MEMORANDUM

TO: All NWFHN Leadership and Staff

THROUGH: Courtney Stanford, Chief Operating Officer
Sharron Washington, Regional Program Administrator

FROM: Charles F. Scherer, Director of Projects

DATE: March 25, 2026

SUBJECT: Directive Addendum – Authorization, Notification, & Access Controls for the NWFHN Incident Reporting (IR) System

REFERENCE: Attachment x1 to NWFHN Policy & Procedure 800-805 and 800-813. Access/Review/Notification; see also NWFHN Policy 900-910.

---

1. Purpose

This Executive Directive serves as an official addendum to NWFHN Policy & Procedure 800-805 and the NWFHN Incident Reporting (IR) Policy and Procedure. It establishes mandatory protocols for authorizing, managing, and auditing user access and automated notifications within the NWFHN Incident Reporting System. This directive applies to all NWFHN staff, regardless of department, work location, or employment status.

2. Employment Status Changes and Access Review

In strict conjunction with established NWFHN Policies and Procedures, and Human Resources protocols, **Information Technology (IT) must be notified** whenever a team member's employment or engagement status changes. This includes, but is not limited to:

- New hires and onboarding ***(notification within one business day)***
- Separations / terminations (voluntary or involuntary) ***(immediate notification)***
- Suspensions or restrictions of access ***(immediate notification)***
- Promotions, demotions, or transfers (including role changes within the same department) ***(notification within one business day)***
- Changes in contractual or affiliate status (consultants, interns, volunteers, students, or vendors with system access) ***(notification within one business day)***

Upon notification of any status change:

- The employee's **access rights and notification status** for the NWFHN Incident Reporting System shall be **immediately reviewed and updated accordingly**.
- Access must be limited strictly to the individual's current job duties and operational need-to-know.
- Any required removal or suspension of access must be executed without delay.

3. The Access and Notification Matrix

The official **NWFHN Access and Notification Matrix** is the controlling document that specifies:

- Which roles may view, create, edit, or close incident reports; and
- Which roles are included on automated incident notification distribution lists.

This matrix is:

- **Owned and maintained by IT** in coordination with the Director of Projects and the Director of Quality & Professional Development; and
- Updated whenever there are organizational, structural, or role-based changes that affect IR access or notifications.
- All extended leadership staff are responsible for reviewing the matrix at least quarterly and confirming that their team's access matches current business needs and this directive.

4. Authority of Access and Notification

Baseline authority to access the IR System and receive incident notifications is restricted to the following **leadership roles**:

- C-Suite Executives (Chief Executive Officer, Chief Operating Officer, Chief Financial Officer, Chief Clinical Officer, Chief Strategy/Compliance Officers, as applicable)
- Director of Projects, Director of Quality & Professional Development, or Regional or Circuit Administrator

Additional access may be requested and granted for staff whose job duties require incident visibility and/or action. In such cases:

- **Administrators, Operations Managers, Directors, the Human Resources Manager, and General Counsel** may request for any respective team member under their purview. Requests should be sent to the **Director of Projects and to the Director of Quality & Professional Development** concurrently to request access.
- **Chief Officers** may also transmit or endorse access approvals.

No staff member may self-authorize access or add themselves to any IR System distribution list.

5. Request and Approval Process

All requests to **grant, modify, or remove** an employee's IR System access or notification settings must follow a formal, documented workflow:

1. The requesting leader (or designee) submits an access request (e.g., via IT ticket, standardized form, or email to IT) stating:
    - Employee name and position;
    - Supervisor and department;
    - Specific access level requested (e.g., view-only, incident entry, supervisory review);
    - Business justification tied to job duties.
    - Specific incident types requested

2. The request must be **approved by at least one** of the following authorities in the employee's chain of command:
    - Director
    - Administrator
    - Human Resources Manager
    - General Counsel
    - Chief Officer
    - Operations Manager

3. IT will only implement access changes upon receipt of documented approval from an authorized approver. All approvals must be retained in accordance with NWFHN records retention standards.

6. Internal Incidents Involving Employees or Affiliates

Incident Reports describing events involving **internal NWFHN employees or affiliates** (including interns, volunteers, or students) are considered **sensitive confidentiality matters** and must be handled with strict discretion.

- These reports are subject to all applicable provisions of NWFHN Policy & Procedure 800-805 and any referenced HR, Compliance, and Privacy policies.
- Access and notification privileges for employee/affiliate incidents are **further restricted** and may **only** be authorized by:
    - Chief Executive Officer (CEO)
    - Chief Operating Officer (COO)
    - Chief Financial Officer (CFO)

No other staff member may expand access or share details of an employee/affiliate incident outside of the approved distribution without express authorization from one of the above C-Suite officers and consistent with applicable law and policy.

7. Quarterly Compliance Review and Emergency Access Actions

To ensure **systemic security, confidentiality, and audit-readiness**, the following oversight is mandatory:

- **Quarterly Access Audit**
    - On at least a quarterly basis, the IT Department and the NWFHN Expanded Leadership Team will jointly review:
        - The current Access and Notification Matrix; and
        - The list of individuals with IR System accounts and/or notifications.

The goal is to verify that each individual's access level is appropriate, necessary, and consistent with this directive and NWFHN Policies 800-805, 800-813, and 900-910 (see www.nwfhealth.org).

- **Emergency Termination or Suspension of Access**
    - IT must be notified **immediately** whenever access needs to be terminated or suspended due to a **safety, security, or risk scenario**, including:
        - Allegations of serious misconduct;
        - Suspected fraud, waste, or abuse;
        - Active internal investigations; or
        - Known or suspected security incidents.

- This obligation applies **at all times**, including **after hours, weekends, and non-NWFHN business days**. Leaders must not delay emergency access actions until the next business day.

8. Directive Effect

This memorandum:

- Has the full force of an **executive directive** and is incorporated by reference into NWFHN Policy & Procedure 800-805;
- Shall govern NWFHN IR System access, review, and notification practices unless and until superseded in writing by updated policy or a subsequent executive directive; and

- Must be distributed to all leaders and staff with Incident Reporting responsibilities and retained as an attachment to the applicable Policy & Procedure.

For questions about this directive or its implementation, please contact the Director of Projects Charles Scherer or Director of Quality & Professional Development Sonja King.