MaineHealth Onboarding and Termination Policy

The MaineHealth Privacy and Security Governance Committee, as authorized by the Affiliated Covered Entity Operating Agreement, adopts the following policy and procedure for MaineHealth, NorDX, MaineHealth Care at Home, The Memorial Hospital at North Conway, NH, Maine Heart Center, and the MaineHealth Accountable Care Organization, LLC, (hereafter, MaineHealth).

I. Purpose

The purpose of this policy is to ensure that access to Electronic Patient Health Information (ePHI) and other Confidential information (CI) is limited to those members of the workforce, and other authorized individuals, whose roles require it and to ensure that access is adjusted or revoked when those Users are no longer authorized for that access, such as when they change roles or terminate their relationship with MaineHealth.

Scope

This policy applies to MaineHealth workforce and other authorized users of MaineHealth Information Systems, (hereafter, MaineHealth Users). MaineHealth Information systems includes MaineHealth managed Information Technology and applications which run on it, as well as any hosted services used by MaineHealth for its operations.

II. Policy

a. Access to MaineHealth information Systems, including those containing ePHI/CI will be provisioned for each MaineHealth User via a unique identifier. Access provided will be based on each individual's role and will be limited to the minimum necessary required for performance of each individual's defined job or jobs within MaineHealth.
b. Access to any MaineHealth Information systems will be promptly revoked when a MaineHealth User has terminated employment or their relationship with MaineHealth. Access revocation will include all steps necessary to ensure that individual cannot subsequently gain access to systems or resources as if they were a current, authorized MaineHealth User.
c. Members of the workforce placed on long term disability may have access suspended or removed until they have been approved by their MaineHealth leader for resuming work[1].
d. MaineHealth Users who work across multiple MaineHealth organizations will have their access adjusted to only what locations and privileges are required if they no longer require access for one of their jobs or locations, but need to retain access for the remaining one(s).

III. Procedure

a. Onboarding Process
    i. MaineHealth conducts reference and background checks on all prospective employees. Offers of employment are conditioned upon satisfactory reference and background checks.
    ii. All workforce members must sign a confidentiality agreement prior to being granted access to any systems, including those containing ePHI/CI or which can access ePHI/CI.
    iii. Access to any system, including those containing ePHI/CI is granted to the extent required for the MaineHealth User to fulfill the responsibilities of their position.
    iv. MaineHealth procedures specify who can authorize access, for what purposes access can be authorized, and the procedures for approving and documenting the access authorization.
    v. Procedures also specify how and when to modify access and the processes appropriate for communicating such changes to the relevant individuals.
    vi. In the event a MaineHealth User's role changes, procedures are in place to adjust the MaineHealth User's access authorization where necessary.

[1] Whether access is suspended or removed will depend on the length of the absence and the capabilities of that application or system. Access suspension or removal would mean that the individual could access the system in any manner at a time they are not performing work for MaineHealth.

b. Termination Process
    i. MaineHealth Users, whose employment or association with MaineHealth is terminated, will have their access to MaineHealth Information Systems, including those containing ePHI/CI revoked upon notification of termination or within 1 business day of a planned termination date (except as noted in section iv and v below). Where a MaineHealth User leaves one department or MaineHealth organization, but retains the clinical privileges or job functions for other MaineHealth organizations, access will be adjusted where appropriate to preserve access for their remaining responsibilities at those other job functions.
    ii. Notification of termination from employment must be provided by MaineHealth leaders to HR through the established process of completing a personnel action form (PAF) and obtaining and relevant approvals. For normal terminations, the PAF must be complete by the manager well in advance of an employee's termination date. Information Technology Services uses the PAF updates to take action of an employees' termination from MaineHealth to lock their account, thus suspending network access for that employee within 24 hours of termination.
    iii. Notification of termination of non-employee workforce or other authorized third party personnel must be communicated to Information Technology Services by MaineHealth leadership with responsibility for overseeing that non-employee MaineHealth User.
    iv. If a terminating MH User is identified as posing a potential risk to operations or data confidentiality, availability or integrity, access to all applicable information systems must be removed immediately upon termination notification.
    v. When a workforce member is terminated for cause, physical and systems access must be revoked immediately upon notification.
    vi. Access revocation will include removal of access to both systems and any secured physical facilities, including any keys, badges or other devices which provide that access. MH access removal standards for common systems access are described in Attachment A.
    vii. Where necessary for purposes of patient safety or continued operations, accounts for terminated workforce may need to remain within a system or as part of a reference list, but access must be blocked or disabled to the extent necessary to prevent future unauthorized use of those credentials by any other individual.

IV. Accountability

a. MaineHealth Leadership is responsible for:
    i. Determining appropriate access to ensure application of the minimum necessary standard for all workforce members under their direction.
    ii. Promptly entering, or informing HR where PAF entry is not possible, for upcoming employee terminations
    iii. Communicating information related to termination of a MaineHealth User to the appropriate departments to ensure timely revocation of access to both physical and system resources.
b. MaineHealth Human Resources is responsible for:
    i. Timely entry and notification of employee terminations in support of MaineHealth leadership as needed.
    ii. Coordination with appropriate physical security resources for revocation and/or retrieval of any physical/building access devices, keys or badges upon termination of employment.
c. Information Technology Services is responsible for:
    i. Timely removal of systems access based on the risk of a terminated MaineHealth User consistent with the procedures described above.
    ii. Identification and management of core information systems and network access to facilitate timely removal and/or adjustment of access as appropriate.

V. Exceptions

If an account cannot be disabled due to extenuating circumstances, Information Technology Services leadership must take any appropriate steps necessary to limit exposure from that account. , For example, putting in place enhanced logging or reporting of activity against that account or changing of the password to a highly complex one that the original user would not know or could not guess.

Any additional exceptions to this policy must be approved by the Chief Information Security Officer (or above) as well as a member of HR leadership for access termination exceptions.

VI. Enforcement

Failure to comply with the requirements of this policy has performance consequences as described in the "MaineHealth HR Standards of Conduct Policy".

VII. References

a. Definitions:
    i. Workforce: employees, students, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity is under the direct control of the entity, whether or not they are paid by the covered entity.
b. Related policies & standards
    i. MaineHealth Information Access Management policy
    ii. MaineHealth HR Standards of Conduct Policy
    iii. MaineHealth HR Termination policy
    iv. MaineHealth Access Policy
    v. MaineHealth System Access Termination Procedure
c. References
    i. HIPAA Final Security Rule, 45 CFR Parts 160, 162, and 164, Department of Health and Human Services.

Appendix A: System Access Termination Processes

Overview

When an employee or non-employee workforce member leaves MaineHealth, access to MaineHealth systems must be removed consistent with state and federal regulatory obligations. Departing system users may leave behind unfinished work or tasks which need management focus to re-assign. The processes described below are intended to support both of those needs.

Planned Termination Notification[2]

Terminations come into the IT Security Operations team via one of two methods:

Lawson (employees only):

Managers submit a Personnel Action Form for their employee with a defined end date of employment. At the end of that employee's last day, the change in status of that employee triggers a 'disable' event for their network access. On the next business day, that network access is removed via a batch process managed by Security Operations.

Manager or MH Contact Notification (non-employees):

The manager or an individual's MH contact submits a network access change request and indicates the date/time for access removal. Access would then be removed within one business day after the date/time specified in the request.

Actions Taken for Access Removal upon Termination

Within one business day of termination, the following actions will occur for a terminated user. These actions are automated, so exceptions would need to be communicated to Security Operations. In all cases, the exception process supports managers or an authorized delegate to access a departed individual's information to support ongoing operations. Access to MH system resources will not be granted to a departed individual.

Access Item	Action	Retention	Exceptions
Network Account	Remove all file and group permission associations for user account and disable account.	Account remains on directory in a disabled status for 60 days and then deleted.	Manager approval required to keep network account enabled.
E-Mail	Account disable process disables the e-mail as well. Any new e-mail to account will receive a bounce message as undeliverable. No access will be available to account.	E-mail account retained on system and within Archive for 30 days. The account and associated archived messages will be removed thereafter.	Manager can request access to e-mail box for up to 30 days post termination to re-assign messages and/or put on an auto-response message directing senders to another account. Manager can request this access in advance of termination by sending the request to the MH IT Security Operations team. In this situation, access would be provided post termination.

[2] Planned implies that the individual leaving has provided advanced notice of their resignation or there is a mutual agreement for a future departure date for that individual.

Access Item	Action	Retention	Exceptions
E-mail and Calendar through MDM	If the user has a personal smart phone or device and has MDM supporting MH e-mail delivery, when the e-mail account is disabled, it is removed from that device.	At point of e-mail being disabled, mail and calendar items residing on that device are removed and unrecoverable.	
'Home Folder'	Individual's home folder retained for 30 days on file server from account disable.	Removed at the end of the month after the 30 days have elapsed.	Manager can request the contents or specific elements of the home folder if request made within 30 days from termination date.
Desktop Files	Access removed when network account disabled.	Desktop files may, or may not exist for a user as their primary storage would be on their home folder. Retention of any local desktop files would depend on dispensation of equipment and configuration after the user leaves.	Manager can request locally cached files in the event that the home folder is empty.
Voice Mail	Voicemail account, where associated to an individual, is removed upon notification of termination.	None	Manager can request voicemail and phone remain active for 30 days to support an automated message and/or to clear out messages left.
Remote Access Token	Access removed when network account disabled.	Token remains active and associated to user until user account is deleted.	Token can be re-assigned to another user at the direction of department manager.

A manager can request access for a terminated individual's home folder or e-mail and delegate that permission to another on the team where necessary to support ongoing clinical operations. When this occurs, the manager remains ultimately responsible for proper use and review of the information.

For all of the above items, should the manager request access in advance of a termination, request for this access must get HR Leadership approval.

Immediate Termination[3]

An immediate termination requires immediate notification of MH IT Security Operations team directly for completion of the above access removal steps. For these situations, the manager or HR should notify the MH IT Security Operations Duty Officer at any hour in order to facilitate the access changes described above.

For these situations, HR or the manager may choose to lock an individual's access and remove e-mail sync to their personal device via MDM immediately and follow up with disabling the account (and removing the ability to send and receive e-mails into the account) on the next business day. This prevents e-mail messages from 'bouncing' prior to the manager being able to notify their staff or others impacted of the change.

[3] Immediate termination are situations where an individual is terminated for cause, resigns from the organization, and manager opts to release them immediately vs. have them work the required notification period, or is removed from the organization as part of a restructuring or staffing adjustment process.