UNIVERSITY OF CALIFORNIA, SAN FRANCISCO
AUDIT & ADVISORY SERVICES

UCSF Benioff Children's Hospital, Oakland
Natus System – Access Controls Review

Project # 23-029

July 2023

CONFIDENTIAL

University of California
San Francisco

Audit & Advisory Services

UCSF Box 0818
1855 Folsom Street
San Francisco, CA 94143

tel: 415.476.3851
fax: 415.476.3326

www.ucsf.edu

July 14, 2023

George Weiss
Vice President, Operations
UCSF Benioff Children's Hospitals

SUBJECT: UCSF Benioff Children's Hospital, Oakland
Natus System – Access Controls Review

UCSF Audit & Advisory Services (A&AS) conducted a review of the security practices relating to user access currently in place for the Natus system within the Neurology Clinic at UCSF Benioff Children's Hospital Oakland (BCH Oakland). The purpose of this review was to evaluate processes and controls in place related to the user access and security of the Natus system.

Our services were performed in accordance with the applicable International Standards for the Professional Practice of Internal Auditing as prescribed by the Institute of Internal Auditors (the "IIA Standards").

Our review was completed, and the preliminary draft report was provided to department management in May 2023. Management provided their final comments and responses to our observations in July 2023. The observations and corrective actions have been discussed and agreed upon with department management and it is management's responsibility to implement the corrective actions stated in the report. A&AS will periodically follow up to confirm that the agreed upon management corrective actions are completed within the dates specified in the final report.

This report is intended solely for the information and internal use of BCH Oakland management and the Audit & Compliance Committee and is not intended to be and should not be used by any other person or entity.

Sincerely,

Irene McGlynn

Irene McGlynn
Chief Audit Officer
UCSF Audit & Advisory Services

EXECUTIVE SUMMARY

I. BACKGROUND

As a planned project for Fiscal Year 2023, Audit & Advisory Services in conjunction with Deloitte & Touche LLP conducted a review of the security practices relating to user access currently in place for the Natus system within the Neurology Clinic, which is administered by the University of California San Francisco (UCSF) Benioff Children's Hospital Oakland (BCH-Oakland).

Natus is a range of systems designed to provide patient data acquisition and storage for Routine Electroencephalogram (EEG), Long Term Epilepsy Monitoring (LTM), Sleep Diagnostics Polysomnography (PSG) and Continuous EEG Monitoring. The Natus system houses patient health information and is connected to the BCH-Oakland's network and is within its security system (firewall) protection. Therefore, Central IT manage application and device level security, however, user account management for the Natus system is managed locally by the system administrator within the Neurology Clinic.

II. PURPOSE AND SCOPE

The purpose of this review was to identify observations and opportunities for improvement related to user access and security of the Natus system given that the system engages in processes that can impact or be impacted by the third parties employed by BCH-Oakland.

After additional scoping discussions and discovery of Natus being an on-premises application, further emphasis was placed on the security controls and user access currently in place for the Natus system and the understanding as to how UCSF manages the system internally.

The scope of the assessment covered internal security practices pertaining to user access as well as contacting the third-party vendor Natus directly to gain an understanding of the configurations set up for the on-premises application hosted by UCSF/BCH-Oakland. These focus areas were selected due to potential implications relating to third party vendor systems and related processes.

Key security practices/areas reviewed included:

- Account Management
- Password Management
- User Access Audit
- Session Management
- Least Privileges
- Segregation of Duties
- Shared Accounts
- Remote Access
- Privileged Access

To conduct our review, the following activities were performed:

- Interviews were conducted to walk through specific aspects of the system's functionality, configurations/capabilities
- Existing documentation/artifacts that relate to the Natus system, including but not limited to, Natus IT Overview Documents, Business Associate Agreement, and internal policies/procedures pertaining to the security and management of the Natus system were assessed.
- Evaluated security practices related to user access as part of a live demonstration of the Natus system
- Reviewed BCH-Oakland policies and procedures as they relate to user access and security of Natus system
- Interviewed key personnel who interact with the Natus system
- Reviewed sample screenshots to further evidence user types and access configurations of the Natus system

The assessment included the review of BCH-Oakland's policies; UC/UCSF IT Security policies as well as user access and security testing based on leading practices of industry standards such as National Institute of Standards and Technology (NIST).

Work performed was limited to the specific activities and procedures described above. As such, this report is not intended to, nor can it be depended upon to provide an assessment of compliance beyond those areas specifically reviewed. The assessment was performed during March and April of 2023.

III. <u>SUMMARY OF OBSERVATIONS</u>

Based on the assessment performed, observations and recommendations for consideration were identified against BCH-Oakland/ UCSF policies and leading security practices of user account management for an on-premises application of the Natus system. The security practices identified have a direct and immediate effect on the security of the Natus environment at BCH-Oakland. As a result, this report documents specific remediation recommendations to consider for each observation. Opportunities for improvement were further identified in the following four areas deemed to be at an elevated risk: account management, password management, least privileges, and segregation of duties.

Overall, the following themes were identified as a result of the assessment. Natus password and account management practices and procedures could be updated to facilitate accurate and standardized Natus user process from onboarding to sunsetting/offboarding. Additionally, ensuring required user access and least privilege controls are configured into Natus, as no approved workflow and/or procedures currently exist to review, approve or track user roles, membership requests, and access rights within the Natus system. Lastly, the gaps in segregation of duties control for Natus creates elevated risks regarding lack of control and potential conflicts of interest of certain individuals (or lack thereof) pertaining to specific Natus processes such as audit log review, user administration, and account recertification or approval.

If not addressed, these activities can lead to unauthorized actions within Natus, potential misuse of user data/PII, and elevated security/insider threats to the BCH-Oakland's systems/network.

The specific observations from this review are listed below and detailed in Section IV of the report.

1. A documented user onboarding and rights authorization (e.g., ServiceNow ticketing system) is not used to process user access requests to Natus system as required by policy.

2. A documented periodic user account review process is not in place for the Natus system.

3. The Natus system does not have a defined acceptable inactivity period to require automatic disabling of inactive user accounts.

4. Currently, there is not a documented process in place to periodically review Natus permissions and corresponding permission rights sets attached to Natus roles and/or group policies to facilitate each user role/group has the least or minimally required privileges required to perform the work prescribed by the role in Natus.

5. There is inadequate separation of duties in place to ensure that the same personnel do not perform administrative, operational and audit functions.

6. Natus system has shared/group/guest accounts, and shared activities logging does not attribute to an individual user using the shared account to access Natus.

7. Currently, there is not a documented process in place to conduct periodic reviews of Natus access / audit logs with sign-off(s).

8. Password Management practices for the Natus system do not meet BCH-Oakland's security requirements.

9. Privileged access account(s) /request(s) for the Natus system are not formally approved and there is not a documented process to periodically review and recertify Natus privileged roles and Natus privileged (admin) accounts to facilitate the correct level of access and need for continued access.

Additionally, during the course of this review, potential opportunities for improvement were noted regarding session management practices and remote access configuration of the Natus system.

IV. OBSERVATIONS AND MANAGEMENT CORRECTIVE ACTIONS

A. Account Management

No.	Observation	Risk/Effect	Recommendation	Management Actions
1	***A documented user onboarding and rights authorization (e.g., ServiceNow ticketing system) is not used to process user access requests to Natus system as required by policy.*** The current process to receive user account access request is via an email request to the Natus system account administrator thereby by-passing the hospital's established authorization approval process using ServiceNow ticketing system. Policy IT. Sec 9.1 states that all requests for access must be submitted to Health Information Systems (HIS) by the requestor's manager using an Account Request Form (ARF). The ARF process is connected to ServiceNow and is utilized to request and disable user access.	Lack of documented process to track/review/approve access requests may result in privilege creep and excessive and/or inappropriate privileges being assigned.	Integrate Natus onboarding and rights authorization into BCH-Oakland's existing ServiceNow ticketing system to process Natus access requests.	Workflow will be developed for integrating Natus onboarding and permission rights into the BCH-Oakland's existing ServiceNow ticketing system to process user account requests to be aligned with IT Security Policy. **Target Implementation Date:** October 31, 2023 **Responsible Party:** Executive Director, Ambulatory Service
2	***A documented periodic user account review process is not in place for the Natus system.*** Regular account recertification is important to ensure that user accounts are still required and appropriate for their assigned access rights. Discussion with the System Administrator for the Natus system identified that there is currently no	Lack of process to review production/ operational privileges periodically may result in privilege creep, privilege misuse, and privilege abuse.	Develop a process to perform documented periodic recertification review with sign-off(s) of Natus user accounts.	Department is in the process of creating policy and procedures for periodic account review. Once completed, it will be submitted to BCH-Oakland Committee to review and approve for upload in PowerDMS.

No.	Observation	Risk/Effect	Recommendation	Management Actions
	process implemented for periodic review of user accounts. HIPAA Security Rule stipulates that the covered entity must implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate (§164.308(a)(3)(ii)(B)*).* University of California policy (BFB-IS-3 and related standard: Identity and Access Management” §III) stipulates that periodic review of membership in the community and review of their authorized access rights should be performed.			**Target Implementation Date:** October 31, 2023 **Responsible Party:** Executive Director, Ambulatory Service
3	***The Natus system does not have a defined acceptable inactivity period to require automatic disabling of inactive user accounts.*** Review of the process for disabling of inactive user accounts for the Natus System found that a specific period of inactivity for disabling user has not been defined in accord with account management policy University of California policy (BFB-IS-3 and related standard: Identity and Access Management Standard §4.14 Inactive Accounts) stipulates that “Workforce Members must ensure accounts under their control or area of responsibility that have not been accessed for one hundred and eighty (180) consecutive days are reviewed. If accounts are not needed, then they must be disabled or removed.”	Lack of automation enabled to automatically disable inactive user accounts may contravene user access policies and allow a malicious actor an opportunity to take over inactive stale accounts and gain access to resources.	Review BCH-Oakland/UCSF standards to sync-up with leading security practices and setup system controls to automate disabling of inactive user accounts after a defined period of inactivity (e.g., 90, but no longer than 180 days).	Following a meeting with the system vendor, the Natus system will be configured for automatic disabling of users after 180 days of inactivity. **Target Implementation Date:** October 31, 2023 **Responsible Party:** Executive Director, Ambulatory Service

B. Least Privileges

No.	Observation	Risk/Effect	Recommendation	Management Actions
4.	***Currently there is not a documented process in place to periodically review Natus permissions and corresponding permission rights sets attached to Natus roles and/or group policies to facilitate each user role/group has the least or minimally required privileges required to perform the work prescribed by the role in Natus.*** University of California policy (BFB-IS-3 and related standard: Identity and Access Management Standard §4.1.6) requires Units to ensure that a process is in place for all account types to update or adjust access rights when changes occur [e.g., job responsibilities, termination, access is no longer required, IT Resource (service) retired, etc.] or the account is no longer needed.	Not reviewing permissions / permission sets attached to roles periodically may result in excessive / overbroad permissions granted to users, thus allowing a user to perform tasks / access sensitive data that are inconsistent and outside the scope of the user's role.	Establish and document a process to review Natus permission sets, user roles, and user role assignments at least once every six months to determine least privileges are met.	Department is in the process of creating policy and procedures for periodic account review including permission rights attached to roles in Natus. Once completed, it will be submitted to BCH-Oakland Committee to review and approve for upload in PowerDMS. **Target Implementation Date:** October 31, 2023 **Responsible Party:** Executive Director, Ambulatory Service

C. Segregation of Duties

No,	Observation	Risk/Effect	Recommendation	Management Actions
5.	***There is inadequate separation of duties in place to ensure that the same personnel do not perform administrative, operational and audit functions.*** Our assessment of the segregation of duties controls for the Natus system identified the following: • The system administrator that provides access control functions for the Natus system also has the ability to access and modify Natus system audit/access logs. • There is no process to document and approve privileged access accounts needed. • Separate accounts for privileged (administrator) and unprivileged (user) access are not created. University of California policy (BFB-IS-3 and related standard Event Logging) requires where possible, IT Workforce Members acting as system administrators on IT Resources classified at Protection Level 3 or higher and Availability Level 3 or higher must not have permission to erase, deactivate or modify logs of their own activities. University of California policy (BFB-IS-3 §12.4.3 Administrative Logs) requires for Institutional Information classified at Protection Level 3 or higher,	Lacking a clear separation of duties control may allow conflicts of interest to occur (e.g., admins reviewing their own audit trails / logs). This could lead to insider threat and malicious activity and the creation of user accounts at will. Not restricting access or facilitating integrity of audit / access logs may compromise subsequent forensic reviews and lead to unmonitored user activities / unfettered access Insufficient separation of user populations may lead to overlap of administrative, audit and operational roles, thus creating situations of possible collusion or conflicting interest (e.g., self-	Select employee who does not currently have administrator or user access to perform audit functions on the Natus System. Ideally, this is someone who has a clear understanding of what actions should and should not be taking place within the system as well as having significant IT background. Apply access controls and permissions to facilitate users only have access to the resources they need to perform their job functions. Configure Natus audit / access logs to only be accessed by outside reviewer or audit team to facilitate no site users or administrators can modify or delete data. In addition, perform routine monitoring to confirm no illicit activity has occurred with audit / access logs.	a) Everyone with access to Natus system can currently view/edit the audit logs folder. Natus system does not have the ability to perform log forwarding, therefore access to the logs folder will be restricted to IT Security only. b) Separate accounts for administrative and non-administrative access \Core privilege account will be created once the integration with active directory is completed. c) Process for approving privileged access accounts will be documented as part of the policy and procedures document being developed **Target Implementation Date:** October 31, 2023

	and IT Resources classified at Protection or Availability Level 4, Units must independently review privileged accounts periodically to ensure that: a) only authorized activities occurred and b) Anomalies are analyzed and corrective actions are implemented. University of California policy (BFB-IS-3 and related standard: Identity and Access Management Standard §5.1)" stipulates that IT Workforce Members must configure IT Resources (devices) with separate accounts for privileged (administrator) and unprivileged (user) access.	approving one's own operational roles)	Define each user type and their associated roles/duties, then create and enforce a policy that limits users to their segregated responsibilities. More user types with varying capabilities may need to be created to help distinguish particular users/duties. In addition, the employed system reviewer/auditor should routinely determine no collusion or conflicting interest is taking place.	**Responsible Party:** Executive Director, Ambulatory Service

D. Shared/Group/Guest Accounts

No.	Observation	Risk/Effect	Recommendation	Management Actions
6.	***Natus system has shared/group/guest accounts and shared activities logging does not attribute to an individual user using the shared account to access Natus.*** Review of Natus system's shared accounts identified three shared accounts: 1) BioMed – used by Medical Device Unit 2) HIS – used by IT Services 3) Guest – a system default account with no access rights set-up. Each of these shared account has a common password. The number of users for the shared accounts are not documented.	Having group / shared accounts in Natus may lead to inability to track individualized actions in forensic investigations and negatively impact security incident response/audit/ access logging requirements.	Limit group/shared accounts by minimizing the level of access so that users cannot modify each other's work. Utilize group accounts instead of shared accounts and assign access to multiple users to specific resources. Restrict usage of guest accounts by making them temporary and track login and logout times.	The initial discovered shared accounts have been removed. The vendor indicated that the guest account is not required and will also be removed. **Target Implementation Date:** October 31, 2023 **Responsible Party:** Executive Director, Ambulatory Service

No.	Observation	Risk/Effect	Recommendation	Management Actions
	HIPAA Security Rule stipulates that a unique name and/or number for identifying and tracking user identity must be assigned (HIPAA § 164.312(a)(2)(i)).			

E. User Access Audit

No.	Observation	Risk/Effect	Recommendation	Management Actions
7.	**Currently, there is not a documented process in place to conduct periodic reviews of Natus access/audit logs with sign-off(s).** Neurology clinic does not have documented procedures for auditing of Natus access logs. Per BCH-Oakland's Policy IT. Sec. 9.1, IAM process supports the control, logging, tracking, and auditing of user access. University of California policy (BFB-IS-3 and related standard: Event Logging § 12.4) Proper logging and monitoring are required practices for recording events and generating evidence.	Not reviewing audit or access logs periodically may allow nefarious activities or impermissible user actions go unnoticed for a prolonged time period allowing for unmonitored or malicious activities to take place.	Establish a user access audit policy in which the frequency, scope, and acceptable practices are defined. Set the audit requirements and determine the activity such as logins, application access, data access and changes made to the access user rights. Conduct regular audits to determine compliance with the user access policy.	IT Security will work with the Natus system administrator to develop a logging and monitoring plan. The logging plan, including frequency of review will be documented in the department's user access policy and procedures **Target Implementation Date:** October 31, 2023 **Responsible Party:** Executive Director, Ambulatory Service

F. Password Management

No.	Observation	Risk/Effect	Recommendation	Management Actions
8.	**Password Management practices for the Natus system do not meet BCH-Oakland's security requirements** Review of the password management practices for the Natus system identified the following: a) Password rules for password reset renewal, expiration and account lockout are not enforced. b) Password rules for minimal password length/complexity are not in line with IT Security policy and exception to policy for the Natus system was not in place. BCH-Oakland's "Password Management Policy" IT.Sec.16.1 stipulates the organizational requirements for strong passwords that includes: • a minimum length of 12 characters, maximum 128 characters • a minimum of 15 characters, maximum 128 characters for Privileged User Accounts • contain at least 3 of the 4-character types: Upper/Lower case, numbers, symbols • automatically expire on annual anniversary • Failed logons allowed before lockout - 5 failed attempts • Lockout duration - 15 minutes	Not meeting organizational password requirements in terms of complexity may lead to stale passwords with reduced strength, which would increase the risk of password cracks via brute-force methods. Failure to implement password reset renewal, or lockout policies could result in widespread account breaches or make it easier for hackers to compromise passwords by allowing them unlimited number of unrestricted password attempts to mount brute-force attacks to crack user passwords / authenticators.	Configure the Natus system to align with organizational password reset, renewal, expiration and account lockout policies. Configure Natus password settings and authenticators to align with BCH-Oakland/UCSF policies to facilitate standardization and approved level of security.	Upon integration with active directory, the user's active directory account that incorporates the BCH-Oakland's password security requirements will be used to access the Natus system. **Target Implementation Date:** October 31, 2023 **Responsible Party:** Executive Director, Ambulatory Service

G. Privileged Access

No.	Observation	Risk/Effect	Recommendation	Management Actions
9.	***Privileged access account(s)/request(s) for the Natus system are not formally approved and there is not a documented process to periodically review and recertify Natus privileged roles and Natus privileged (admin) accounts to facilitate the correct level of access and need for continued access.*** A privileged role has greater access to sensitive data, permissions, and privileges to perform critical tasks. Discussions with Natus system administrator identified that the department did not have a practice to document and approve privileged access accounts nor a process for periodic review and recertify Natus privileged roles. BCH-Oakland Policy IT Sec.9.1 Identity & Access Management Section G states that “Privileged accounts are restricted for persons requiring elevated access to sensitive information and/or highly controlled areas and functions of BCH Oakland information systems. The CISO must approve all requests for privileged access.” University of California “Account and Authentication Management Standards (§4.12)” stipulates that units must document and approve privileged access accounts needed to perform installations, updates or other administrative activities, and, if possible, only enable them to	Not having a documented process to periodically review and recertify Natus privileged roles and admin accounts may allow privilege creep or privilege abuse of separated / demoted / transferred / departed / inactive admin users.	Implement layered review process for approved elevated access requests. The different tiers of review may involve current administrators checking the requests granted by other administrators, then the outside site reviewer / auditor performing periodic reviews, then finally an internal audit team confirming the legitimacy of access requests. Develop a documented process to periodically review and recertify Natus privileged roles and accounts.	Workflow will be developed for integrating Natus onboarding and permission rights into the BCH-Oakland’s existing ServiceNow ticketing system to process user account requests that will provide a layered review process and be aligned with IT Security Policy **Target Implementation Date:** October 31, 2023 **Responsible Party:** Executive Director, Ambulatory Service

No.	Observation	Risk/Effect	Recommendation	Management Actions
	perform the specific administrative task(s) and then disable them.			

V. OPPORTUNITIES FOR IMPROVEMENT

No.	Observation	Risk/Effect	Recommendation
1.	<u>**Session Management**</u>: ***Session management practices for the Natus system are not configured.*** Review of the Natus system's configuration identified the following: • The Natus system does not have a limit configured on the number of concurrent sessions allowed per user connecting / accessing the Natus system(s) / database. • Session inactivity timeout is not configured on the Natus system/database. NIST 800-53 AC-10 states that organizations may define the maximum number of concurrent sessions for system accounts globally, by account type, by account, or any combination thereof. NIST 800-53 AC-2 (5) states that inactivity logout is behavior or policy-based and requires users to take physical action to log out when they are expecting inactivity longer than the defined period	Lack of limitation on number of concurrent sessions allowed may impact server availability and result in denial-of-service (DoS) attacks / exhaustion of resources (e.g., connection pools). Lack of session inactivity timeout configuration may increase exposure to session-based attacks and allow compromise of valid session IDs via brute-force methods.	Assess the feasibility of configuring the Natus system to allow only limited concurrent sessions per user in accord with organizational policies and procedures. Review BCH-Oakland/UCSF standards on session inactivity and configure Natus in accordance with the standards (ex: automatically terminate session after 30 minutes of inactivity). If configuration is not possible, review other ways in which BCH-Oakland can establish controls to limit session length.
2.	<u>**Remote Access**</u> **Natus system does not have a configured / enabled concurrent-session access control for each user via Citrix**.	Not enabling concurrent-session control for each user may allow insider	Establish control/restriction on number of concurrent sessions for each user via Citrix. Number of sessions for one user should not exceed 3 at any time, and BCH-Oakland should establish a

	Review of Natus system showed there is no configuration in place on the limit of concurrent session for each user. NIST 800-53 AC-10 states that organizations may define the maximum number of concurrent sessions for system accounts globally, by account type, by account, or any combination thereof. For example, organizations may limit the number of concurrent sessions for system administrators or other individuals working in particularly sensitive domains or mission-critical applications.	attacks and exhaustion of connection resources (e.g., connection pools or server availability).	monitoring/notification application to facilitate no insider threats are occurring.