but identifiable as belonging to ARMC should be treated at least as IUO unless it clearly falls into the ORGANIZATIONAL category.

Examples of information in the INTERNAL classification

- Personnel policy manual.
- Computer reports of files containing daily activity which do not contain individually identifiable staff or patient information.

C. **CONFIDENTIAL**

Information in this category must be limited to those with a need to know and the appropriate “clearance” as given by management. It must be securely handled and never left where unauthorized persons might see it. If contained in written reports, the distribution of the reports must be controlled. The word “CONFIDENTIAL” should be stamped or written on the envelope used for distribution. When discarded, it must be shredded or placed in secure shred containers.

Examples of information in the CONFIDENTIAL classification:

- Employee performance reviews and contents of personnel files.

- Computer reports or files containing patient information.
- Strategic plans for ARMC.

D. **RESTRICTED**

This type of information is only available to selected individuals of ARMC. Only the originator can determine who is privileged to see this information. All recipients must have specific authorization from the originator before distributing it to others. Handle with extreme care.

Restricted information represents very important and highly sensitive material that must be held confidential by law or ethical practice. Unauthorized disclosure, modification, capture, or destruction of this information could cause serious harm to employees, non-employee practitioners, clinics, or patients.

Examples of information in the RESTRICTED classification:

- Court case material.
- Consultant's analysis and recommendation.
- Medical Staff organization proceedings.
- Case review and peer review documents.

9. **HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) REQUIREMENTS**

To understand the requirements of the HIPAA Security Rule, it is helpful to be familiar with the basic security terminology it uses to describe the security measures. By understanding the requirements and the terminology in the HIPAA Security Rule, it becomes easier to see how ARMC policies and procedures work.

Each security measure of the HIPAA Security Rule can be categorized as being an administrative, physical, or technical safeguard.

- **Administrative Safeguards** are defined as the administrative actions, policies, and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

- **Physical Safeguards** are defined as the security measures to protect information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

- **Technical Safeguards** are defined as the technology and policies and procedures for its use that protect information and control access to it.

These safeguards, as defined by the HIPAA Security Rule, require the establishment of policies, procedures and processes in order to comply with the standards. These policies must interact well as to not cause confusion or conflict with one another. **A chart at the end of this document shows the interaction or "links" between such policies as created for ARMC in order to prevent conflicts or redundancy when creating or complying with ARMC security policy requirements.**

A. **Hybrid Entities**

A "hybrid entity", as defined in the HIPAA Privacy and Security Rules, is a "single legal entity, whose business activities include both covered and non-covered functions," which designates one or more "health care components" in writing. The County is a hybrid entity under HIPAA and as such has designated certain departments of the County as its covered healthcare component (See County Policy 10-04 and 10-04 SP1 for more information). A health care component is that part or parts of a hybrid entity that performs covered functions involving the use or disclosure of protected health information ("PHI"). A hybrid entity is responsible for ensuring that its health care components do not use or disclose PHI for purposes other than its covered functions unless such use or disclosure would be permitted by a covered entity. A hybrid entity is also responsible for the health care component's compliance with the requirements of the Security Rule. Compliance with these provisions generally requires identification of personnel and facilities involved in the covered functions of a designated health care component, and creating a policy and procedural "firewall" separating it from other elements of the hybrid entity.

B. **Organized Health Care Arrangements (OHCA)**

An OHCA, as defined in the HIPAA Privacy and Security Rules, exists as a matter of fact, and does not require any regulatory filing, election, or agreement. When an OHCA exists, the parties may, but need not agree to be covered by a joint notice of privacy practices. Since all parties must abide by the terms of the joint notice, an OHCA agreement (or bylaws or other binding policy document, where appropriate) is recommended to clarify rights and obligations of the OHCA participants. The management of an OHCA may have important implications for Security Rule compliance. In "integrated" or "organized system" settings in particular, such as ARMC, different legal entities share access to and use of the facilities, equipment and information. It is important to understand that all contracted health care providers and medical groups/corporations of ARMC agree to abide by these policies as a prerequisite of participation in the ARMC's OHCA. **OHCA participants further agree to accept application of ARMC's sanction policies to their personnel for violations of ARMC privacy and security policies. (OHCA members are listed on the back page of the ARMC Notice of Privacy Practices.)**

10. **ENFORCEMENT**

Information systems/Applications may be removed, uninstalled, locked or disconnected from the ARMC network/computing systems and appropriate disciplinary action taken for failure to comply with this and related privacy & security policies.

A. **Monitoring**

Information technology and systems usage will be monitored by authorized staff to support and enforce protection of all information and assets of ARMC. Monitoring may be performed by use of the audit capabilities built in to the operating systems, in-house developed programs, purchased software, random audits and investigations.

B. **Unauthorized Use**

Unauthorized use includes but is not limited to: unauthorized personal use; possession and retention of ARMC files outside of the scope of individual job responsibilities; installation of computer games or programs that are used to bypass security measures; unauthorized access to, copying, removing, or disclosing of ARMC files, programs or information; authoring or forwarding "chain" e-mail messages; use of another user's identification badge/user id or password; unauthorized possession of ARMC information; installation of unauthorized software; modifying the configuration of installed PC hardware by adding cards, boards, modems, peripherals, or attachments without prior authorization of the Information Management Department; connecting to and/or using any computer or related equipment/software for the purposes of "hacking" into or bypassing any security measures of ARMC or another entity or failing to log off or "lock" a computer workstation or terminal prior to leaving it unattended. Serious misuses involving possible termination may require review by representatives of County Counsel, Security, Human Resources, and department management (or management of persons providing services to ARMC).

C. **Disciplinary Action**

Failure of employees, medical groups, departments, volunteers, students and system and data users to safeguard information and assets as defined in this policy, HIPAA Privacy and Security Regulations [45 CFR 160 – 164] and other state and federal laws may subject the individual(s) to disciplinary action up to and including termination of employment or contract or expulsion from training programs.

Refer to policy 700.04 Information Access Management for access termination requirements.

11. **Policy Exception Requests**

If a department manager/system owner finds that it is impractical (financially or otherwise) to secure its confidential or restricted information as outlined in the ARMC privacy and/or security policies, then an exception request must be submitted to the Hospital Privacy & Security Officer detailing (1) which policy areas cannot be complied with, (2) the reasons why the policy requirements cannot be met, and (3) the alternative measures to be taken to adequately secure the confidential or restricted information, system or area. The Hospital Privacy & Security Officer or his/her designee is responsible for approving/denying such measures.

12. **POLICY RESPONSIBILITIES**

A. **System/Application Owners/Department Managers/Chairpersons**

All policies related to information security must be reviewed at least annually or upon any breach or suspected breach of privacy or security and revised if necessary.

Department-specific policies must be reviewed, compared to the Standard Practice Security policies and created or modified to comply. Such policies will be submitted to the Hospital Privacy & Security Officer for review and approval prior to implementation.

B. **Supervisors/Managers**

Supervisors must ensure that workforce members and system/information users are held responsible for protecting ARMC information and complying with policies, standards, and procedures governing its use.

Managers are responsible to correctly identify systems and resources and any security weaknesses/vulnerabilities in those systems, including insecure workforce member behavior, pursue reasonable actions to correct violations and report outcomes as necessary to management (this includes sanctioning workforce members for privacy and/or security violations after training staff on appropriate security responsibilities). Documentation of enforcement must be maintained for 6 years from occurrence.

Managers/Supervisors who fail to enforce this policy will be reported to their appropriate Associate Administrator for appropriate disciplinary action.

C. **All Workforce Members (including management and others granted access to information or assets)**

Preventing unauthorized access to computer systems and/or information must be of utmost concern to all workforce members. All workforce members and those granted access to ARMC information resources must:

1) Create and maintain information in a secure, protected environment. (This includes protecting information in paper and electronic form by locking or logging off computer workstations when leaving unattended, locking doors that control access to areas where confidential information is stored, etc.)
2) Secure all information assets and systems whether in physical (paper, etc.), oral or electronic format, stored on any medium or in any system or area.
3) Use the access control system(s) provided (e.g. user ID's & passwords, badge access control system, keys, etc.) appropriately to protect information created, stored or transmitted from loss, theft, corruption or unauthorized disclosure.
4) Ensure integrity & accuracy of information by following proper data integrity procedures. (e.g. backing up data, using antivirus software, ensuring accurate data input, never installing unauthorized software, etc.)
5) Promptly report any incidents or suspicious activity in an area or on any computer system.
6) Maintain compliance with all established information safeguards as required as a condition of continuous employment.

D. **Additionally all staff must ensure that:**

1) Medical charts are secured at all times. (Charts are not left on counters or in unsecured areas.)
2) Computers are locked/ logged off when unattended; screens not viewable by unauthorized persons.
3) Printed documents are secured from inappropriate access (printouts not left on printers, faxes or copiers).
4) Patient and confidential information is disposed of in locked shred containers only (confidential or restricted information is not placed in "recycle" bins).
5) Patient identifying information is never included in emails unless the appropriate safeguards are in place. (See Standard Practice Policy 700.15 Transmission Security.)
6) Interoffice mail containing confidential or restricted information is sealed and marked confidential prior to sending.
7) Identity & authority of persons requesting access to patient information is verified prior to allowing access.
8) Patient and confidential information is not left in conference rooms or training sessions and only the minimum necessary confidential or restricted information is used when meeting minutes or training require confidential or restricted information to be included in such documents.

9) Devices capable of text messaging or wireless communication or data transfer (e.g. alphanumeric pagers, blackberry devices, PDA's and other handheld/mobile information technology devices) are not used to send or receive confidential or restricted information unless proper access control mechanisms are in place and approved by the Hospital Privacy & Security Officer.

REFERENCES: Administrative Operations Policies:

700.02 Security Management & Evaluation Process
700.03 Workforce Security Requirements
700.04 Information Access Management
700.05 Security Awareness and Training
700.06 Security Incident Procedures
700.07 Contingency Planning
700.08 Physical Security Access Controls
700.09 Workstation Use and Security
700.10 Device and Media Controls
700.11 Access Control
700.12 Audit Controls
700.13 Data Integrity
700.14 Person or Entity Authentication
700.15 Transmission Security

County Policies 10-04 and 10-04 SP1

DEFINITIONS: **Workforce -** Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for ARMC, is under the direct control of ARMC, whether or not they are paid.

ATTACHMENTS: **Attachment 1: ARMC Security Policy Interaction Chart**

APPROVAL DATE: **5/22/08 Administration**
5/22/08 Executive Committee

REPLACES: **Administrative Policy No. 700.01 Issue 1**

EFFECTIVE: **5/26/05** **REVISED**: **04/28/08**

REVEIWED: **N/A**

ARROWHEAD REGIONAL MEDICAL CENTER
Administrative Policies and Procedures

SECTION: **COMPLIANCE** **SUB SECTION:** **GENERAL**

SUBJECT: **USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION**

APPROVED BY: ____
Chief Executive Officer

_

POLICY

It is the policy of Arrowhead Regional Medical Center (ARMC) that an individual's identifiable protected health information (PHI) may only be used within the Medical Center or disclosed to entities outside the Medical Center after notification to and/or with the expressed permission of the patient, except in cases of emergency or where specifically permitted or required by law. Such use and disclosures are also subject to the minimum necessary information. Access to health information stored in any ARMC file or depository, stored electronically, or that exists in any recording device or in any clinical or research data base, collectively hereafter referred to as the "medical record", is limited to those who have a valid business or medical need for the information or otherwise have a right or appropriate need to know the information. With the exception of purposes related to treatment, access to an individual's protected health information or the use or disclosure of an individual's protected health information must, to the extent practicable, be limited to only the minimum necessary to accomplish the intended purpose of the approved use, disclosure or request.

For purposes of compliance with the Health Insurance Portability and Accountability Act (HIPAA), employee records and student records subject to the Family Educational Rights and Privacy Act (FERPA) are specifically excluded from the definition of "medical record".

AMPLIFICATION

The purpose of this policy is to assure that individually identifiable protected health information contained in any ARMC medical record or otherwise stored or held in the possession of ARMC is only used or disclosed for its intended purpose and in accordance with general and/or specific patient notifications, permissions, or authorizations except where permitted or required by law.

PROCEDURES

An individual's protected health information (PHI) may be used by ARMC for treatment, payment, and healthcare operations (routine purposes), after ARMC has provided to the individual its Notice of Privacy Practices and has made a good faith effort to obtain an acknowledgment of its receipt. Additionally, ARMC may use an individual's health information for other (non-routine) purposes or may disclose an individual's health information to external entities for non-routine purposes upon obtaining a valid authorization from the individual giving permission for that stated use or disclosure. Further, ARMC may use and disclose an individual's protected health information without prior permission or authorization where the protected health information has been sufficiently "de-identified", so that it does not identify the individual(s), is part of a "limited data set", or for other uses where allowable by statute. Where authorization is required, the requirement to obtain authorization may only be waived by the Medical Center's Institutional Review Board (IRB) after final approval of the Chief Compliance Officer.

EMERGENCY USE AND DISCLOSURE

Protected health information (PHI) may be used or disclosed without a patient's acknowledgment of receipt of the Notice of Privacy Practices in the event of an emergency or where a communications barrier makes prior permission or notification impossible. ARMC health professionals may, at their discretion, use or disclose an individual's protected health information without prior notification of privacy practices or without acknowledgment where providing or obtaining such would compromise patient care (e.g. emergency situations)

TREATMENT, PAYMENT AND OTHER HEALTHCARE OPERATIONS USE

From time to time, ARMC may disclose identifiable protected health information to other entities for use by the entities for treatment. Further, ARMC may disclose identifiable protected health information to other entities to assist the recipient in obtaining payment and, under limited circumstances, may disclose identifiable health information to other entities for purposes associated with healthcare operations.

MINIMUM NECESSARY RESTRICTIONS

Protected health information may only be accessed, used or disclosed by authorized personnel. With the exception of the use and disclosure of health information directly related to treatment and to the extent practicable, access to protected health information by ARMC staff or other authorized personnel is restricted to the minimum necessary to execute their job responsibilities. (See Minimum Necessary Restrictions policy)

RESPONSIBILITIES

It is the responsibility of each department to identify those persons or classes of persons who are authorized to access, use or disclose protected health information and specifically to identify to what health information they may have access and the reasons why. This list must be kept current at all times and a copy of the list must be provided to the Privacy & Security Officer upon request. Departments will maintain historical records pertaining to such lists for documentation purposes and is subject to audit.

REVOCATION

Physical access to controlled areas and user accounts/badges that provide access to protected health information are to be revoked upon the termination of an employee, student, or trainee or when others, such as contractors and vendors, no longer require access. All protected health information in the possession of these individuals or entities is to be returned to ARMC or an attestation provided that such information has been destroyed, or, if that is not possible due to the nature of an on-going research effort, a statement attesting that the information will remain confidential and safeguarded as long as it is in the possession of the third party.

DISCIPLINARY ACTION

The unauthorized access to or unauthorized use or disclosure of protected health information in any form may subject the responsible employee, resident, volunteer, student, or trainee to disciplinary action up to and including termination of employment/contract or suspension or expulsion from a student or trainee program. This extends to the unauthorized use or disclosure of health information that is obtained in any way (including the receipt of oral communications of PHI) during the course of business or health information that is otherwise learned or secured by any person affiliated with or in the employ of ARMC.

REPORTING

Departments that become aware of the unauthorized use or disclosure of protected health information that causes or reasonably could cause harm should immediately report the incident to the Medical Center Privacy & Security Officer. To the extent practicable, ARMC will attempt to minimize the known harmful effects and/or correct known instances of harm.

TRAINING

All ARMC employees who may use, disclose, or have access to identifiable protected health information contained in any medical record must, as a condition of continued employment, complete an approved training program that outlines employee responsibility and patient rights under the statutory privacy regulations contained in the Health Insurance Portability and Accountability Act (HIPAA) or otherwise demonstrate knowledge of their responsibilities as outlined in the HIPAA regulations and Medical Center Standard Practice Policies. Additionally, all students or trainees who may use, disclose, or have access to any protected health information contained in any medical record must complete an approved training program or otherwise demonstrate an understanding of their obligations under HIPAA and Medical Center policy.

BUSINESS ASSOCIATES

ARMC will, from time to time, disclose identifiable protected health information to business associates who have been contracted with to provide a service or function for the Medical Center. Protected health information provided to a business associate must be pursuant to an assurance that the business associate, and its sub-contractors, will use the information only for the purpose(s) intended, will restrict access to the information on a “need to know” basis only, and will otherwise take appropriate measures to safeguard the information in its possession. There will be a valid, signed business associate agreement/contract in place before identifiable protected health information may be provided.

PRIVACY NOTICE

Except to the extent that patient care might be compromised, the use or disclosure of protected health information must comply with the Medical Center approved and published ARMC Notice of Privacy Practices. In addition, except to the extent that patient care might be compromised, the use and disclosure of an individual’s protected health information must comply with any restrictions requested and subsequently agreed to by ARMC. Therefore, it is the policy of Arrowhead Regional Medical Center not to agree to any such restrictions. An individual, however, maintains the right to request such restrictions.

BUSINESS ASSOCIATE REQUESTS FOR ACCESS, USE OR DISCLOSURE OF PHI

All requests for access, use or disclosure of protected health information by entities wishing to engage in a contracted business relationship with the Medical Center must be submitted using the form(s) designated by the Medical Center. Such requests will be submitted to the Chief Compliance Office for approval. No identifiable protected health information will be accessed, used or disclosed prior to approval of such request. Requests/Contracts are subject to further evaluation at any time and all accesses, uses or disclosures subject to the request may be revoked for failure to comply with medical center requirements.

REFERENCES: **Privacy Rule Requirements 164.502, 164.508, 164.512 and 164.520**
ARMC Administrative Policy & Procedure Manual, Sections 700, 800 and 1000

DEFINITIONS: **N/A**

ATTACHMENTS: **Attachment 1: PHI Access Request Form - Business Associates**

APPROVAL DATE: **5/26/05 Administration**
5/26/05 Executive Committee

REPLACES: **Standard Practice Policy 1009.05 Issue 1**

EFFECTIVE: **5/26/05** **REVISED**: **N/A**

REVIEWED: **N/A**

Acknowledgment Form

I have received and read the HIPAA & California State Patient Confidentiality Laws Staff Training document and ARMC policies 700.01 and 1000.07. I understand that I must protect patient information in all forms at all times. I understand that disciplinary action may be imposed upon me for failing to comply with Medical Center policies. Failure to protect health information or computer access, or inappropriately accessing, using or disclosing protected health information may subject me to disciplinary action, up to and including termination of employment or contract or expulsion from training programs.

I agree to safeguard patient information in any form or medium at all times and to comply with all administrative and department specific policies related to compliance with the Health Insurance Portability and Accountability Act (HIPAA) privacy and security regulations and applicable state laws.

I will refrain from accessing patient information out of curiosity or without a valid business need-to-know and understand that such access is a violation of law and must be reported to the state and the patient in certain circumstances.

Signature: ______________________________________ Date: ____________

Name (Print):____

Position Title: _______________________________ Department: ______________