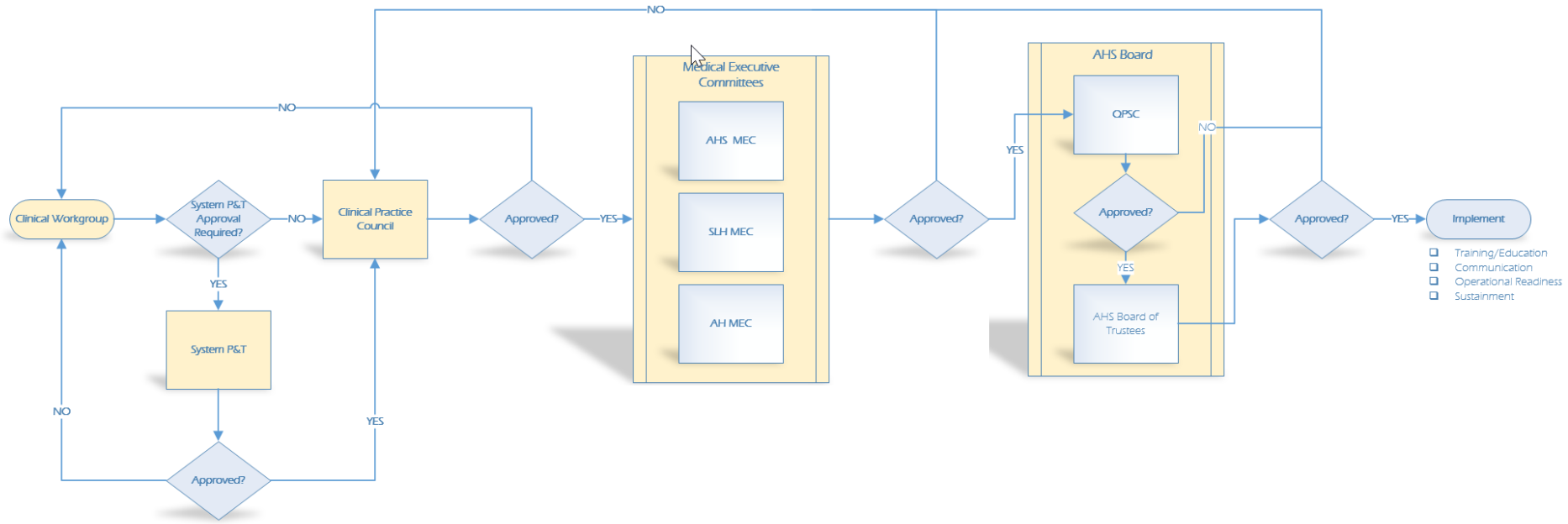
Policy Approval Workflow



*__Clinical Workgroup__ broadly includes any medical staff committee, nursing committee such as Patient Care Leadership Team, administrative committee, and/or other ad hoc workgroups.

CPC Executive Summary BOT October 2020

Alameda Health System Policies and Procedures				CPC Executive Summary to Medical Executive Committee September 2020	Chair: Dr. Felicia Tornabene and Janet McInnes	
TOPIC or TITLE OF POLICY	**Last Approved Date**	**Next review date after BOT approval**	**Document Owners**	**Purpose**	**Summary of Changes**	**History of Review Committee**
AHS System Wide Policies & Procedures						
Communication Guidelines for Patient Care	New Policy	11/2023	Theresa Cooper, Vice President, Patient Care Services	Alameda Health System is committed to providing safe patient care through timely and effective communication. All staff members shall be expected to use standardized communication processes such as SBAR to communicate patient related issues consistently, thoroughly, and within defined timeframes.	• New Policy • Purpose and policy statement require separation • Page 3, Item f.: Change Assistant CMO to CMO • Start emphasizing using the SBAR process, even when verbal for consistent communication (not requiring additional comments within policy on completing SBAR)	• Departmental: 09/2020 • CPC: 09/2020 • MEC: 09/2020
Information System Access	New Policy	11/2023	E'Jaaz Ali, Chief Information Security Officer	To safeguard the confidentiality, integrity, and availability of protected health information (PHI), business and proprietary information within its information systems by controlling access to these systems/ applications.	• Replaces HR: Section 3.00 – Policy 3.14 Use of AHS Telephones, Mail Systems and HR: Section 3.00 – Policy 3.15 Use of Computer Systems	• Departmental: 09/2020 • CPC: 09/2020 • MEC: 09/2020
Information System Activity Review	New Policy	11/2023	E'Jaaz Ali, Chief Information Security Officer	This policy outlines how to ensure appropriate safeguards are in place to safeguard the confidentiality, integrity, and availability of patient health information by reviewing logs of access and activity against applications, systems, network, and users.	• New policy • Defines what OCR looks for with Activity review • Compliance requirements for employee review	• Departmental: 09/2020 • CPC: 09/2020 • MEC: 09/2020
Prevention of Unplanned Retained Procedure Items	08/2018	11/2023	Theresa Cooper, Vice President, Patient Care Services	To outline surgical team responsibilities for accounting for all sponges, sharps, instruments and miscellaneous items, on all procedures; to protect the patient from undue harm related to unplanned retained items.	• Updates for triennial review • Includes ○ Active pause and verification count process ○ Procedure when count is off	• Departmental: 09/2020 • CPC: 09/2020 • MEC: 09/2020

Alameda Health System Policies and Procedures				CPC Executive Summary to Medical Executive Committee September 2020	Chair: Dr. Felicia Tornabene and Janet McInnes	
TOPIC or TITLE OF POLICY	**Last Approved Date**	**Next review date after BOT approval**	**Document Owners**	**Purpose**	**Summary of Changes**	**History of Review Committee**
Release of Patient Information Complying with ONC Final Rule Policy	New Policy	11/2023	Rick Kibler, Vice President, Compliance and Internal Audit	The purpose of the Release of Patient Information: Complying with ONC (Office of National Coordinator for Health Information Technology) Final Rule Policy is to provide guidance to Alameda Health System (AHS) workforce members on how requests for patient medical information and test results will be released to patients.	• New policy • Focuses specifically on what can/can't be released to the patient; how and when	• Departmental: 09/2020 • CPC: 09/2020 • MEC: 09/2020
Risk Management Policy	New Policy	11/2023	E'Jaaz Ali, Chief Information Security Officer	This policy establishes the scope, objectives, and procedures of Alameda Health System's (AHS) information security risk management process. The risk management process is intended to support and protect the organization and its ability to fulfill its mission.	• New policy • Procedures as to how to assess and manage risk and conduct annual risk assessments	• Departmental: 09/2020 • CPC: 09/2020 • MEC: 09/2020
Utilization Review Policy	10/2017	11/2023	Sheila Lyzwa, Vice President, Care Management	To establish processing guidelines and timelines for member and provider notification of organizational determinations. The purpose of this policy is to provide standardized utilization review processes, follow regulatory guidelines, accreditation standards and payer contracts for patients admitted as inpatient or placed in outpatient observation status.	• Reviewed all processes around approach to admitting patients • Policy & procedure integral to medical staff utilization review committee • Rick Kibler to work with Sheila on policy statement and other edits	• Departmental: 09/2020 • CPC: 09/2020 • MEC: 09/2020
Highland Hospital Policies & Procedures						
Immune Globulin (IVIG) Intravenous Administration in the Special Care Nursery	10/2019	11/2023	Christine Delgado, Clinical Nurse V, Labor and Delivery; Karen Meyer, Clinical Nurse Specialist	Comments: Vote not required – Routing back as departmental procedural document Approval: Rejection:	• Revised policy • Sent to P&T; Is departmental only • Determined only needs P&T and not CPC approval • Don't need procedure for every medication	• Departmental: 09/2020 • Pharmacy and Therapeutics: 09/2020 • CPC: 09/2020 • MEC: 09/2020
San Leandro Hospital Policies & Procedures						
None	N/A	N/A	N/A	N/A	• N/A	• N/A
John George Psychiatric Hospital Policies & Procedures						
None	N/A	N/A	N/A	N/A	• N/A	• N/A

Alamedа Health System				CPC Executive Summary to Medical Executive Committee		
Policies and Procedures				**September 2020**	**Chair: Dr. Felicia Tornabene and Janet McInnes**	
TOPIC or TITLE OF POLICY	**Last Approved Date**	**Next review date after BOT approval**	**Document Owners**	**Purpose**	**Summary of Changes**	**History of Review Committee**
Alameda Hospital Policies & Procedures						
None	N/A	N/A	N/A	N/A	• N/A	• N/A

AHS System Policies COMBINED

ALAMEDA HEALTH SYSTEM

COMMUNICATION GUIDELINES FOR PATIENT CARE

Department	Nursing, Patient Care	***Effective Date***	09/2020
Campus	AHS System	***Date Revised***	09/2020
Category	Clinical	***Next Scheduled Review***	11/2023
Document Owner	Vice President, Patient Care Services	***Executive Responsible***	Chief Administrative Officer/Chief Nurse Executive

Printed copies are for reference only. Please refer to electronic copy for the latest version.

POLICY

Alameda Health System is committed to providing safe patient care. The 'Communication Guidelines for Patient Care represents a channel of communication process through which patient related issues should be directed. All staff members shall be expected to invoke this procedure in furtherance of patient's safety and AHS mission, values, and goals.

The policy delineates a mechanism to notify the responsible provider of a patients change on condition, concerns or questions, with guidance on the appropriate mode of communication based upon relative urgency. It also provides the structure and support for healthcare providers to assure patient care needs are met in a timely manner.

COMMUNICATION CONTENT

Clearly identify the patient care issues to be resolved.

1. Ensure that all pertinent information is conveyed using the SBAR format.

2. SBAR is a communication tool used to standardize discussion among caregivers to ensure that critical information about a patient's status is communicated effectively. The communication tools recommended to be used are Secure Chat and Text Page.

S- SITUATION	Identify the situation as Routine, Urgent or Emergent and communicate it in text format. This should be followed by patient identification details.
B – BACKGROUND	State the patient care concern. Only the relevant circumstances to the situation.
A – ASSESSMENT	Analysis and consideration of the options – What do you think the problem is? Be specific.
R- RECOMMENDATION	Action you request. To be done/ordered/what will correct the problem?

HEALTH CARE ISSUES

1. ***Routine issues***

   Definition: Issues/concerns which may be reasonably addressed with an appropriate outcome within a 2 hour period.

Mode of communication: Secure Chat a function in EPIC is the preferred mode of communication.

Procedure: Utilizing the SBAR format send a message on Secure Chat including all members on the primary patient care team ie. Intern, Resident and Attending. The issue is expected to be addressed by any member on the team within a 2-hour period. If no response within the 2-hour timeframe, text page the intern and follow the procedure outlined under '*Urgent Issues*".

Documentation: Clinical documentation indicated as appropriate.

2. ***Urgent Issues***
Definition: Issues/concerns that require expedited attention requiring an appropriate outcome within a 20 minute time period. It also includes 'Routine Issues' which have not been adequately resolved become urgent issues.

Mode of Communication: Text page is the appropriate mode of communication. Please note 'Secure Chat' is not an acceptable mode of communication for 'Urgent issues'.

Procedure: Notify responsible intern via text page giving them 5 minutes to respond. If no response, repeat the text page giving them another 5 minutes. If still no response then text page the Resident. If a total of 20 minutes have elapsed without an appropriate outcome then text page the Attending and inform the Charge Nurse. Anytime during this waiting period if the patients status deteriorates or becomes unstable, please text page the Attending and follow the procedure outlined under 'Emergent Issues'.

Documentation: Clinical documentation is required (see Documentation requirements below). Complete an Occurrence report for any instance of failure to timely or inadequate response.

3. ***Emergency Issues***
Definition: Issues/concerns that require immediate attention requiring an appropriate response within 5 minutes.

Mode of Communication: Text page is an acceptable mode of communication. Please include 911 in the beginning of your text page. 'Secure Chat' is not an acceptable mode of communication.

Prodecure: Notify the responsible Attending and Charge Nurse. Notifying the Rapid Response Team as needed. Please refer to the 'Code Blue Policy' for further guidelines.

Documentation: Clinical documentation is required (see Documentation requirements below). Complete an Occurrence report for any instance of failure to timely or inadequate response.

ESCALATION PROTOCOL

The procedures outlined above must be followed to invoke the chain of command before taking an issue to the next level of authority and any subsequent authority levels thereafter. If the issue/concern remains unresolved, move up the Chain of Command until the issue is resolved.

Take the issue from the authority figure closest to the event and move up the organization's chain of command, as the situation warrants (see attached for each facility):

a. Charge Nurse
b. Department Manager/Supervisor
c. House Supervisor
d. Director of Unit (if applicable)
e. VP of Patient Care Services/ Administrator on Duty
f. Assistant CMO

This document is meant to serve as a Guideline for communication channels however when patient safety is a concern, alternate channels are expected as appropriate. As a part of this document, we will not be collecting data unless requested.

DOCUMENTATION

a. Required for all urgent/emergent issues.
b. The date, time, name of person contacted, information provided, and orders received and/or actions implemented should be documented in the medical record. Relevant additional information should be documented as well.
c. Documentation should be done factually and objectively. Do not criticize other professionals in the medical record.

APPROVALS

		System	Alameda	AHS/Highland/John George/San Leandro
Department	**Date:**	N/A	09/2020	09/2020
Pharmacy and Therapeutics (P&T)	**Date:**	N/A	N/A	N/A
Clinical Practice Council (CPC)	**Date:**		N/A	N/A
Medical Executive Committee	**Date:**	N/A		
Board of Trustees	**Date:**		N/A	N/A

Information System Access Policy

ALAMEDA HEALTH SYSTEM

INFORMATION SYSTEM ACCESS POLICY

Department	Information Security	***Effective Date***	09/2020
Campus	AHS System	***Date Revised***	09/2020
Category	Administrative	***Next Scheduled Review***	11/2023
Document Owner	Chief Information Security Officer	***Executive Responsible***	Chief Information Officer

Printed copies are for reference only. Please refer to electronic copy for the latest version.

PURPOSE

To safeguard the confidentiality, integrity, and availability of protected health information (PHI), business and proprietary information within its information systems by controlling access to these systems/applications. Access to information systems by workforce members is allowable only on a minimum necessary basis. The same levels of confidentiality that exist for hard copy PHI, business, and proprietary information apply to digital and/or electronic protected health information (ePHI) within the organization's information systems and are extended even after termination or other conclusion of access. These safeguards have been established to address the HIPAA Security regulations.

DEFINITION

Protected Health Information (PHI) includes but is not limited to any and all individually identifiable information about the physical or mental health condition or treatment of any individual, including but not limited to: any identifying information about a patient, such as a patient's name or a photo or video of the patient; any information about a patient's health condition or medication; and any information about payment for a patient's care and services.

Workforce members include employees, contracted/temporary staff, students, volunteers, medical staff and individuals representing or working at AHS.

POLICY

Management is responsible for determining the level of access required for workforce members under their supervision, based upon the minimum necessary information needed to accomplish their function. Management is also responsible for promptly notifying Information Systems of any changes in roles or termination of workforce members.

PROCEDURE:

1. **ACCESS ESTABLISHMENT AND MODIFICATION**
    A. All requests for access to any of the organization's information systems and applications must be accompanied with an "Information System Logon Request" (ISLR) form (Appendix 1) approved by the requestor's immediate supervisor

B. For employees, the "Confidentiality and Security Agreement" (Appendix 2) is a required item of New Employee Orientation and must be completed as part of the ISLR request. This is done by Human Resources.
C. For non-employees, the "Confidentiality and Security Agreement" is a required item of on-boarding. The immediate supervisor of the non-employee is responsible for ensuring the "Confidential and Security Agreement is completed and sent to the Service Desk as part of the ISLR request.
D. Access will not be granted until signed "Confidentiality and Security Agreement" and "ISLR" forms are received, reviewed, and additional approval is obtained if required.
E. Access for users on a contract or a student must have an end date established on the "ISLR" form. Any changes to the end date will be notified to the IT Department and/or Service Desk by immediate supervisor of the user and the immediate supervisor will also notify the correct Department (Human Resources, Contracting Office, and Medical Staff Office) of the contract change.
F. The end date will only be extended if the Department (Human Resources, Contracting Office, and Medical Staff Office) approve the contract extension.
G. Training related to security, confidentiality, and incident reporting must occur before log in credentials are issued.
H. The "ISLR" forms are maintained by the IT Department's Service Desk.

2. WORKFORCE TRANSFERS

A. The Human Resources Department is responsible for notifying the Service Desk of approved employees transferred into a new department or new role. The Service Desk will create a ticket to track this change.
B. The workforce members outgoing manager will inform the Service Desk what access should be terminated from an Active Directory perspective. The outgoing manager will ensure all local accounts are terminated upon transfer of the employee.
C. The new manager of the transferred workforce member is required to complete a new "ISLR" form and forward it to the Service Desk.
D. The Service Desk is responsible for changing the user's access to information systems based on the user's new role within five business days of notification. For employees, the Service Desk will close the ticket once this work is done
E. For non-employees the Service Desk will transfer the ticket to the Information Security Office to evaluate any changes in risk with the transfer and new access
F. Once evaluation is complete the Information Security Office will close the ticket

3. **WORKFORCE CLEARANCE PROCEDURES**

A. The level of security assigned to a user to the organization's information systems is based on the minimum necessary information (amount of data) access required to carry out legitimate job responsibilities assigned to a user's job classification and/or to a user needing access to carry out treatment, payment, or healthcare operations.
B. All access requests are processed to provide the necessary level of access while also adhering to the minimum necessary requirements of the Privacy Rule.

Blanket access is not provided for any user.

C. Any access not specifically authorized is prohibited.

4. **ACCESS AUTHORIZATION**
   A. Role based access categories for each information system/application are pre-approved by Human Resources and Information Security Office.
   B. Categories are defined by the importance of the applications running on the information system, the value or sensitivity of the ePHI on the information system, security controls on the information system, security controls on the workstation utilized to access the information system, the specific activity of the user or workstation (e.g. Department, activity, shift, floor, employee-specific responsibilities) and the extent to which the information system is connected to other information systems. Any access must be based on the minimum necessary information needed for the user's role.
   C. The Service Desk grants the level of access to users based on these pre-determined categories.

5. **PERSON OR ENTITY AUTHENTICATION**
   A. Each user has and uses a unique User Login ID and password that identifies and authenticates him/her as the user of the information system.
   B. No user shall enter a shared "generic" user login id or password to authenticate onto an information system without the written consent of the Chief Information Security Officer (CISO)

6. **UNIQUE USER IDENTIFICATION**
   A. Access to the organization's information systems/applications is controlled by requiring a unique User Login ID and password for each authorized user.
   B. Password requirements should be based on current industry standards whenever possible (for example 8 character minimum with upper- and lower-case letters, numbers, and symbol).
   C. When typing their passwords, users will have their passwords replaced with asterisks "*" or other characters when typed. To ensure the correct password is typed, users can display their actual passwords (if the feature is available), for a max of 3 seconds, only when no one can see or screenshot the password.
   D. Users cannot select passwords that may be easily guessed or obtained using personal information (i.e., names, favorite sports team, etc.)
   E. The IS Department assigns a User Login ID and generic password for each user to utilize for first time access into each information system. The User Login ID and password are forwarded to the user securely (e.g., in a sealed envelope, personal communication, separate emails, etc.).
   F. Each information system shall automatically require users to change their password upon first-time use of the information system.

7. **PASSWORD MANAGEMENT**
    A. User Login IDs and passwords are used to control access to the organization's information systems and should not be disclosed to anyone.
    B. If an employee is terminated and a supervisor needs access to employee shared files or emails, the supervisor will first need approval from HR. Once approval is given then the ServiceDesk will change the password of the terminated employee and send the password to the supervisor securely. Based on the Risk Analysis for the department, application, system or organization, multi-factor authentication (MFA) may be required.
    C. Users may not allow anyone for any reason to have access to any information system using another user's unique User Login ID and password, or in the case of MFA the token or other methodology, with the exception of IT support as outlined above.
    D. Each information system automatically requires users to change passwords at a pre-determined interval as determined by the organization, based on the criticality and sensitivity of the ePHI contained within the network, system, application, and/or database whenever possible.
    E. The information systems are programmed to deny user's ability to re-use the 10 prior passwords whenever possible.
    F. Users that do not recall their password may contact the Service Desk. The Service Desk provides the employee with a temporary, one-time use password which must be changed on first use.
    G. Passwords are inactivated upon an employee's termination (refer to the termination procedures in this policy).
    H. If a user believes their User Login ID has been compromised, they are required to immediately report the incident to the Service Desk and /or the Information Security Office.

8. **ACCESS TO INFORMATION SYSTEMS**
    A. Workstations
        i. Workstations are the property of organization and must always remain on the premises, unless prior authorization by the CISO or other designee has been granted for removal of workstations from the premises.
        ii. Workstations utilized off organization's premises are protected with security controls equivalent to or exceeding those for on-site workstations.
        iii. Workstations should only be used for authorized business purposes.
        iv. When possible, workstations should be placed in secure areas. Workstations in patient rooms or public areas must be logged off or locked when not in use. Users must take actions to prevent unauthorized viewing (e.g. privacy screens, minimizing sessions, closing laptops, positioning screens away from public view, and so on).
        v. All users are responsible for practicing precautions to protect the confidentiality, integrity, and availability of ePHI in the information systems at all times.

vi. Workstations may not be used to engage in any activity that is illegal or is in violation of the organization's Acceptable Use Policy
vii. Users may access and utilize workstations as assigned by their supervisor.
viii. Supervisors are responsible for monitoring use of workstations.
ix. All users must report unauthorized workstation use to the Information Security Office or Compliance Office.
x. The organization must install on all workstations anti-virus or NextGen end point protection software to prevent transmission of malicious software. This software should be installed to allow for regular and automatic updates. All workstations should have full-disk encryption.

B. Portable Devices
    i. Portable workstations (e.g. laptops, mobile devices etc.) are also subject to the same safeguards and protections. Portable workstations must be maintained in a safe and secure manner when transported. Any portable device including laptop computers that contains PHI must be encrypted.
    ii. Portable or removable media, such as USB flash drives, must be approved for use by the Information Security Office with respect to PHI or any other sensitive information. PHI or sensitive data portable or removable media are also subject to the same safeguards and protections as portable workstations.

C. Networks Devices
    i. AHS will implement a secured with a stateful packet inspection Firewall.
    ii. Network access is limited to legitimate and established connections. An established connection is return traffic in response to an application request submitted from within the secure network.
    iii. Firewall console and other management ports are appropriately secured or disabled and are located in a physically secure environment. Only authorized individuals shall be allowed access to firewall(s) at any time, and login should only be allowed from internal networks, and include multi-factor authentication.
    iv. Mechanisms to log failed access attempts are in place.
    v. The configuration of firewalls used to protect networks is maintained by the IS Department. All changes to firewall configuration shall be approved by the Information Security Office and presented by the requestor to the Change Advisory Board, and fully tested before implementation. A complete log of changes and approval should be maintained. Firewalls need to be maintained as staff change positions.

D. Server Devices
    i. Servers are located in a physically secure environment and are on a secure network with firewall protection.
    ii. The system administrator or root account is password protected.
    iii. A security patch and update procedure is established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.

iv. All unused or unnecessary services are disabled.

E. Remote Access
    i. Refer to the Remote Access Policy for further guidance.
    ii. Remote access, if approved, shall be accompanied by multi-factor authentication or a secure alternative approved by the CISO

9. **AUTOMATIC LOGOFF**
    A. Users are required to make information systems inaccessible by any other individual when unattended by the users (i.e., locking or logging off the systems; if the device is used only by a single individual with a unique log in, it may be locked).
    B. Users must log off information systems/applications at the end of their shift, or at the end of their need to use the system/application, whichever is sooner.
    C. Information systems should automatically log users off the systems after 10 minutes of inactivity. Shortened automatic log off times should be implemented for workstations located in public or high traffic areas or for portable devices.
    D. The CISO can approve exceptions to automatic log off requirements.

10. **TERMINATION PROCEDURES**
    A. The Human Resources Department, Medical Staff Office, and supervisors of terminated workforce members are required to notify the IT Department and/or the Service Desk upon completion and/or termination of access for users.
    B. Notification of termination should be accompanied by a complete "Termination Checklist"(Appendix 3) to determine all AHS assets are returned to the organization and all application logons are disabled.
    C. The IT Department/Service Desk will disable users' access rights immediately upon the listed termination date. Accounts will be in a disabled status for (90) days in case the workforce member returns to work. However, (91) days after the termination date, the disabled account will be deleted.
    D. The IS Department audits and may disable access of users that have not logged into organization's information systems/applications for a period of over thirty-three (33) days without a termination notice.
    E. For accounts that have been disabled for more than sixty-one (61) days without a termination notice, the ISO will contact the listed supervisor inquiring about the account. If no answer is received after thirty (30) days of first inquiry, the account will be deleted.

COMPLIANCE

Violation of this policy or procedures by workforce members may result in disciplinary action, up to and including termination of employment or termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.

REGULATORY REFERENCES:

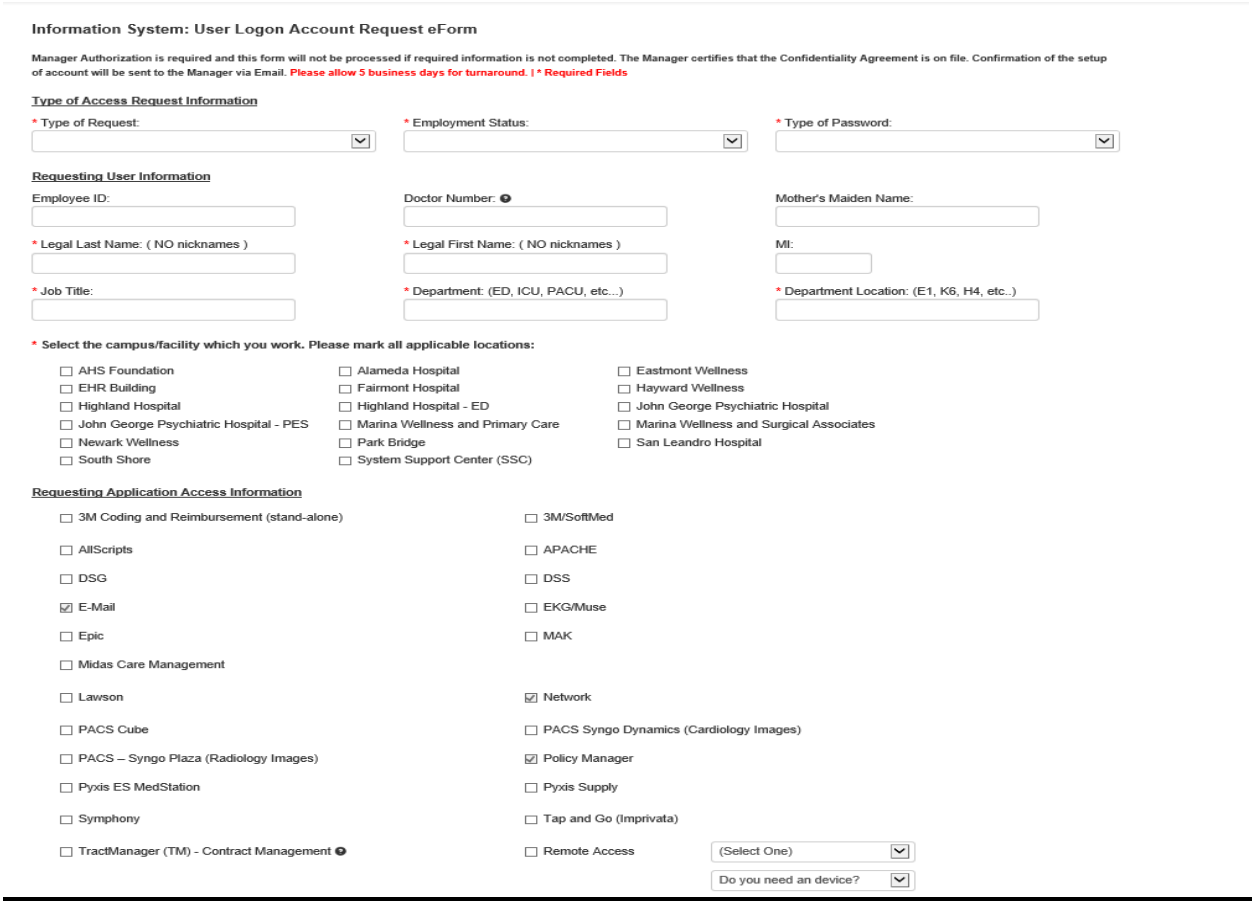
1. HIPAA REGULATORY REFERENCE
    A. 164.308(a)(3)(i)
    B. 164.308(a)(3)(ii)(A)
    C. 164.308(a)(3)(ii)(B)
    D. 164.308(a)(3)(ii)(C)
    E. 164.308(a)(4)(i)
    F. 164.308(a)(4)(ii)(C)
    G. 164.308(a)(5)(ii)(D)
    H. 164.310(b)
    I. 164.312(a)(1)
    J. 164.312(a)(2)(i)
    K. 164.312(a)(2)(iii)
    L. 164.312(d)

APPROVALS

		System	Alameda	AHS/Highland/John George/San Leandro
Department:	**Date:**		N/A	N/A
Pharmacy and Therapeutics (P&T)	**Date:**	N/A	N/A	N/A
Clinical Practice Council (CPC)	**Date:**		N/A	N/A
Medical Executive Committee	**Date:**		N/A	N/A
Board of Trustees	**Date:**		N/A	N/A

APPENDIX

Attachment 1



Information System: User Logon Account Request eForm

Manager Authorization is required and this form will not be processed if required information is not completed. The Manager certifies that the Confidentiality Agreement is on file. Confirmation of the setup of account will be sent to the Manager via Email. Please allow 5 business days for turnaround. | * Required Fields

Type of Access Request Information

* Type of Request:
* Employment Status:
* Type of Password:

Requesting User Information

Employee ID:
Doctor Number:
Mother's Maiden Name:
* Legal Last Name: (NO nicknames)
* Legal First Name: (NO nicknames)
MI:
* Job Title:
* Department: (ED, ICU, PACU, etc...)
* Department Location: (E1, K6, H4, etc..)

* Select the campus/facility which you work. Please mark all applicable locations:

- ☐ AHS Foundation
- ☐ EHR Building
- ☐ Highland Hospital
- ☐ John George Psychiatric Hospital - PES
- ☐ Newark Wellness
- ☐ South Shore
- ☐ Alameda Hospital
- ☐ Fairmont Hospital
- ☐ Highland Hospital - ED
- ☐ Marina Wellness and Primary Care
- ☐ Park Bridge
- ☐ System Support Center (SSC)
- ☐ Eastmont Wellness
- ☐ Hayward Wellness
- ☐ John George Psychiatric Hospital
- ☐ Marina Wellness and Surgical Associates
- ☐ San Leandro Hospital

Requesting Application Access Information

- ☐ 3M Coding and Reimbursement (stand-alone)
- ☐ 3M/SoftMed
- ☐ AllScripts
- ☐ APACHE
- ☐ DSG
- ☐ DSS
- ☑ E-Mail
- ☐ EKG/Muse
- ☐ Epic
- ☐ MAK
- ☐ Midas Care Management
- ☐ Lawson
- ☑ Network
- ☐ PACS Cube
- ☐ PACS Syngo Dynamics (Cardiology Images)
- ☐ PACS – Syngo Plaza (Radiology Images)
- ☑ Policy Manager
- ☐ Pyxis ES MedStation
- ☐ Pyxis Supply
- ☐ Symphony
- ☐ Tap and Go (Imprivata)
- ☐ TractManager (TM) - Contract Management
- ☐ Remote Access (Select One)
- Do you need an device?

Attachment 2

ALAMEDA HEALTH SYSTEM

Confidentiality and Security Agreement

This Agreement applies to all Alameda Health System (AHS) workforce members, including all providers and their office staff, employees, temporary and contract employees, volunteers and students. The purpose of this Agreement is to help you understand your obligation regarding privacy and security of confidential information.

As an individual working at AHS, you may have access to confidential information including patient, financial or business information obtained through your association with Alameda Health System. Confidential information is protected by State and Federal laws and by AHS policies.

Accordingly, as a condition of and in consideration of my access to confidential information, I acknowledge that:

1. I WILL ONLY access information I need to do my job.
2. I WILL NOT access my own records, the records of my family members, friends or co-workers except for assigned job-related duties.
3. I WILL NOT access, use, disclose, copy, release, sell, alter or destroy any confidential information, either electronic or paper unless it is part of my job.
4. I WILL NOT publish or disclose any confidential information to others using personal email or to any social media sites.
5. I WILL ONLY use my officially assigned user ID and password and never share or disclose it to anyone.
6. I ACCEPT responsibility for all activities undertaken using my user ID and/or password.
7. I UNDERSTAND my access to confidential information may be audited.
8. I WILL report any activities to my supervisor and AHS IT Department that I suspect may compromise the confidentiality, security and/or integrity of information. I understand these reports, made in good faith, will be held in confidence and there will be no retaliation, retribution or harassment for doing so.
9. I WILL protect the privacy of all information included in any AHS systems, and only access the minimum necessary information to complete the job.
10. I UNDERSTAND I have no ownership interest in any AHS information accessed or created by me during my relationship with AHS, including AHS equipment or devices, and will return them when no longer working at AHS.

By agreeing to this document, I acknowledge that I have read this Confidentiality and Security Agreement and I agree to comply with all the terms and conditions stated above. I further understand that I am responsible for any breach of confidentiality resulting from access made to any AHS systems using my User ID and Password, and may result in termination of my access, and/or loss of my privileges with AHS.

Attachment 3

AHS Off-Boarding

WEEK ONE CHECKLIST: *GET Off-Boarded*

Last Day_____

	TASK	How Too	Responsible Party
Employee Voluntary Exit			
o	Receive Employee resignation and accept on behalf of AHS	Review AHS voluntary termination process: Link	Manager
o	Ensure PAR is completed and Submitted	Complete PAR, effective date should be last day worked. This should be submitted to PARS e-mail address 2 weeks prior to last day.	Manager
o	Delivery of Final Check	Verify with payroll that final check is ready (if previous step does not occur this will not happen) collect the check from payroll the day of termination.	Manager
o	Final Meeting and delivery of Check	Establish the time with the employee. Ensure you deliver their check to them.	Manager
o	Gather assets	In the final meeting ask the employee for any laptop, phone, keys, badge and any other AHS property they may have.	Manager
o	Turn Off IT access	A termination report is provided to IT and security so they can disable network access for all terminated employees in a timely manner.	HR/IT
Contractor			
o	Establish final day of assignment or project	Establish prior or during the assignment	Manager
o	Ensure delivery of work assignment	Ensure agreed upon deliverables have been met and that you are satisfied with the work product.	Manager
o	Final Meeting	Meet with contractor and collect any laptops, phone, badges, keys and other AHS assets which may have been used during the assignment	Manager
o	Deactivate Badge	Notify security(Jeff Celestino) of the contractors exit date and time so the badge can be deactivated.	Manager
o	Deactivate IT access	http://acmc-intranetb/eform/logonrequest/	Manager

Information System Activity Review

ALAMEDA HEALTH SYSTEM

INFORMATION SYSTEMS ACTIVITY REVIEW

Department	Information Security	***Effective Date***	09/2020
Campus	AHS System	***Date Revised***	09/2020
Category	Administrative	***Next Scheduled Review***	11/2023
Document Owner	Chief Information Security Officer	***Executive Responsible***	Chief Information Officer

Printed copies are for reference only. Please refer to electronic copy for the latest version.

PURPOSE

This policy outlines how to ensure appropriate safeguards are in place to safeguard the confidentiality, integrity, and availability of patient health information by reviewing logs of access and activity against applications, systems, network, and users.

SCOPE

The Security Rule requires healthcare organizations to implement reasonable hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. It does not describe in detail the data that should be gathered in system logs or the length of time these must be kept. Review activities may be limited by application, system, and/or network reviewing capabilities and resources. AHS shall make reasonable and good-faith efforts to safeguard information privacy and security through a well-thought-out approach to reviewing of logs which is consistent with available resources.

DEFINITIONS

Protected Health Information (PHI) includes but is not limited to any and all individually identifiable information about the physical or mental health condition or treatment of any individual, including but not limited to: any identifying information about a patient, such as a patient's name or a photo or video of the patient; any information about a patient's health condition or medication; and any information about payment for a patient's care and services.

Workforce members include employees, contracted staff, students, volunteers, medical staff and any other individual representing or working at AHS.

Log Review: The internal process of reviewing information system access and activity (e.g., logins, file accesses, and security incidents). A review may be done as a periodic event, as a result of a patient complaint, or suspicion of employee wrongdoing. Review activities shall also take into consideration AHS' information system risk analysis results.

System Logs: Records of activity maintained by the system which provide:

1. date and time of activity;
2. origin of activity;
3. identification of user performing activity; and
4. description of attempted or completed activity.

Review Trail: A means to monitor information operations to determine if a security violation occurred by providing a chronological series of logged events (review logs) that relate to an operating system, an application, or user activities. Review trails provide:

1. Individual accountability for activities such as an unauthorized access of ePHI;
2. Reconstruction of an unusual occurrence of events such as an intrusion into the system to alter information;
3. Problem analysis such as an investigation into a slowdown in a system's performance, and
4. Other data as needed based on AHS objectives

*A review trail identifies **who** (login) did **what** (create, read, modify, delete, add, etc.) to **what** (data) and **when** (date, time).*

Trigger Event*:* Activities that may be indicative of a security breach that require further investigation (See Appendix).

POLICY STATEMENT

AHS shall review logs of access and activity of electronic protected health information (ePHI) applications, systems, and networks and address standards set forth by the HIPAA Security Rule to ensure compliance to safeguarding the privacy and security of ePHI.

PROCEDURE

1. GENERAL
    a. Responsibility for reviewing information system access and activity is assigned to the Information Security Office (ISO).
    b. The ISO's reviewing process shall address access and activity at the following levels listed below. Review process may address date and time of each log-on attempt, data and time of each log-off attempt, devices used, functions performed, etc.
        i. *User*: User level review trails generally monitor and log all commands directly initiated by the user, such as all identification and authentication attempts, and access attempts to files, patients, and resources.
        ii. *Application*: Application level review trails generally monitor and log user activities, including data files opened and closed, patients accessed, specific actions, and printing reports.
        iii. *System*: System level review trails generally monitor information on current operations, penetrations, and vulnerabilities

c. The ISO shall determine the systems or activities that will be tracked or reviewed by:
    i. Focusing efforts on area of greatest risk and vulnerability as identified in the Information Security's risk analysis and ongoing risk management process.
    ii. Maintaining confidentiality, integrity, and availability of ePHI applications and systems.
    iii. Assessing the appropriate scope of system reviews by determining; information/ePHI at risk, any processes which are vulnerable to unauthorized or inappropriate access, activities that should be monitored (create, read, update, delete = CRUD), and information to be included in the review record
    iv. Assessing available resources
d. ISO shall identify "trigger events" or criteria that raise awareness of questionable conditions of viewing of confidential information. The "events" may be applied to the entire organization or may be specific to a department, unit, or application.
e. ISO shall determine review criteria with a risk-based approach. This may include but is not limited to reviewing security risk analysis findings, past experience, current and projected future needs, and industry trends and events. The ISO will determine its ability to generate, review, and respond to review reports using internal resources. The ISO may determine that external resources are also appropriate.
f. The ISO shall designate the employees or contractors who are authorized to use security testing and monitoring tools. Such tools may not be used by anyone not specifically authorized. These tools may include, but are not limited to:
    i. Scanning tools and devices.
    ii. War driving software.
    iii. Password cracking utilities.
    iv. Network or wireless packet capture utilities.
    v. Passive and active intrusion detection systems.
    vi. Other devices as determined by the ISO.
g. Review documentation/reporting tools shall address, at a minimum, the following data elements:
    i. Authorizing official or policy, Application, System, Network, Department, and/or User Reviewed.
    ii. Review Type.
    iii. Individual/Department Responsible for Review.
    iv. Date(s) of Review.
    v. Reporting Responsibility/Structure for Review Results.
    vi. Conclusions.
    vii. Recommendations.
    viii. Actions.
    ix. Assignments.
    x. Follow-up.
h. The process for review of logs, trails, and reports shall include:
    i. Description of the activity as well as rationale for performing review.
    ii. Identification of which workforce members or department/unit will be responsible for review (workforce members should not review logs which

pertain to their own system activity unless there is no alternative or an inherent conflict of interest).

iii. Frequency of the reviewing process.

iv. Determination of significant events requiring further review and follow-up.

v. Identification of appropriate reporting channels for review of results and required follow-up.

1. VULNERABILITY TESTING AND PROTECTING AGAINST MALICIOUS SOFTWARE
    a. Vulnerability testing software will be used to probe the network by the ISO. This will be to identify what is running (e.g., operating system or product versions in place). Any validated vulnerabilities with a risk score of High to Critical should be corrected immediately
    b. Testing patches for vulnerabilities may be carried out internally or provided through an external third-party vendor. Testing patches shall be done on a monthly basis
    c. Tools to detect malicious software will be placed on every system. No workforce member is allowed to modify this setting. Any attempt to modify will be an audible event for log and review by the ISO

2. REVIEW REQUEST FOR SPECIFIC CAUSE
    a. A request may be made to review for a specific cause. The request may come from a variety of sources including, but not limited to, Human Resources, Chief Compliance Officer, Chief Information Officer, and Chief Information Security Officer.
    b. A request to review for specific cause must include time frame and nature of the request. The request must be reviewed and approved by The Compliance Officer or a Human Resource Business Partner.
    c. A request to review as a result of a patient concern shall be initiated by the Compliance Office. Should the review disclose that a workforce member has accessed a patient's PHI inappropriately, the information shall be shared with the workforce member's supervisor/and or Human Resources Department to determine appropriate sanction/corrective disciplinary action.

3. EVALUATION AND REPORTING OF REVIEW FINDINGS
    a. System logs that are routinely gathered must be reviewed in a timely manner.
    b. Report of review of results shall be limited on a minimum necessary/need to know basis. Review of results may be disclosed as deemed necessary. If this is the case, Legal counsel shall be consulted.
    c. The reporting process allows for meaningful communication of the review findings to the appropriate departments/units.
    d. Significant findings shall be reported immediately in a written format.
    e. Routine findings shall be reported to the sponsoring leadership structure in a written report format.
    f. Whenever indicated through evaluation and reporting, appropriate corrective actions must be undertaken. These actions shall be documented and shared with the responsible and sponsoring departments/units.

g. If criminal activity is discovered during a review, legal counsel will be notified immediately to take the right course of action.

4. REVIEWING BUSINESS ASSOCIATE AND/OR VENDOR ACCESS AND ACTIVITY
    a. Periodic monitoring of business associate and vendor information system activity should be carried out to ensure that access and activity is appropriate for privileges granted and necessary to the arrangement between AHS and the external agency.
    b. If it is determined that the business associate or vendor has exceeded the scope of access privileges, AHS must reassess the business relationship.
    c. If it is determined that a business associate has violated the terms of the HIPAA business associate agreement, AHS must take immediate action to remediate the situation. Continued violations may result in discontinuation of the business relationship.

5. REVIEW LOG SECURITY CONTROLS AND BACKUP
    a. Review logs shall be protected from unauthorized access or modification, so the information they contain will be available if needed to evaluate a security incident.
    b. Whenever possible, audit trail information is stored on a separate system. This is done to apply the security principle of "separation of duties" to protect audit trails from hackers. Audit trails maintained on a separate system would not be available to hackers who may break into the network and obtain system administrator privileges. A separate system would allow the ISO to identify hacking security incidents.
    c. Review logs maintained within an application shall be backed-up as part of the application's regular backup procedure. The ISO shall review internal back-up, storage and data recovery processes to ensure that the information is readily available in the manner required.

6. WORKFORCE TRAINING, EDUCATION, AWARENESS AND RESPONSIBILITIES
    a. AHS workforce members are provided training, education, and awareness on safeguarding the privacy and security of business and patient protected health information.
    b. AHS' commitment to reviewing access and activity of the information applications, systems, and networks is communicated through new employee orientation, ongoing training opportunities and events, and applicable policies.
    c. Workforce members are made aware of responsibilities with regard to privacy and security of information as well as applicable sanctions/corrective disciplinary actions should the reviewing process detect a workforce member's failure to comply with organizational policies.

7. EXTERNAL REVIEWS OF INFORMATION ACCESS AND ACTIVITY
    a. System review information and reports gathered from contracted external review firms, business associates and vendors shall be evaluated, and appropriate corrective action steps taken as indicated. Prior to contracting with an external review firm, the ISO shall:

i. Outline the review responsibility, authority, and accountability.
ii. Choose a review firm that is independent of other organizational operations.
iii. Ensure technical competence of the review firm staff.
iv. Require the review firm's adherence to applicable codes of professional ethics.
v. Obtain a signed HIPAA-compliant business associate agreement.
vi. Assign organizational responsibility for supervision of the external review firm.

8. RETENTION OF REVIEW INFORMATION
    a. Review logs and audit trail report information shall be maintained based on organizational needs. There is no standard or law addressing the retention of review log/trail information. Retention of this information shall be based on:
        i. Organizational history and experience.
        ii. Available storage space.
    b. Reports summarizing review activities shall be retained for a period of six years.

COMPLIANCE:

Violation of this policy or procedures by workforce members may result in disciplinary action, up to and including termination of employment or termination of the business relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.

REFERENCES

1. HIPAA REGULATORY REFERENCE
    a. 164.308(a)(1)(ii)(D)
    b. 164.308(a)(2)
    c. 164.308(a)(5)(ii)(B-C)
    d. 164.312(b)
    e. 164.312(c)(2)
    f. 164.312(e)(2)(i)

APPROVALS

		System	Alameda	AHS/Highland/John George/San Leandro
Department:	**Date:**	09/2020	N/A	N/A
Pharmacy and Therapeutics (P&T)	**Date:**	N/A	N/A	N/A
Clinical Practice Council (CPC)	**Date:**		N/A	N/A
Medical Executive Committee	**Date:**		N/A	N/A
Board of Trustees	**Date:**		N/A	N/A

APPENDIX 1: TRIGGER EVENTS

POTENTIAL TRIGGER EVENTS THAT MAY REQUIRE FURTHER INVESTIGATION/REVIEWING

Examples include:

- High risk or problem prone incidents or events.
- Patient and/or employee complaints.
- High profile patient/event (e.g., accident, homicide, assault, etc.).
- Requests by law enforcement or other outside agency with proper subpoena if applicable.
- Atypical patterns of activity.
- Failed authentication attempts.
- Users that have the same last name, address, or street name as in the patient file being viewed.
- VIPs encounters (board members, celebrities, governmental or community figures, authority figures, physician providers, management staff, or other highly publicized individuals).
- Patient files with no activity for XX days.
- Employees viewing other employee records.
- Diagnosis related (e.g., STD, HIV, pregnancy, AODA, mental health, etc.).
- Remote access use and activity.
- After-hours activity if applicable.
- Activity post termination.
- Department- or unit-specific circumstances – risk areas to be determined by individual departments/business units:

Prevention of Unplanned Retained Procedure Items v2

ALAMEDA HEALTH SYSTEM

PREVENTION OF UNPLANNED RETAINED PROCEDURE ITEMS

Department	Perioperative	***Effective Date***	02/2011
Campus	AHS System	***Date Revised***	08/2018, 08/2020
Category	Perioperative, Labor and Delivery	***Next Scheduled Review***	11/2023
Document Owner	Vice President, Patient Care Services	***Executive Responsible***	Chief Administrative Officer/Chief Nurse Executive

Printed copies are for reference only. Please refer to electronic copy for the latest version.

PURPOSE

To outline surgical team responsibilities for accounting for all sponges, sharps, instruments and miscellaneous items, on all procedures; to protect the patient from undue harm related to unplanned retained items.

DEFINITIONS

- *Sponges* – are linen items used to absorb fluids, protect tissues, and/or apply pressures or traction (i.e., gauze pads, cottonoids, peanuts, dissectors, laparotomy sponges).

- *Sharps* – include suture needles, scalpel blades, hypodermic needles, electrosurgical needles and blades, and safety pins.

- *Instruments* - are surgical tools or devices designed to perform a specific function such as cutting, dissecting, grasping, holding, retracting, or suturing.

- *Miscellaneous Items* – include ligaclip bars, vessel loops, umbilical and hernia tapes, vascular inserts, cautery scraper pads, trocar sealing caps, and any other small items that have the potential for being retained in a surgical wound.

POLICY

I. Every item that has the potential to unintentionally be left in the patient must be accounted for prior to completion of the procedure. Effective team communication and a standardized surgical count process will be utilized in all operative and other invasive procedures to prevent unintentional retention of a surgical item.
   - An ‘active pause’ and verification count process will be performed, to help foster team awareness and shared responsibility for prevention of retained surgical items (see section II. Effective Communication). Any member of the operative team is empowered to call for a surgical count if a discrepancy is suspected.

II. Effective Communication and actions among the surgical team:

- Before the procedure as part of the time out, the surgeon will remind the team that the patient or procedure is at risk for an unintended retained foreign object and that during the procedure, an active pause by the entire surgical team will occur for surgical count verifications and the final closing count verification.
- An active pause will be triggered by the surgical team announcing readiness for skin closure during which an accurate final count must be confirmed prior to completion of skin closure.

III. Sponges, instruments and other miscellaneous items will be counted on all procedures in which the possibility exists that they could be retained.

- Sharps will be counted on all procedures.

IV. Counting techniques are to be consistently performed, utilizing standardized processes, by all staff, in all procedures.

A. The RN Circulator keeps a running total of the counted items on the count board (with the exception of instruments) throughout the procedure. The instrument count status is maintained on the instrument count sheet.

1. The RN Circulator documents the initial count values on the count board / sheet.

2. Additional sponges, sharps, instruments, or miscellaneous items will be counted as they are added to the field; and added to the count total.

3. When adding items to the count board, place initials of individuals that passed items to the sterile field, next to the number of items added, in hypertext. (see below)

4. The running total on the count board should be in the format of: $5^{5\ ts}10^{5\ ts}15$; in which the first number is the beginning amount, the hypertext is the number of items added, and the next regular number is the new total of the item. More examples:
   - Raytec: $30^{10\ ts}40^{10\ ts}50$
   - Lap: $5^{5\ ts}10^{5\ ts}15$
   - Needle: $12^{8\ ts}20^{2\ ts}22$

B. The sequence and progression of the closing counts will be the same. The closing counts will be performed in the following sequence, per item type:

1. Incision site
2. Operative field
3. Mayo stand (or whichever table you are primarily working off)
4. Back table(s)
5. Unsterile field

C. Hanging count bags will be utilized for every procedure in which sponges are used and counted.
    1. The hanging bag should remain on the IV holder until the final accounting has occurred.
        a. If the IV pole becomes overloaded, the hanging bags may be taken down and placed in a clear plastic bag
        2. At the end of the procedure, every pocket, of every bag must be viewed by two individuals, one of which is an RN, to verify that all sponges are accounted for.

D. Surgeons should perform a methodical cavity/wound "sweep" prior to initiating wound closure, specifically to look for unplanned retained items.

E. Item specific standard processes:
    1. Suture needles:
        a. Are to be counted as one total group. (i.e. Do not total vascular suture needles separately from skin suture needles.)
        b. During the counts, unopened suture packages are counted according to the number marked on the outer package
            - Once the package is opened, the RN circulator and the scrub person must verify the number in the package matches what is expected.
        c. Matching needle packages to the count may be helpful to identify the type of needle that is missing, but this method **cannot** be utilized to indicate a correct count. The number of needles counted must match the total on the board, to be considered correct.
    2. All cottonoids are counted as one group.
    3. Lap sponges are grouped, and counted, by the size of the sponge.

V. Distractions, noise, and unnecessary interruptions should be minimized during the accounting process.
A. Factors that contribute to distractions should be minimized. (i.e.: telephones, wireless devices, wireless communication systems, paging systems, computers, music devices, etc,)
B. Circulator and scrub person should verify that the surgeon has everything needed to eliminate interruptions and delay surgery prior to initiating count.
C. Nothing should interrupt count, unless urgent need arises.
D. The Anesthesia professional will plan anesthetic milestone actions (e.g., emergence from anesthesia) so that these actions do not pressure the perioperative team to circumvent safe accounting practices.
E. The Anesthesia professional will not use counted items.

VI. The use of technology (i.e.: Radio Frequency or Code scanning), to assist with the accounting process, does not substitute for any portion of this standardized process.
1. The policy and process for use of such technology, if utilized, should also be standardized for all users of such technology; and that information should be within a policy specific to that technology and process.

VII. Timing and number of counts:

A. Counts will be performed at least three (3) times:

1. Initial Count: Prior to the beginning of the procedure to establish the baseline quantity.
2. Initial Closing count initiated before closure of first layer of tissue (i.e. fascia).
3. Final Closing count is completed prior to the end of skin closure.

B. Additional counts may be completed in the following circumstances:

1. Changing from less invasive procedures to open procedures (i.e. laparoscopic to open).
2. At the time of permanent relief of either the scrub person or the circulating nurse (although direct visualization of all sponges or sharps may not be possible.) The time and the count results will be documented on the Perioperative Record.
3. Before closure of a cavity within a cavity.
4. Before wound closure (at first layer of closure).
5. At any time requested by a member of the surgical team

C. Counts and events that require a count (i.e.: relief of the scrub person or RN circulator) should not be performed during critical phases of the procedure, including:

1. Time-out periods
2. Critical dissections
3. Confirming and opening of implants
4. Induction of and patient's emergence from anesthesia
5. Care and handling of specimens

IV. Items within multi-item packages, which are no longer contained within one sealed package upon transitioning to sterile field, will be counted when received on the sterile field, to verify the amount in the package matches the amount expected to be in the package.

A. If the count of the items does not match the amount that should be in the package, the items shall be handed off of the field and removed from the room; thus, not included in the count. i.e: A package of Raytec 4x4's with only nine in the package should not be utilized, as there should be ten in the package.

V. All counts are audibly and visually performed by the circulating RN and scrub person.

A. Both team members must see each item as it is counted aloud.
B. Items must be separated during the count process, so that each individual item is clearly identified. (i.e.: Sponges cannot be "fanned".)

VI. If a counted sharp is passed off or inadvertently drops from the sterile field, the circulating RN will retrieve it, show it to the scrub person, properly dispose of the sharp and account for it on the count board.

VII. The circulating nurse will compare the final counts to the totals of each item that has been recorded on the count board / sheet.

A. The outcome will be announced to the primary surgeon. (i.e. "All final counts are correct", "We are missing one lap sponge.")

1. The RN circulator should hear an acknowledgement from the surgeon that confirms comprehension of the results.

B. The types of counts (i.e., sponges, sharps, instruments, miscellaneous) and results of counts will be documented on the Perioperative Record.

C. The identity of the staff members performing the counts will be documented on the Perioperative Record.

VIII. All counted items will remain within the Operating Room until the patient has left the room:

A. Used linen and trash bags are never removed from the Operating Room before the end of the procedure.

B. No counted sponges will be sent with the specimen

IX. Radiographic detectable sponges will not be used for dressings.

X. Only radiographic detectable sponges are utilized during the procedure.

A. Dressing sponges are only opened onto the field after the final count has been completed.

B. Dressing sponges that are supplied pre-packaged within custom set-up packs are kept wrapped or bagged (however packaged in the custom pack),and segregated on the sterile field; until after the final count.

XI. When needed, only radiographic cloth towels will be placed into the incision.

A. Radiographic cloth towels will be a different color from the non-radiographic towels.

XII. Counted sponges are not to be altered in any way. Examples:

- The tails will not be removed from Lap sponges.
- The sponges may not be cut to make them smaller.
- The radiographic material may not be removed so that the sponge can be used as a dressing sponge.

XIII. If a non-sponge counted item is altered in any way, the item must be accounted for in its entirety. Examples:

- If a vessel loop is cut, compare the combined length of all pieces of that vessel loop to another identical vessel loop to verify that all portions were removed from the patient.
- If a needle breaks, verify that all pieces are recovered.
- If an instrument can be disassembled or breaks, account for all pieces of the instrument.

XIV. If an unplanned item, or part of an item, is deemed to be irretrievable, and surgeon concludes that it must be left in the patient, the following steps must be followed:

A. Situation should be documented on the Peri-operative record.
B. A Safety Alert should be completed and submitted.
C. Perioperative leadership should be notified as soon as possible.
D. Surgeon should disclose to the patient / family what was retained, and the rationale.

XV. When there is an incorrect count, the Charge Nurse and Attending surgeon is notified immediately.

A. If, after searching, the item is not found, and the count is still incorrect; then an intraoperative radiograph should be obtained.
   a. The requisition for intraoperative imaging should specify:
      i. That the exam is for an "*incorrect surgical count*".
      ii. What the missing item is, (i.e.: lap sponge, small needle, ribbon retractor, etc.) with description as appropriate.
      iii. The preferred technique and views. Intraoperative imaging should provide full coverage of the surgical site and should include any views deemed necessary by the surgeon to maximize the opportunity to identify a missing surgical item.
      iv. Radiological techniques may include:
         - use of portable or fixed radiographic equipment
         - portable anterior and posterior and oblique views
         - multiple images for full coverage of the surgical site or body cavity
         - confirmed by the surgeon
         - fluoroscopy
   b. Unless there is a risk to the patient's life, the intraoperative radiograph must be taken, and results reviewed before completion of the procedure. If the radiologist is not immediately available, the surgeon may interpret the image.
      i. "Completion of Procedure" is defined as actual completion of procedure, not when the patient leaves the Operating or procedure room. (i.e. last skin stitch has been applied.)

B. The Charge Nurse and the Perioperative Director are to confirm and communicate that OR policy has been followed and that additional X-rays are not needed. They will determine if the Administrator on call or Chief of Surgery should be notified immediately. If decision is made to not contact VP Of Patient Care Services and Chair of Surgery an email with details will be sent to them for information no later than end of day.
   i. If, after completion of the procedure, it is identified that there is an unplanned retained items, the event must be communicated to Risk Department immediately via phone call, (In addition to submitting a Safety alert.) and is a mandatory reporting event to regulatory agencies.
   ii. The results of the radiographic image and the physician that read the radiographic image will be documented in the medical record.

iii. If after completion of the procedure there are any unplanned retained surgical items, an immediate notification is made to the Regulatory Affairs Department via phone call to the System Director of Regulatory Affairs and an email to RegulatoryAffairs@alamedahealthsystem.org .

iv. A Safety Alert will be completed by the RN Circulator regarding the incorrect count that results in a radiographic exam.

C. All unresolved counts are marked as *incorrect* in the intraoperative record

D. If sponges are packed into a wound and intentionally left in post-operatively, the number of packed sponges must be documented on the Peri-operative record.

E. If the number of visible sponges, combined with the number of known packed sponges matches the total on the count board, the count is correct.
   1. The surgeon will inform the patient or patient's representative of any surgical soft goods purposely left in the wound at the end of the procedure and the plan for removing these items.
   2. The patient or patient's representative will be provided written information/ instructions regarding removal of materials and contact information for any issues that result.

F. Upon removal, the number of packed sponges removed will be documented in the patient record.

G. After removal of sponge a radiograph will be obtained until execution of Radio Frequency or Code Scanning devices are implemented.
   a. If removal occurs in a subsequent OR visit, the number of sponges removed should be documented in the Perioperative record of that visit.
      i. The removed sponges should also be added to the count total of that visit and accounted for at the end of the procedure.
   b. If removal occurs outside of the OR, the number of sponges removed should be documented in the documentation of the clinician that is performing the removal.

Responsible Person(s)/Dept.	*Procedure*
Scrub person, RN Circulator	Prior to preparing room for procedure, verify that all counted items from previous procedure are removed. Verify that count board is clear of any previous information.
Scrub person, RN Circulator	Perform initial count: count every item that has the potential to be left in the incision.
RN Circulator	Document beginning count totals in the appropriate spot (Instruments on the instrument count sheet; everything else on the dry erase count boards)
RN Circulator	Document that the initial count was performed and the staff that were involved.
Scrub person, RN Circulator	Count any additional items that are added to the sterile field during the procedure
RN Circulator	Accurately calculate the number of items added to the running total of each item utilizing the standard format.
Scrub Person	Be observant and help to verify that the number added to the count board is correct, and that the addition is accurate.
Scrub Person	During procedure, pass off the used lap sponges and 4x4 radiographic sponges, as soon as possible. Pass off cottonoids to circulator in a small basin or tray when no longer needed for the procedure. Keep all other items on the sterile field to count.
RN Circulator	Periodically throughout the procedure, place all lap sponges and 4x4 radiographic sponges into the hanging count bag. Place each sponge in a separate pocket on the hanging bag. Utilize a different hanging bag for each type of sponge. Fill the hanging count bag from left to right, working from the bottom of the bag to the top. Place the sponge so that the blue strip or tail is easily visible from the front.
RN Circulator	Place cottonoids on a flat, covered surface (cover with blue wrap from instrument pan, or something similar) that can be easily visualized by the scrub person, separate in groups of ten, per each style of cottonoid.

Responsible Person(s)/Dept.	*Procedure*
Scrub Person	At end of procedure, pass off all sponges to the circulator
RN Circulator	Place the remaining lap sponges and 4x4 radiographic sponges into the hanging count bags, as described above; so that every sponge can easily be seen and accounted for at the end of the procedure. Verify that there are no unexpected empty pockets in the count bags. The only empty pockets should be the remaining 5 pockets in a bag that only contains one set of five laps.
Scrub Person	Maintain awareness of sponges and items as they are placed into the incision and removed.
Scrub person, RN Circulator	Perform counts as dictated by the procedure and circumstances
RN Circulator	Document that each count was performed, the names of the staff involved, and the result of the count. (On relief counts, document the above in addition to the time of the count. This may be done in the nursing comments section of the procedure record, if need be.)
RN Circulator	Notify the surgeon of the results of the final counts and verify acknowledgement by the surgeon.
All team members	Allow uninterrupted time to perform a proper accounting of all items.
Surgeon	Perform a wound exam and sweep prior to closing. Visualize the sponge bags and verify that all pockets are filled as expected.
RN Circulator	Complete any needed radiology exam request for missing items with reason for exam, and the item that is missing.
RN Circulator	Complete a Safety Alert for each incorrect count that results in a Radiologic exam, to include the exam results, who read the exam, surgeon awareness, and final count results.

REFERENCES

1. AORN: Standards, Recommended Practice Guidelines, (2017) online edition.

2. The Joint Commission. *The Joint Commission Sentinel Event Alert, Issue 51: Preventing unintended retained foreign objects* (accessed July 20, 2020)

3. Association of Perioperative Nurses (2018). *AORN Guidelines for Perioperative Practices: Retained Surgical Items.* 367-413.

4. Hospital Council of Northern and Central California. (2014). *Surgical Safety: Preventing Retained Surgical Items Using the Sponge Accounting System (SAS).*

APPROVALS

		System	Alameda	AHS/Highland/John George/San Leandro
Department	**Date:**	08/2020	N/A	N/A
Pharmacy and Therapeutics (P&T)	**Date:**	N/A	N/A	N/A
Clinical Practice Council (CPC)	**Date:**		N/A	N/A
Medical Executive Committee	**Date:**	N/A		
Board of Trustees	**Date:**		N/A	N/A

Release of Patient Information Complying with ONC Final Rule Policy_BL

RELEASE OF PATIENT INFORMATION: COMPLYING WITH ONC FINAL RULE POLICY – PATIENT ACCESS

Department	Internal Audit and Compliance	***Effective Date***	08/2020
Campus	AHS System	***Date Revised***	08/2020
Category	Administrative	***Next Scheduled Review***	11/2023
Document Owner	Privacy and Regulatory Counsel	***Executive Responsible***	Vice President, Audit and Compliance

Printed copies are for reference only. Please refer to electronic copy for the latest version.

PURPOSE

The purpose of the Release of Patient Information: Complying with ONC (Office of National Coordinator for Health Information Technology) Final Rule Policy is to provide guidance to Alameda Health System (AHS) workforce members on how requests for patient medical information and test results will be released to patients. The "21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Final Rule" (the "ONC Final Rule") prohibits health providers, technology vendors, health information exchanges and health information networks from practices that inhibit the exchange, use, or access of electronic health information (EHI) [1]. There is inherent tension between the promotion of electronic information sharing in the ONC Final Rule and the strict standards under HIPAA and related state laws to safeguard the privacy and security of protected health information (PHI). Prior to the ONC Final Rule, providers could err on the side of caution when disclosing PHI, but now, permitted disclosures of EHI/PHI are required unless an exception applies.

POLICY

The ONC Final Rule promotes secure and more immediate access to health information for patients and helps ensure that patients can also electronically access their electronic health information at no cost. Thus, AHS will provide patients the right to access their medical information subject to narrow exceptions defined in both federal and state regulations.

[1] Per 45 § 171.102, "Electronic health information (EHI) means electronic protected health information as defined in 45 CFR 160.103 to the extent that it would be included in a designated record set as defined in 45 CFR 164.501, regardless of whether the group of records are used or maintained by or for a covered entity as defined in 45 CFR 160.103, but EHI shall not include: (1) Psychotherapy notes as defined in 45 CFR 164.501; or (2) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding."

BACKGROUND

Patients have a broad right to access their own medical information and records under both federal and California laws, subject to narrow exceptions even when it comes to mental health and sensitive test results. AHS require that patients submit requests for medical records (including physician notes and clinical lab results) in writing if they want to receive the records in electronic form. However, the ONC Final Rule establishes eight categories of exceptions that are deemed to not constitute informational blocking. These eight "safe harbors" are available at: https://www.healthit.gov/sites/default/files/cures/2020 03/InformationBlockingExceptions.pdf. One of them is the "Privacy Exception," which includes the circumstances where "if an actor is permitted to provide access, exchange, or use of EHI under a privacy law, then the actor should provide that access, exchange, or use. However, an actor should not be required to use or disclose EHI in a way that is prohibited under state or federal privacy laws."

Both the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA) and California's Confidentiality of Medical Information Act (CMIA), which provides stronger privacy protections for medical information than HIPAA, recognize that a patient has the right to access his or her own medical information. This right of patient access extends to physician notes, HIV, STD, genetic screening and other sensitive test results, and applies regardless of whether a test is positive or negative. However, there are differences in the preconditions that a provider can impose before sharing medical records with a patient, especially when shared in electronic form, and processes that must be followed under California law when sharing certain sensitive test results.

For example, Health and Safety Code § 123148(d) specifically provides that "[t]he electronic disclosure of test results under this section shall be in accordance with any applicable federal law governing privacy and security of electronic personal health records. However, any state statute that governs privacy and security of electronic personal health records, shall apply to test results under this section and shall prevail over federal law if federal law permits." Because the ONC Final Rule allows state law to preempt it, § 123148 remains the governing provision at this time. As such, these additional requirements and preconditions per state statute must be met before certain sensitive lab results can be disclosed electronically.

DEFINITION

Electronic Health Information (EHI) means electronic protected health information to the extent that it would be included in a designated record set, regardless of whether the group of records are used or maintained by or for a covered entity. EHI shall not include: (1) Psychotherapy notes; or (2) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

Protected Health Information (PHI) includes but is not limited to any and all individually identifiable information about the physical or mental health condition or treatment of any individual, including but not limited to: any identifying information about a patient, such as a patient's name or a photo or video of the patient; any information about a patient's health condition or medication; and any information about payment for a patient's care and services.

Workforce members include employees, contracted staff, students, volunteers, medical staff and any other individual representing or working at AHS.

PROCEDURE

1. **Test Results:**
    a. **Health and Safety Code § 123148 and Disclosing Clinical Lab Test Results**: Health and Safety Code § 123148 requires that a health care professional disclose clinical lab test results to a patient who is the subject of the tests if requested by the patient in oral or written form. Disclosure to the patient must also be in oral or written form and cannot be electronic unless electronic disclosure is (1) requested/consented by the patient and (2) deemed most appropriate by the health care professional who requested the test.
    b. AHS must obtain the consent of the patient in order to provide the patient's lab results through the internet or electronic means. The consent must meet the requirements of Civil Code § 56.10 or 56.11.
    c. The following sensitive test results cannot be disclosed to a patient electronically or via the internet unless (1) the patient requests the disclosure, (2) the health care professional deems this electronic disclosure as an appropriate means, and (3) a healthcare professional has first discussed in person, by telephone, or by any other means of oral communication, the test results with the patient:
        - HIV antibody test result, unless the test subject is anonymously tested and the internet posting follows other requirements that does not link to any patient-identifying information;
        - Presence of antigens indicating a hepatitis infection;
        - Abusing the use of drugs; and
        - Test results related to routinely processed tissues, including skin biopsies, Pap smear tests, products of conception, and bone marrow aspirations for morphological evaluation, *if they reveal a malignancy*.
    d. For HIV test results, California law imposes additional preconditions when disclosing the results to a patient. Per Health and Safety Code § 120990(h), after the HIV test result has been received by the provider, the medical care provider or the person who administers the test shall ensure that the patient receives timely information and counseling, as appropriate, to explain the results and the implications for the patient's health:
        - If the patient tests positive for HIV infection, the medical provider or the person who administers the test shall inform the patient that there are numerous treatment options available and identify follow up testing and

care that may be recommended, including contact information for medical and psychological services.

- If the patient tests negative for HIV infection and is determined to be at high risk for HIV infection by the medical provider or person administering the test, the medical provider or the person who administers the test shall advise the patient of the need for periodic retesting, explain the limitations of current testing technology and the current window period for verification of results, and provide information about methods that prevent or reduce the risk of contracting HIV, including, but not limited to, pre-exposure prophylaxis and post-exposure prophylaxis, consistent with guidance of the federal Centers for Disease Control and Prevention, and may offer prevention counseling or a referral to prevention counseling.

e. AHS has 2 categories when releasing test results electronically upon a patient's request and consent:
   - All test results not restricted by the above guidelines are released.
   - The above sensitive test results are restricted unless the requirements/preconditions of Health and Safety Code § 123148 have been met.

2. Patient Right of Access to Medical Information:

a. A patient's right to review, access and obtain copies of his or her medical information is reflected in the following provisions, among others:

45 CFR § 164.524

- (1) *Right of access.* Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set[2], for as long as the protected health information is maintained in the designated record set, except for:
  - (i) Psychotherapy notes[3]; and

[2]Per 45 CFR § 164.501, designated record set means:

(1) A group of records maintained by or for a covered entity that is:

(i) The medical records and billing records about individuals maintained by or for a covered health care provider;

(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.

(2) For purposes of this paragraph, 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 a covered entity.

[3]Per 45 CFR § 164.501, Psychotherapy notes means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished,

- (ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

Health & Safety Code § 123100

- The Legislature finds and declares that every person having ultimate responsibility for decisions respecting his or her own health care also possesses a concomitant right of access to complete information respecting his or her condition and care provided. Similarly, persons having responsibility for decisions respecting the health care of others should, in general, have access to information on the patient's condition and care. It is, therefore, the intent of the Legislature in enacting this chapter to establish procedures for providing access to health care records[4] or summaries of those records by patients and by those persons having responsibility for decisions respecting the health care of others.

42 CFR § 2.23

- (a) Patient access not prohibited. These regulations do not prohibit a part 2 program (substance abuse program) from giving a patient access to their own records, including the opportunity to inspect and copy any records that the part 2 program maintains about the patient. The part 2 program is not required to obtain a patient's written consent or other authorization under the regulations in this part in order to provide such access to the patient.

b. Under these federal and state regulations, a health care provider must disclose medical information to the patient if the patient requests it in accordance with the above regulations. This right of access is limited only in specific circumstances, such as for temporary research purposes, situations that would

results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

[4]Per HSC § 123105(d), "Patient records" means records in any form or medium maintained by, or in the custody or control of, a health care provider relating to the health history, diagnosis, or condition of a patient, or relating to treatment provided or proposed to be provided to the patient. "Patient records" includes only records pertaining to the patient requesting the records or whose representative requests the records. "Patient records" does not include information given in confidence to a health care provider by a person other than another health care provider or the patient, and that material may be removed from any records prior to inspection or copying under Section 123110 or 123115. "Patient records" does not include information contained in aggregate form, such as indices, registers, or logs.

endanger the life of self/another[5] or if the PHI makes reference to another person's PHI[6].

3. **Exceptions to the Right of Access**
    a. Both HIPAA and California laws contain exceptions to an individual's right of access to his or her health information. However, the exceptions included in HIPAA are different from those included in California law.
    b. **California Law:** provides a patient greater access to his or her medical records than does HIPAA. Thus, California law prevails over HIPAA's right to access provisions. California law states that a patient has the right to inspect and obtain a copy of all of his or her medical records with only two exceptions:
        i. Mental health records under specified circumstances (i.e. when a license health professional has determined, in the exercise of professional judgement, that the access requested is reasonably likely to endanger the life or physical safety of the patient).
        ii. Copies of X-rays or tracings derived from electrocardiography, electroencephalography, or electromyography need not be provided to the patient or patient's representative (although they must be permitted to review them), if the original X-rays or tracings are transmitted to another health care provider upon written request of the patient or patient's representative and within 15 days after receipt of the request.
        iii. California law does not permit the withholding of any other medical records from the patient.
    c. **HIPAA Exceptions**
        i. **Psychotherapy Notes:** HIPAA distinguishes between psychotherapy notes (which must be kept separate from the rest of the medical record) and other mental health records. California law does not treat psychotherapy notes differently from other mental health records.
        ii. HIPAA permits the outright denial of access to a patient's separately maintained psychotherapy notes, even if there is no potential harm to

[5]Per HSC § 123115(b), When a health care provider determines there is a substantial risk of significant adverse or detrimental consequences to a patient in seeing or receiving a copy of mental health records requested by the patient, the provider may decline to permit inspection or provide copies of the records to the patient, subject to the following conditions:

(1) The health care provider shall make a written record, to be included with the mental health records requested, noting the date of the request and explaining the health care provider's reason for refusing to permit inspection or provide copies of the records, including a description of the specific adverse or detrimental consequences to the patient that the provider anticipates would occur if inspection or copying were permitted.

(2) (A) The health care provider shall permit inspection by, or provide copies of the mental health records to, a licensed physician and surgeon, licensed psychologist, licensed marriage and family therapist, licensed clinical social worker, or licensed professional clinical counselor, designated by request of the patient.

[6]HIPAA permits a denial of access to that portion of any PHI that makes reference to another person (other than the provider) if a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such person.

the patient from seeing the notes. However, under state law, a health care provider may decline to permit inspection or provide copies of such records only if the provider determines there is a substantial risk of significant adverse or detrimental consequences to a patient in seeing or receiving a copy of mental health records.
    - Lanterman-Petris-Short (LPS) Act [Welfare and Institutions Code § 5328-5328.9] follows HIPAA standards as it relates to disclosure of mental health information to a patient that requests access to his or her information.

iii. Based on federal and state law differences, the **state standard is the one that must be used for denying access by a patient to his or her separately maintained psychotherapy notes.** If a provider refuses to permit inspection by, or to provide copies of the separately-maintained psychotherapy notes to, the patient, this state standard of harm must be met along with the requirements for denying access.

iv. A healthcare provider is not liable to the patient or any other person for any consequences that result from disclosure of patient records to the patient as required by California law (*see HSC § 123110(h)).*

4. **Denial of Right to Access**
    a. Federal and state regulations allow providers to deny a patient's request to access his or her information in specified circumstances as indicated above. Since denials are to be narrowly construed, the rule requires that providers give the patient access to any other PHI requested, after excluding PHI to which the provider has *lawful reason to deny access*.
    b. When a provider denies a patient access to Mental Health records the patient must be advised of their right to authorize release of those records to a third party (e.g., attorney, another provider).

5. **Process for Requesting Medical Records in General:** Under both HIPAA and California law, a health care provider can require that individuals make requests for access to medical records in writing, provided that the provider informs individuals of such a requirement. California law, which is stricter than HIPAA[7], requires that the provider allow the patient to inspect his/her medical record within 5 business days of making a written request. If the patient asks for copies of the records, the copies must be provided within 15 business days.
    a. **Disclosure of AHS Patient Medical Record:** AHS has a process to intake and respond to patient record requests in accordance with HIPAA, CMIA and related laws.
    b. Disclosure of AHS patient medical record, whether paper or electronic, may be given to the patient following the patient's written request and the above guidelines.

[7]Under HIPAA, once the covered entity receives the request for access, it must act on it (grant in whole or in part, deny, etc.) no later than 30 days after receipt, subject to one 30-day extension. But California law governs here because it is more stringent in favor of the patient.

6. **Minor's Medical Information:** A minor[8] patient or their legal representative can access or request copies of their records. Limited exceptions to this right exist. In general, whether the minor or the parent (or other legal representative) has the ability to access the medical record depends on who may legally consent to the treatment that the records relate to.
    a. If the minor has the authority to consent to medical treatment under state law, then the minor is generally the person authorized to have access to the records regarding the treatment, and to decide whether the records may be released to others (including the parent or other legal representative).
    b. Where a parent or other legal representative has the authority to consent to medical treatment for the minor, then the parent or other legal representative is generally the person authorized to have access to the minor's records regarding the treatment, and to decide whether the records may be released to others. However, a provider may deny a parent or other legal representative access to the minor's records, even though the parent or other legal representative had the authority to consent to the treatment, if the provider determines that access to the records would have a detrimental effect on the provider's professional relationship with the minor patient, or the minor's physical safety or psychological well-being.
        i. NOTE: There are several situations in which the minor has the legal authority to consent to medical treatment, but the provider is authorized, or required, to provide specified information to the parents. These situations involve self-sufficient minors, minor victims of sexual assault, minors receiving outpatient mental health treatment or residential shelter services, and minors receiving substance use disorder treatment where the care is *not* provided in a federally-assisted substance abuse program.
            1. However, HIPAA allows a provider to refuse access to a parent or legal representative if the provider makes a good faith determination that the minor's physical safety or psychological well-being would be harmed as a result, the parent(s) or guardian committed the sexual assault on the minor, or the disclosure would be inappropriate.
    c. "Mixed" Medical Record: A minor's medical record may contain information regarding treatment that the minor may consent to, and information regarding treatment that the parent or other legal representative must consent to. In such cases, the health care provider should take extra care to ensure that records are released appropriately.

[8] Emancipated minor may review his/her own chart and may restrict access to his/her own record by parent or guardian. Sensitive services to a minor allow a minor to restrict access to his/her record by parent or guardian.

REFERENCES

42 CFR § 2.23
45 CFR § 164.524
Civil Code § 56.10 and 56.11
Health and Safety Code § 120990(h)
Health & Safety Code § 123100
Health & Safety Code § 123115(b)
Health and Safety Code § 123148(d)
Welfare and Institutions Code § 5328-5328.9

APPROVALS

		System	Alameda	AHS/Highland/John George/San Leandro
Department	**Date:**	N/A	08/2020	08/2020
Pharmacy and Therapeutics (P&T)	**Date:**	N/A	N/A	N/A
Clinical Practice Council (CPC)	**Date:**		N/A	N/A
Medical Executive Committee	**Date:**		N/A	N/A
Board of Trustees	**Date:**		N/A	N/A

Release of Patient Information Complying with ONC Final Rule

RELEASE OF PATIENT INFORMATION: COMPLYING WITH ONC FINAL RULE POLICY – PATIENT ACCESS

Department	Internal Audit and Compliance	***Effective Date***	08/2020
Campus	AHS System	***Date Revised***	08/2020
Category	Administrative	***Next Scheduled Review***	11/2023
Document Owner	Privacy and Regulatory Counsel	***Executive Responsible***	Vice President, Audit and Compliance

Printed copies are for reference only. Please refer to electronic copy for the latest version.

PURPOSE

The purpose of the Release of Patient Information: Complying with ONC Final Rule Policy is to provide guidance to Alameda Health System (AHS) workforce members on how requests for patient medical information and test results will be released to patients. The "21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Final Rule" (the "ONC Final Rule") prohibits health providers, technology vendors, health information exchanges and health information networks from practices that inhibit the exchange, use, or access of electronic health information (EHI) [1]. There is inherent tension between the promotion of electronic information sharing in the ONC Final Rule and the strict standards under HIPAA and related state laws to safeguard the privacy and security of protected health information (PHI). Prior to the ONC Final Rule, providers could err on the side of caution when disclosing PHI, but now, permitted disclosures of EHI/PHI are required unless an exception applies.

POLICY

The ONC Final Rule promotes secure and more immediate access to health information for patients and helps ensure that patients can also electronically access their electronic health information at no cost. Thus, AHS will provide patients the right to access their medical information subject to narrow exceptions defined in both federal and state regulations.

[1] Per 45 § 171.102, "Electronic health information (EHI) means electronic protected health information as defined in 45 CFR 160.103 to the extent that it would be included in a designated record set as defined in 45 CFR 164.501, regardless of whether the group of records are used or maintained by or for a covered entity as defined in 45 CFR 160.103, but EHI shall not include: (1) Psychotherapy notes as defined in 45 CFR 164.501; or (2) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding."

BACKGROUND

Patients have a broad right to access their own medical information and records under both federal and California laws, subject to narrow exceptions even when it comes to mental health and sensitive test results. AHS require that patients submit requests for medical records (including physician notes and clinical lab results) in writing if they want to receive the records in electronic form. However, the ONC Final Rule establishes eight categories of exceptions that are deemed to not constitute informational blocking. These eight "safe harbors" are available at: https://www.healthit.gov/sites/default/files/cures/2020 03/InformationBlockingExceptions.pdf. One of them is the "Privacy Exception," which includes the circumstances where "if an actor is permitted to provide access, exchange, or use of EHI under a privacy law, then the actor should provide that access, exchange, or use. However, an actor should not be required to use or disclose EHI in a way that is prohibited under state or federal privacy laws."

Both the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA) and California's Confidentiality of Medical Information Act (CMIA), which provides stronger privacy protections for medical information than HIPAA, recognize that a patient has the right to access his or her own medical information. This right of patient access extends to physician notes, HIV, STD, genetic screening and other sensitive test results, and applies regardless of whether a test is positive or negative. However, there are differences in the preconditions that a provider can impose before sharing medical records with a patient, especially when shared in electronic form, and processes that must be followed under California law when sharing certain sensitive test results.

For example, Health and Safety Code § 123148(d) specifically provides that "[t]he electronic disclosure of test results under this section shall be in accordance with any applicable federal law governing privacy and security of electronic personal health records. However, any state statute that governs privacy and security of electronic personal health records, shall apply to test results under this section and shall prevail over federal law if federal law permits." Because the ONC Final Rule allows state law to preempt it, § 123148 remains the governing provision at this time. As such, these additional requirements and preconditions per state statute must be met before certain sensitive lab results can be disclosed electronically.

DEFINITION

Electronic Health Information (EHI) means electronic protected health information to the extent that it would be included in a designated record set, regardless of whether the group of records are used or maintained by or for a covered entity. EHI shall not include: (1) Psychotherapy notes; or (2) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

Protected Health Information (PHI) includes but is not limited to any and all individually identifiable information about the physical or mental health condition or treatment of any individual, including but not limited to: any identifying information about a patient, such as a patient's name or a photo or video of the patient; any information about a patient's health condition or medication; and any information about payment for a patient's care and services.

Workforce members include employees, contracted staff, students, volunteers, medical staff and any other individual representing or working at AHS.

PROCEDURE

1. **Test Results:**
    a. **Health and Safety Code § 123148 and Disclosing Clinical Lab Test Results**: Health and Safety Code § 123148 requires that a health care professional disclose clinical lab test results to a patient who is the subject of the tests if requested by the patient in oral or written form. Disclosure to the patient must also be in oral or written form and cannot be electronic unless electronic disclosure is (1) requested/consented by the patient and (2) deemed most appropriate by the health care professional who requested the test.
    b. AHS must obtain the consent of the patient in order to provide the patient's lab results through the internet or electronic means. The consent must meet the requirements of Civil Code § 56.10 or 56.11.
    c. The following sensitive test results cannot be disclosed to a patient electronically or via the internet unless (1) the patient requests the disclosure, (2) the health care professional deems this electronic disclosure as an appropriate means, and (3) a healthcare professional has first discussed in person, by telephone, or by any other means of oral communication, the test results with the patient:
        - HIV antibody test result, unless the test subject is anonymously tested and the internet posting follows other requirements that does not link to any patient-identifying information;
        - Presence of antigens indicating a hepatitis infection;
        - Abusing the use of drugs; and
        - Test results related to routinely processed tissues, including skin biopsies, Pap smear tests, products of conception, and bone marrow aspirations for morphological evaluation, *if they reveal a malignancy*.
    d. For HIV test results, California law imposes additional preconditions when disclosing the results to a patient. Per Health and Safety Code § 120990(h), after the HIV test result has been received by the provider, the medical care provider or the person who administers the test shall ensure that the patient receives timely information and counseling, as appropriate, to explain the results and the implications for the patient's health:
        - If the patient tests positive for HIV infection, the medical provider or the person who administers the test shall inform the patient that there are numerous treatment options available and identify follow up testing and

care that may be recommended, including contact information for medical and psychological services.

- If the patient tests negative for HIV infection and is determined to be at high risk for HIV infection by the medical provider or person administering the test, the medical provider or the person who administers the test shall advise the patient of the need for periodic retesting, explain the limitations of current testing technology and the current window period for verification of results, and provide information about methods that prevent or reduce the risk of contracting HIV, including, but not limited to, pre-exposure prophylaxis and post-exposure prophylaxis, consistent with guidance of the federal Centers for Disease Control and Prevention, and may offer prevention counseling or a referral to prevention counseling.

e. AHS has 2 categories when releasing test results electronically upon a patient's request and consent:
   - All test results not restricted by the above guidelines are released.
   - The above sensitive test results are restricted unless the requirements/preconditions of Health and Safety Code § 123148 have been met.

2. Patient Right of Access to Medical Information:

a. A patient's right to review, access and obtain copies of his or her medical information is reflected in the following provisions, among others:

45 CFR § 164.524

- (1) *Right of access.* Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set[2], for as long as the protected health information is maintained in the designated record set, except for:
  - (i) Psychotherapy notes[3]; and

[2]Per 45 CFR § 164.501, designated record set means:

(1) A group of records maintained by or for a covered entity that is:

(i) The medical records and billing records about individuals maintained by or for a covered health care provider;

(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.

(2) For purposes of this paragraph, 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 a covered entity.

[3]Per 45 CFR § 164.501, Psychotherapy notes means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished,

- (ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

Health & Safety Code § 123100

- The Legislature finds and declares that every person having ultimate responsibility for decisions respecting his or her own health care also possesses a concomitant right of access to complete information respecting his or her condition and care provided. Similarly, persons having responsibility for decisions respecting the health care of others should, in general, have access to information on the patient's condition and care. It is, therefore, the intent of the Legislature in enacting this chapter to establish procedures for providing access to health care records[4] or summaries of those records by patients and by those persons having responsibility for decisions respecting the health care of others.

42 CFR § 2.23

- (a) Patient access not prohibited. These regulations do not prohibit a part 2 program (substance abuse program) from giving a patient access to their own records, including the opportunity to inspect and copy any records that the part 2 program maintains about the patient. The part 2 program is not required to obtain a patient's written consent or other authorization under the regulations in this part in order to provide such access to the patient.

b. Under these federal and state regulations, a health care provider must disclose medical information to the patient if the patient requests it in accordance with the above regulations. This right of access is limited only in specific circumstances, such as for temporary research purposes, situations that would

results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

[4]Per HSC § 123105(d), "Patient records" means records in any form or medium maintained by, or in the custody or control of, a health care provider relating to the health history, diagnosis, or condition of a patient, or relating to treatment provided or proposed to be provided to the patient. "Patient records" includes only records pertaining to the patient requesting the records or whose representative requests the records. "Patient records" does not include information given in confidence to a health care provider by a person other than another health care provider or the patient, and that material may be removed from any records prior to inspection or copying under Section 123110 or 123115. "Patient records" does not include information contained in aggregate form, such as indices, registers, or logs.

endanger the life of self/another[5] or if the PHI makes reference to another person's PHI[6].

3. **Exceptions to the Right of Access**
    a. Both HIPAA and California laws contain exceptions to an individual's right of access to his or her health information. However, the exceptions included in HIPAA are different from those included in California law.
    b. **California Law:** provides a patient greater access to his or her medical records than does HIPAA. Thus, California law prevails over HIPAA's right to access provisions. California law states that a patient has the right to inspect and obtain a copy of all of his or her medical records with only two exceptions:
        i. Mental health records under specified circumstances (i.e. when a license health professional has determined, in the exercise of professional judgement, that the access requested is reasonably likely to endanger the life or physical safety of the patient).
        ii. Copies of X-rays or tracings derived from electrocardiography, electroencephalography, or electromyography need not be provided to the patient or patient's representative (although they must be permitted to review them), if the original X-rays or tracings are transmitted to another health care provider upon written request of the patient or patient's representative and within 15 days after receipt of the request.
        iii. California law does not permit the withholding of any other medical records from the patient.
    c. **HIPAA Exceptions**
        i. **Psychotherapy Notes:** HIPAA distinguishes between psychotherapy notes (which must be kept separate from the rest of the medical record) and other mental health records. California law does not treat psychotherapy notes differently from other mental health records.
        ii. HIPAA permits the outright denial of access to a patient's separately maintained psychotherapy notes, even if there is no potential harm to

[5]Per HSC § 123115(b), When a health care provider determines there is a substantial risk of significant adverse or detrimental consequences to a patient in seeing or receiving a copy of mental health records requested by the patient, the provider may decline to permit inspection or provide copies of the records to the patient, subject to the following conditions:

(1) The health care provider shall make a written record, to be included with the mental health records requested, noting the date of the request and explaining the health care provider's reason for refusing to permit inspection or provide copies of the records, including a description of the specific adverse or detrimental consequences to the patient that the provider anticipates would occur if inspection or copying were permitted.

(2) (A) The health care provider shall permit inspection by, or provide copies of the mental health records to, a licensed physician and surgeon, licensed psychologist, licensed marriage and family therapist, licensed clinical social worker, or licensed professional clinical counselor, designated by request of the patient.

[6]HIPAA permits a denial of access to that portion of any PHI that makes reference to another person (other than the provider) if a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such person.

the patient from seeing the notes. However, under state law, a health care provider may decline to permit inspection or provide copies of such records only if the provider determines there is a substantial risk of significant adverse or detrimental consequences to a patient in seeing or receiving a copy of mental health records.
    - Lanterman-Petris-Short (LPS) Act [Welfare and Institutions Code § 5328-5328.9] follows HIPAA standards as it relates to disclosure of mental health information to a patient that requests access to his or her information.

iii. Based on federal and state law differences, the **state standard is the one that must be used for denying access by a patient to his or her separately maintained psychotherapy notes.** If a provider refuses to permit inspection by, or to provide copies of the separately-maintained psychotherapy notes to, the patient, this state standard of harm must be met along with the requirements for denying access.

iv. A healthcare provider is not liable to the patient or any other person for any consequences that result from disclosure of patient records to the patient as required by California law (*see HSC § 123110(h)).*

4. **Denial of Right to Access**
    a. Federal and state regulations allow providers to deny a patient's request to access his or her information in specified circumstances as indicated above. Since denials are to be narrowly construed, the rule requires that providers give the patient access to any other PHI requested, after excluding PHI to which the provider has *lawful reason to deny access*.
    b. When a provider denies a patient access to Mental Health records the patient must be advised of their right to authorize release of those records to a third party (e.g., attorney, another provider).

5. **Process for Requesting Medical Records in General:** Under both HIPAA and California law, a health care provider can require that individuals make requests for access to medical records in writing, provided that the provider informs individuals of such a requirement. California law, which is stricter than HIPAA[7], requires that the provider allow the patient to inspect his/her medical record within 5 business days of making a written request. If the patient asks for copies of the records, the copies must be provided within 15 business days.
    a. **Disclosure of AHS Patient Medical Record:** AHS has a process to intake and respond to patient record requests in accordance with HIPAA, CMIA and related laws.
    b. Disclosure of AHS patient medical record, whether paper or electronic, may be given to the patient following the patient's written request and the above guidelines.

[7]Under HIPAA, once the covered entity receives the request for access, it must act on it (grant in whole or in part, deny, etc.) no later than 30 days after receipt, subject to one 30-day extension. But California law governs here because it is more stringent in favor of the patient.

6. **Minor's Medical Information:** A minor[8] patient or their legal representative can access or request copies of their records. Limited exceptions to this right exist. In general, whether the minor or the parent (or other legal representative) has the ability to access the medical record depends on who may legally consent to the treatment that the records relate to.
    a. If the minor has the authority to consent to medical treatment under state law, then the minor is generally the person authorized to have access to the records regarding the treatment, and to decide whether the records may be released to others (including the parent or other legal representative).
    b. Where a parent or other legal representative has the authority to consent to medical treatment for the minor, then the parent or other legal representative is generally the person authorized to have access to the minor's records regarding the treatment, and to decide whether the records may be released to others. However, a provider may deny a parent or other legal representative access to the minor's records, even though the parent or other legal representative had the authority to consent to the treatment, if the provider determines that access to the records would have a detrimental effect on the provider's professional relationship with the minor patient, or the minor's physical safety or psychological well-being.
        i. NOTE: There are several situations in which the minor has the legal authority to consent to medical treatment, but the provider is authorized, or required, to provide specified information to the parents. These situations involve self-sufficient minors, minor victims of sexual assault, minors receiving outpatient mental health treatment or residential shelter services, and minors receiving substance use disorder treatment where the care is *not* provided in a federally-assisted substance abuse program.
            1. However, HIPAA allows a provider to refuse access to a parent or legal representative if the provider makes a good faith determination that the minor's physical safety or psychological well-being would be harmed as a result, the parent(s) or guardian committed the sexual assault on the minor, or the disclosure would be inappropriate.
    c. "Mixed" Medical Record: A minor's medical record may contain information regarding treatment that the minor may consent to, and information regarding treatment that the parent or other legal representative must consent to. In such cases, the health care provider should take extra care to ensure that records are released appropriately.

[8] Emancipated minor may review his/her own chart and may restrict access to his/her own record by parent or guardian. Sensitive services to a minor allow a minor to restrict access to his/her record by parent or guardian.

REFERENCES

42 CFR § 2.23
45 CFR § 164.524
Civil Code § 56.10 and 56.11
Health and Safety Code § 120990(h)
Health & Safety Code § 123100
Health & Safety Code § 123115(b)
Health and Safety Code § 123148(d)
Welfare and Institutions Code § 5328-5328.9

APPROVALS

		System	Alameda	AHS/Highland/John George/San Leandro
Department	**Date:**	N/A	08/2020	08/2020
Pharmacy and Therapeutics (P&T)	**Date:**	N/A	N/A	N/A
Clinical Practice Council (CPC)	**Date:**		N/A	N/A
Medical Executive Committee	**Date:**		N/A	N/A
Board of Trustees	**Date:**		N/A	N/A

Consent Requirements for MEDICAL TREATMENT OF MINORS

IF MINOR IS:	*Is parental consent required?*	*Are parents responsible for costs? †*	*Is minor's consent sufficient?*	*May M.D. inform parents of treatment without minor's consent?*
Unmarried, no special circumstances	Yes	Yes	No	Yes
Unmarried, emergency care and parents not available [Business and Professions Code § 2397]	No	Yes	Yes, if capable	Yes
Married or previously married [Family Code § 7002]	No	No	Yes	No
Emancipated (declaration by court, identification card from DMV) [Family Code §§ 7002, 7050, 7140]	No	Probably Not[1]	Yes	No
Self-sufficient (15 or older, not living at home, manages own financial affairs) [Family Code § 6922]	No	No	Yes	[1]
Not married, care related to prevention or treatment of pregnancy, except sterilization [Family Code § 6925]	No	No	Yes	No
Not married, seeking abortion [Family Code § 6925]	No	No	Yes	No
Not married, pregnant, care not related to prevention or treatment of pregnancy and no other special circumstances	Yes	Yes	No	Yes
On active duty with Armed Forces [Family Code § 7002]	No	No	Yes	No
12 or older, care related to diagnosis or treatment of a communicable reportable disease or to prevention of an STD [Family Code § 6926]	No	No	Yes	No
12 or older, care for rape[1] [Family Code § 6927]	No	No	Yes	Yes, usually
Care for sexual assault[1] [Family Code § 6928]	No	No	Yes	Yes, usually
12 or older, care for alcohol or drug abuse[1] [Family Code § 6929]	No[2]	Only if parents are participating in counseling	Yes	Yes, usually
12 or older, care for mental health treatment, outpatient only[1] [Family Code § 6924; Health and Safety Code Section 124260]	No	Only if parents are participating in counseling	Yes	Yes, usually
17 or older, blood donation only [Health and Safety Code § 1607.5]	No	No	Yes	Probably not

[1] Special requirements or exceptions may apply. See *Chapter 4* of the *Consent Manual* or *Chapter 3* of *Minors & Health Care Law.*

[2] Parental consent *is* required for a minor's participation in replacement narcotic abuse treatment (such as methadone, LAAM or buprenorphine products) in a program licensed pursuant to Health and Safety Code Section 11875 (now codified at Section 11839 *et. seq.* [Family Code § 6929(e)]

Note: Notwithstanding the above information, a psychotherapist may not disclose mental health information to a parent who has lost physical custody of a child in a juvenile court dependency hearing unless the parent has obtained a court order granting access to the information.

† Reference: Welfare and Institutions Code Section 14010

Minors are defined as all persons under 18 years of age.

03/17

Risk Management Policy

ALAMEDA HEALTH SYSTEM

RISK MANAGEMENT POLICY

Department	Information Security	***Effective Date***	09/2020
Campus	AHS System	***Date Revised***	09/2020
Category	Administrative	***Next Scheduled Review***	09/2023
Document Owner	Chief Information Security Officer	***Executive Responsible***	Chief Information Officer

Printed copies are for reference only. Please refer to electronic copy for the latest version.

PURPOSE

This policy establishes the scope, objectives, and procedures of Alameda Health System's (AHS) information security risk management process. The risk management process is intended to support and protect the organization and its ability to fulfill its mission.

DEFINITIONS

Protected Health Information (PHI) includes but is not limited to any and all individually identifiable information about the physical or mental health condition or treatment of any individual, including but not limited to: any identifying information about a patient, such as a patient's name or a photo or video of the patient; any information about a patient's health condition or medication; and any information about payment for a patient's care and services.

Workforce members include employees, contracted staff, students, volunteers, medical staff and individuals representing or working at AHS.

POLICY:

It is the policy of AHS to conduct thorough and timely risk assessments of the potential threats and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) (and other confidential and proprietary electronic information) it stores, transmits, and/or processes. It is also the policy to develop strategies to efficiently and effectively mitigate the risks identified in the assessment process as an integral part of the AHS's information security program.

PROCEDURE

1. **Risk Assessment**
   The intent of completing a risk assessment is to determine potential threats and vulnerabilities and the likelihood and impact should they occur. The output of this process helps to identify appropriate controls for reducing or eliminating risk.
   A. **System Characterization**- The first step in assessing risk is to define the scope of the effort. To do this AHS must identify

i. where ePHI is received, maintained, processed, or transmitted.
ii. Where network access is required for both internal and external connections

B. **Assessment-** Conduct an assessment via the Security Risk Assessment (SRA) document and subsequent questions to evaluate threats, vulnerabilities, and data controls.

C. **Likelihood Determination**- Determine the overall likelihood rating that indicates the probability that a vulnerability could be exploited by a threat-source given the existing or planned security controls.

D. **Impact Analysis-** Determine the level of adverse impact that would result from a threat successfully exploiting a vulnerability. Factors of the data and systems to consider should include the importance to AHS's mission; sensitivity and criticality (value or importance); costs associated; loss of confidentiality, integrity, and availability of systems and data.

E. **Risk Determination-** Establish a risk level. By multiplying the ratings from the likelihood determination and impact analysis, a risk level is determined. This represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk rating also presents actions that senior management must take for each risk level. (0-9) will be considered "business as usual"; (10-15) will require T/SAC approval; (16-25) will be considered too high to accept.

F. **Control Recommendations for scores higher than 9-** Identify controls that could reduce or eliminate the identified risks, as appropriate to the organization's operations to an acceptable level. Factors to consider when developing controls may include effectiveness of recommended options (i.e., system compatibility), legislation and regulation, organizational policy, operational impact, and safety and reliability. Control recommendations provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented. Output - Recommendation of control(s) and alternative solutions to mitigate risk.

G. **Results Documentation-** Results of the risk assessment are documented in a spreadsheet maintained by the Information Security Office. Risk decisions are then given to appropriate person or committee.

2. **Risk Mitigation**

Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the Risk Assessment process to ensure the confidentiality, integrity and availability of AHS's ePHI. Determination of appropriate controls to reduce risk is dependent upon the risk tolerance of the organization consistent with its goals and mission.

A. **Prioritize Actions-** The information security office will utilize the risk register to maintain the risk of AHS. Each risk will be given a risk score and a corresponding risk rating. Higher scores will move to the top of the register This establishes a prioritized list of actions needing to be taken. The most immediate attention and top priority in allocating resources will be on the top of the register.

B. **Evaluate Recommended Control Options-** The feasibility (e.g., compatibility, user acceptance, etc.) and effectiveness (e.g., degree of protection and level of risk mitigation) of the recommended controls should be analyzed. In the end, select a "most appropriate" control option to reduce the risk. Alternative controls should also be identified.

C. **Conduct Cost-Benefit Analysis-** Determine the extent to which a control is cost-effective. Compare the benefit (e.g., risk reduction) of applying the "most appropriate" control with its subsequent cost of application. Controls that are not cost-effective are also identified during this step. Analyzing each control or set of controls in this manner, and prioritizing across all controls being considered, can greatly aid in the decision-making process.

D. **Select Control(s)-** Taking into account the information and results from previous steps, AHS's mission, and other important criteria, the Information Security Office determines the best control(s) for reducing risks to the information systems and to the confidentiality, integrity, and availability of ePHI. These controls may consist of a mix of administrative, physical, and/or technical safeguards.

E. **Assign Responsibility-** Identify the workforce members with the skills necessary to implement each of the specific controls outlined in the previous step and assign their responsibilities. Also identify the equipment, training and other resources needed for the successful implementation of controls. Resources may include time, money, equipment, etc.

F. **Develop Safeguard Implementation Plan-** Develop an overall implementation or action plan and individual project plans needed to implement the safeguards and controls identified. The Implementation Plan should contain the following information:

    i. Each risk and risk level;
    ii. Prioritized actions;
    iii. The recommended feasible control(s) for each identified risk;
    iv. Required resources for implementation of selected controls;
    v. Team member responsible for implementation of each control;
    vi. Start date for implementation
    vii. Target date for completion of implementation;
    viii. Maintenance requirements.

The overall implementation plan provides a broad overview of the safeguard implementation, identifying important milestones and timeframes, resource requirements (staff and other individuals' time, budget, etc.), interrelationships between projects, and any other relevant information. Regular status reporting of the plan, along with key metrics and success indicators should be reported to Chief Information Security Officer and/or Senior Management.

Individual project plans for safeguard implementation may be developed and contain detailed steps that resources assigned carry out to meet implementation timeframes and expectations. Additionally, consider including items in individual project plans such as a project scope, a list of deliverables, key assumptions, objectives, task completion dates and project requirements.

G. **Implement Selected Controls-** As controls are implemented, monitor the affected system(s) to verify that the implemented controls continue to meet expectations. Elimination of all risk is not practical. Depending on individual situations, implemented controls may lower a risk level but not completely eliminate the risk. Continually and consistently communicate expectations to senior management and other key people throughout the risk mitigation process. Identify when new risks are identified and when controls lower or offset risk rather than eliminate it. Additional monitoring is especially crucial during times of major environmental changes, organizational or process changes, or major facilities changes. If risk reduction expectations are not met, then repeat all or a part of the risk management process so that additional controls needed to lower risk to an acceptable level can be identified.

3. **Risk Management Schedule**
   The two principle components of the risk management process - risk assessment and risk mitigation - will be carried out according to the following schedule to ensure the continued adequacy and continuous improvement of AHS's information security program:
   A. **Scheduled Basis** - an overall risk assessment of AHS's information system infrastructure will be conducted annually. The assessment process should be completed in a timely fashion so that risk mitigation strategies can be determined and included in the corporate budgeting process.
   B. **Throughout a System's Development Life Cycle** - from the time that a need for a new, untested information system configuration and/or application is identified through the time it is disposed of, ongoing assessments of the potential threats to a system and its vulnerabilities should be undertaken as a part of the maintenance of the system.
   C. **As Needed** - the CISO or senior management may call for a full or partial risk assessment in response to changes in business strategies, information technology, information sensitivity, threats, legal liabilities, or other significant factors that affect AHS's systems

4. **Process Documentation**
   Maintain documentation of all risk assessment, risk management, and risk mitigation efforts for a minimum of six years.

COMPLIANCE

Violation of this policy or procedures by workforce members may result in sanctions and/or disciplinary action, up to and including termination of employment or termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.

REGULATORY REFERENCES

1. HIPAA REGULATORY REFERENCE
    a. 164.308(a)(1)(ii)(A)
    b. 164.308(a)(1)(ii)(B)
    c. 164.308(a)(8)

APPROVALS

		System	Alameda	AHS/Highland/John George/San Leandro
Department:	**Date:**	09/2020	N/A	N/A
Pharmacy and Therapeutics (P&T)	**Date:**	N/A	N/A	N/A
Clinical Practice Council (CPC)	**Date:**		N/A	N/A
Medical Executive Committee	**Date:**		N/A	N/A
Board of Trustees	**Date:**		N/A	N/A

Utilization Review Policy

ALAMEDA HEALTH SYSTEM

UTILIZATION REVIEW POLICY

Department	Care Management	***Effective Date***	05/2019
Campus	AHS System	***Date Revised***	05/2020
Category	Clinical	***Next Scheduled Review***	10/2023
Document Owner	Manager, Care Management	***Executive Responsible***	Vice President, Care Management

Printed copies are for reference only. Please refer to electronic copy for the latest version.

PURPOSE

To establish processing guidelines and timelines for member and provider notification of organizational determinations. The purpose of this policy is to provide standardized utilization review processes, follow regulatory guidelines, accreditation standards and payer contracts for patients admitted as inpatient or placed in outpatient observation status. The goal is to ensure that the hospital provides medically necessary, reimbursement – eligible services at the appropriate level of care while promoting quality outcomes and financial performance. This policy:

- Delineates the responsibilities and authority for those involved in the performance of internal and external utilization review;
- Establishes the protocols for medical necessity review of admissions, extended stays, professional services provided and appropriateness of the level of care;
- Mandates the review of outlier cases based upon extended length of stay and / or extraordinary high costs; and
- Identifies trends and patterns related to inefficient utilization of resources as well as over and under utilization of resources and recommend and / or initiate actions to improve the use of healthcare resources
- Establishes data to be collected and reviewed including length of stay, avoidable days, discharge dispositions and readmissions
- Establishes the mechanisms to communicate utilization information to committees, senior leadership, the medical staff and the governing board of the hospital.
- Provide education on appropriate utilization of resources to individual practitioners and departments.

POLICY

It is the policy of AHS that care managers will utilize InterQual criteria to assure patients are at the appropriate level of care to ensure appropriate reimbursement, ensure safe patient care and to facilitate discharge planning.

PROCEDURES

1. **Pre-Admission Review**
   a) **Surgical** – Review preformed for planned surgical admissions to determine whether inpatient or outpatient is the **appropriate status per the planned procedure codes.**

a) Utilizes the Medicare Inpatient Only List and the planned CPT code submitted by the surgeon for Medicare and Medi-Cal admissions

b) Reviews and documents the authorized admission status for all other payers

b) **ED** – RN CM provides level of care review determinations for real time decision support in the emergency department

a) Is performed when the ED physician makes the decision that the patient should be moved from the ED and placed in a hospital bed to determine whether the patient is appropriate to receive observation services vs inpatient admission.

b) The case manager will:

i. Evaluate the data that is available at the time a decision to admit is being made such as:

a. Previously provided interventions
b. Results of laboratory, imaging or other tests
c. Services provided prior to admission in the ED
d. Location of patient prior to arrival in the ED e.g. SNF, home, etc.

c) Apply InterQual criteria

i. Inform physician of review results including the appropriate level of care and admission status based upon the information available at the time of the review

a. In the ED setting not all diagnostic data are back prior to the decision to admit the patient
b. Communicate via hand off in the D/C Action Plan section of EPIC for additional review when the level of care or admission status order is different than the InterQual review determination so that additional data can be reviewed and the assigned unit case manager can prioritize an additional admission review and secondary review when necessary.
c. When criteria are not met CM will discuss with the attending physician options to discharge to lower level of care.

2. Admission Review

a) The RN case manager will complete reviews using InterQual criteria on all inpatient elective and emergency admissions within 24 hours of admission or entry into the facility including patients with orders to receive Observation services regardless of the payer source.

b) RN case managers will use the guidelines below to determine the appropriateness of admission:

i. Services ordered are medically indicated and can only be rendered at an acute hospital

ii. Appropriate use of evidence-based InterQual criteria and review process and evaluation

iii. Severity of Illness review - preliminary diagnosis and other documented clinical information to substantiate the need for admission or the delivery of observation or outpatient services e.g. the history and physical and admission notes, pre-admission orders

iv. Intensity of Service review – Clinical documentation that substantiates the medical necessity of admission including the services the patient will receive reflected in the admission and pre-admission orders and treatment plan

v. If the InterQual criteria do not match the admission order status, the case manager will discuss the review findings with the attending physician to request additional documentation and / or clarification of the patient's admission status. The RN case manager will refer to physician advisor to clarify admission level of care.
    a. If the admission review and secondary review does not support the inpatient admission order status
        i. The Physician Advisor will discuss the case with the attending physician
        ii. The attending physician may elect to continue the inpatient order The RN case manager will enter the bed day at the level of certification for payment without changes to the inpatient order.
        iii. For Medi-cal payors, if patient meets observation InterQual criteria, Care Manager will follow secondary review process.
        iv. Patients who are beneficiaries of a managed care program will be reviewed utilizing InterQual criteria. The case manager will seek certification for care in accordance with the payor's authorization process. When a managed care plan denies admission, the case manager will initiate peer to peer communication as soon as the denial is received.
        v. Admission reviews are not required for cases with pre-authorized days, however reviews are required for days exceeding the approved length of stay or when additional services are required but not included in the pre-authorization.
        vi. For admission reviews the template will be required in the note section per guidelines.

3. **Medicare Admission reviews** – When admission criteria are applied to Medicare beneficiaries, documentation should clearly reflect medical necessity for greater than or equal to a two-midnight stay in the hospital.

4. **Change in Status Orders- Medicare-** If the final secondary review determination is that the medical necessity of acute admission is not met and observation services or outpatient is determined to be the appropriate level of care, the Case Manager will speak with the admitting physician. The RN case manager will request the physician to change the admission order to reflect the determination of the secondary review. When a change in status occurs for a Medicare beneficiary from inpatient to outpatient, the case manager will complete the **Condition Code 44** status change requirements set forth by CMS including:
    a) The change in status from inpatient to outpatient is made prior to discharge or release while the beneficiary is still a patient of the hospital
    b) The hospital has not submitted a claim to Medicare for the inpatient admission
    c) The attending physician concurs with the utilization review committee's decision
    d) The physicians' concurrence with the utilization review committee's decision is documented in the patients' medical record.
    e) Provide a MOON letter to patient per guidelines.

5. **Admission Denial / Denial of Services-** When the case management department receives a denial of services from a payer including managed care plans after presenting current review information including clinical and secondary review information to support the admission, the RN case manager will contact the attending physician to discuss payer approval or denial information. The attending physician will be informed daily when denial of services by a payer exists.

6. **Reviews Conducted in the Emergency Department:**
   a. The ED case manager will conduct InterQual reviews to determine the appropriate admission status.
   b. When patients are admitted and remain in the ED > 24 hours related to lack of bed space, continued stay reviews will be conducted according to the continued stay section of this policy.
   c. When cases do not meet medical necessity criteria, the ED case manager will discuss the case with the attending physician to request clarification and additional documentation for the stay.
   d. After discussion with the attending physician, the ED case manager will follow physician advisor process.
   e. The ED case manager may contact the care transition team when appropriate to determine if the patient can be safely discharged from the ED with resources or transferred to a lower level of care.

7. **Surgical Patients -** The RN case manager will review the appropriate and most recent Medicare Inpatient Only List for elective surgical procedures. The Medicare Inpatient Only List is published November 1 annually. This list refers to procedures and services that CMS has identified as typically only provided in the inpatient setting and therefore not paid under OPPS (outpatient prospective payment system). For commercial and Medi-Cal plans, the case manager will verify surgical procedures using the Inpatient List provided in the current year InterQual criteria.
   a) The length of stay category for surgical procedures are as follows:
      i. Short stay: expected length of stay 1-2 days
      ii. Moderate stay: expected length of stay 3-5 days
      iii. Long stay: expected length of stay <u>> 6 days</u>
   b) The RN case manager will apply the short stay length of stay criteria for procedures that are not on the inpatient list.

8. **Labor and Delivery or Ante Partum Patients** – The case manager will review labor delivery and ante partum patients according to the guidelines provided within the InterQual current year criteria set.
   a. Observation patients will be reviewed daily to determine the appropriate level of care or readiness for discharge.
   b. For a C-section delivery, conduct an InterQual review for day 4 or for the day a new diagnosis or complication arises if the patient is not discharged on day 4.
   c. For a vaginal delivery, conduct an InterQual review on day 2 or for the day a new diagnosis, condition or complication exists if the patient is not discharged on day 2.

9. **Observation Services**
    a. **Medicare -** Hospitals are required to provide Medicare Outpatient Observation Notice (MOON) to Medicare beneficiaries including Medicare Advantage health plan enrollees informing them that they are outpatients receiving observation services and are not inpatients of a hospital.
        i. Case management staff will provide the MOON to each Medicare or Medicare Advantage patient receiving Observation Services and
        ii. When there is a status change from Inpatient to Observation status. This notice explains possible financial responsibilities associated with the care therefore must be provided as soon as possible and not to exceed within 36 hours of the stay.
        iii. The case manager will provide the patients with a verbal explanation of the reason outpatient services are indicated.
    b. **Medi-cal -** Medi-cal does not reimburse for observation services so a secondary review process is required to either approve as in-patient, deny the admission or apply administrative days per policy.
    c. **Commerical/Managed Care** – Care Manager/CM Specialist will obtain authorization per payor requirement.

10. **Continued Stay Review**--The RN case manager will conduct daily reviews to determine medical necessity for patients with **Medi-Cal (TAR-free process only) HPAC with Medi-Cal pending and self-pay** insurance and will complete the review template.
    a. The RN case manager will review **Commercial, Medicare Advantage and Workers' Comp** patients every other day. The review template is required for this group.
    b. Reviews are not required on the **day of discharge or transfer**.
    c. When criteria is not met the Physician Advisor Policy will be followed.
    d. **Observation** patients will be reviewed daily to determine if the patient meets acute inpatient criteria or is appropriate for discharge.
    e. **Payor Communication -** If a patient does not meet InterQual continued stay criteria but requires inpatient stay for a medical reason, the RN case manager will provide additional clinical documentation to support medical necessity to remain in the hospital including related clinical information and discharge planning efforts and submit the documentation regularly to the payor.
    f. **OB/Normal Newborn -** Continued stay review for OB / normal newborn will be required when the patient stays past the global days of 2 after vaginal delivery or 4 days after C-section delivery.
        i. Episode Day 1 will apply in the appropriate InterQual subset when the stay is beyond the global allowed days.
    g. **NICU** - Admission review is required when a patient is transferred to NICU and will conduct continued stay reviews for NICU as per the payer requirements. Medi-cal payor review is completed daily.
    h. **Level of care changes** require review at that level of care in the appropriate subset on the day of transfer even though a continued stay review might not have been due.
        i. Same diagnosis or condition requiring transfer to higher level – use higher level of care for same episode day
        ii. Observation patient that requires higher level of care – Conduct Episode Day 1 review in appropriate subset and level of care

iii. New condition or diagnosis requiring higher level of care – Conduct Episode Day 1 or operative review

11. **Patients awaiting placement** do not require InterQual reviews.
    a. The case manager will review the record every 3 days to assure there is no change in the clinical status.
    b. A corresponding note in the patient's medical record is required documenting the progression of the placement and barriers that exist.
    c. Apply discharge screens and if there is a significant change in condition, resume InterQual continued stay reviews following guidelines.

12. **TAR-Free Medi-Cal Fee For Service Medi-Cal pending, HPAC-** patient will be referred to the physician advisor for final status determination based on policy.

13. **Administrative Days**-The administrative day process is initiated when a Medi-Cal (TAR – free process)
    a. The patient no longer requires acute hospital care and needs placement in a skilled nursing facility, intermediate care facility or for patients with tuberculosis or high-risk OB patients.
    b. These cases should be reviewed at least once per week through discharge including application of discharge screens.
    c. CM must confirm per Medi-Cal Guidelines ten (10) SNF referrals are submitted daily, (Monday-Friday excluding weekends and holidays).
    d. For Managed Medi-Cal it is ten (10) SNF referrals the first day and five (5) SNF referrals subsequent days. Care Manager will confirm with the managed Medi-Cal health plan representative authorization for administrative days (weekends included).

14. **Transfers within AHS System –** The case manager may conduct a continued stay review based upon the frequency required by the payer.
    a. If the transfer is to a higher level of care or if there is a significant change in treatment or diagnosis, Episode Day 1 criteria should be reviewed.

15. **Long Stay Critical Care Patients –** The case manager will conduct daily reviews for Medi-Cal (TAR-free), Medi-Cal pending and self-pay patients.
    a. For other payers, the case manager will apply continued stay criteria and discharge screens every 2 days.
    b. Long Term Acute Care (LTAC) will be discussed and considered when the patient requires long term inpatient services especially those requiring ventilation and those with extensive wound care.

16. **Changes in Condition –** When there is a change in condition and additional treatment prolongs the hospital stay, the case manager will select the appropriate subset and apply Episode Day 1 or Operative Day criteria as appropriate.

17. Acute Rehabilitation and Skilled Nursing Facilities

a. Acute Rehabilitation Care Managers will complete reviews on admission and every (3) days.
b. Skilled Nursing Facility Care Managers will complete reviews for patients on admission and every (10) days.

18. **Weekend expectations:** The Care Manager will prioritize completion of initial reviews within 24 hours of admission beginning with new admissions from the previous day, Observation patients and those with commercial payers.

19. **Discharge Reviews:** If a patient does not meet acute criteria or the discharge screen, the Care Manager will discuss the case with the attending physician to determine the appropriate lower level of care and plan for discharge.

20. **Responsible person:** AHS Managers are responsible to ensure that all personnel adhere to the requirements of this policy, and that these procedures are implemented and followed at AHS hospitals.

All employees whose responsibilities are affected by this policy are expected to be familiar with the basic procedures and responsibilities. Failure to comply with the standard will be subject to appropriate performance management.

REFERENCES

1. Title 22, Section 51213

2. Inpatient Only List for Medicare Surgical Patients

3. State of California Medi-Cal Superior Systems Waiver Comprehensive Renewal

4. Department of Health Care Services (DHCS) Clinical Assurance and Administrative Support Division (CAASD): Designated Public Hospital Project Provider Training DHCS CAASD Frequently Asked Questions for the Public Hospital Project

5. InterQual Acute Care Criteria 2020

6. Cross-Reference

7. AHS Care Management Physician Advisor Policy and Procedure

APPROVALS

		System	Alameda	AHS/Highland/John George/San Leandro
Department	**Date:**	N/A	05/2020	05/2020
Pharmacy and Therapeutics (P&T)	**Date:**	N/A	N/A	N/A
Clinical Practice Council (CPC)	**Date:**	06/2020	N/A	N/A
Medical Executive Committee (MEC)	**Date:**	N/A		
Board of Trustees	**Date:**		N/A	N/A