myAvatarNX – Access & Use for Contacted Providers

01/7/2025

Purpose: This document explains how employees at a contracted residential facility, which includes CRU, SUD Residential (3.1 and 3.5), and Transitional Living (TL) placement, can gain access myAvatarNX.

Contents

Contracted Provider User Access On-Boarding

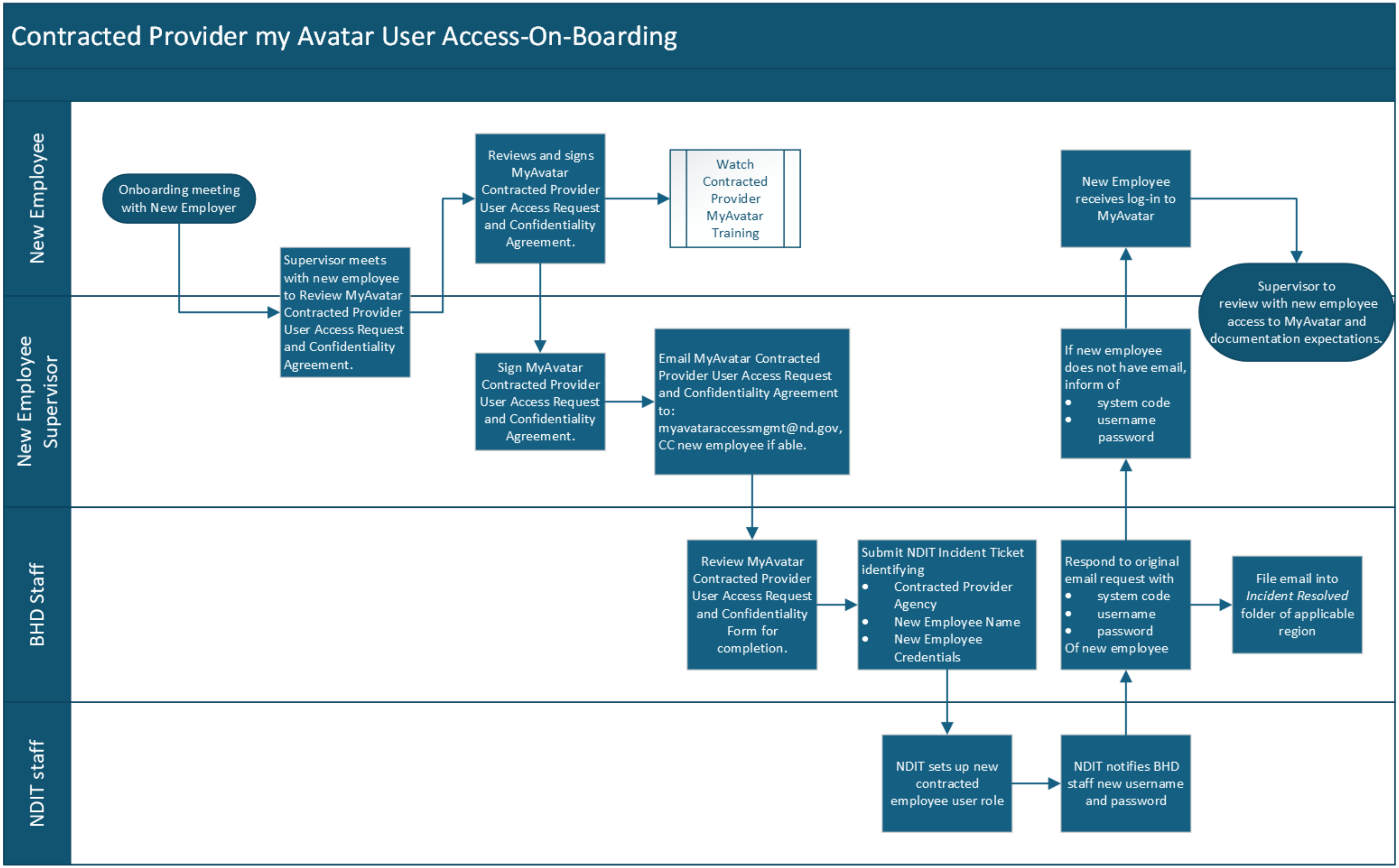
The process flow on the following page provides an overview of how to obtain access when new employees at a contracted provider facility are hired who will be using the myAvatar system. It details the steps involved, the roles of different individuals, and the sequence of actions.

The diagram is divided into four vertical swim lanes, each representing a different role or department:

1. **New Employee:** This lane shows the actions and responsibilities of the new employee being onboarded.
2. **New Employee Supervisor:** This lane represents the supervisor of the new employee, who is responsible for reviewing and approving certain aspects of the onboarding process.
3. **BHD Staff:** This lane refers to staff from the Behavioral Health Division, who play a role in the onboarding and access provisioning process.
4. **NDIT Staff:** This lane represents the staff from the North Dakota Information Technology (NDIT) department, who are responsible for setting up user accounts and managing access to the myAvatar system.

Key Steps in the Onboarding Process:

1. **Onboarding Meeting**: The process begins with an onboarding meeting between the new employee and their supervisor.
2. **myAvatar User Access Request:** The new employee and their supervisor review and sign the myAvatar User Access Request and Confidentiality Agreement.
3. **Email to myAvatar Access Management:** The supervisor emails the completed myAvatar User Access Request and Confidentiality Agreement to myavataraccessmgmt@nd.gov, including the new employee's credentials.
4. **Review myAvatar User Access Request:** The BHD staff reviews the completed myAvatar User Access Request and Confidentiality Agreement.
5. **Submit NDIT Incident Ticket:** The BHD staff submits an incident ticket to identify the agency, contracted provider, new employee name, and credentials.
6. **NDIT Sets Up User Account**: The NDIT staff sets up a new user account for the contracted employee in the myAvatar system.
7. **NDIT Notifies BHD Staff**: The NDIT staff notifies the BHD staff of the new username and password.
8. **Send Email to New Employee**: The BHD staff sends an email to the new employee, or supervisor if new email does not have a work e-mail, with their username and password.
9. **New Employee Receives Login:** The new employee receives their login credentials for the myAvatar system.
10. **Supervisor Reviews with New Employee:** The supervisor reviews with the new employee their access to myAvatar and documentation expectations.


Contracted Provider my Avatar User Access-On-Boarding
New Employee
New Employee Supervisor
BHD Staff
NDIT staff
Onboarding meeting with New Employer
Supervisor meets with new employee to Review MyAvatar Contracted Provider User Access Request and Confidentiality Agreement.
Reviews and signs MyAvatar Contracted Provider User Access Request and Confidentiality Agreement.
Watch Contracted Provider MyAvatar Training
Sign MyAvatar Contracted Provider User Access Request and Confidentiality Agreement.
Email MyAvatar Contracted Provider User Access Request and Confidentiality Agreement to: myavataraccessmgmt@nd.gov, CC new employee if able.
Review MyAvatar Contracted Provider User Access Request and Confidentiality Form for completion.
Submit NDIT Incident Ticket identifying
• Contracted Provider Agency
• New Employee Name
• New Employee Credentials
NDIT sets up new contracted employee user role
NDIT notifies BHD staff new username and password
Respond to original email request with
• system code
• username
• password
Of new employee
File email into Incident Resolved folder of applicable region
If new employee does not have email, inform of
• system code
• username password
New Employee receives log-in to MyAvatar
Supervisor to review with new employee access to MyAvatar and documentation expectations.

Contracted Provider Training Resources

myAvatarNX 101 This training provides an overview of the myAvatarNX platform

myAvatarNX- Navigation for Contracted Providers

myAvatarNX- Residential Face Sheet Report

myAvatarNX- Residential Shift Note

myAvatarNX- Vitals Entry

myAvatarNX- CIWA Form and Reports

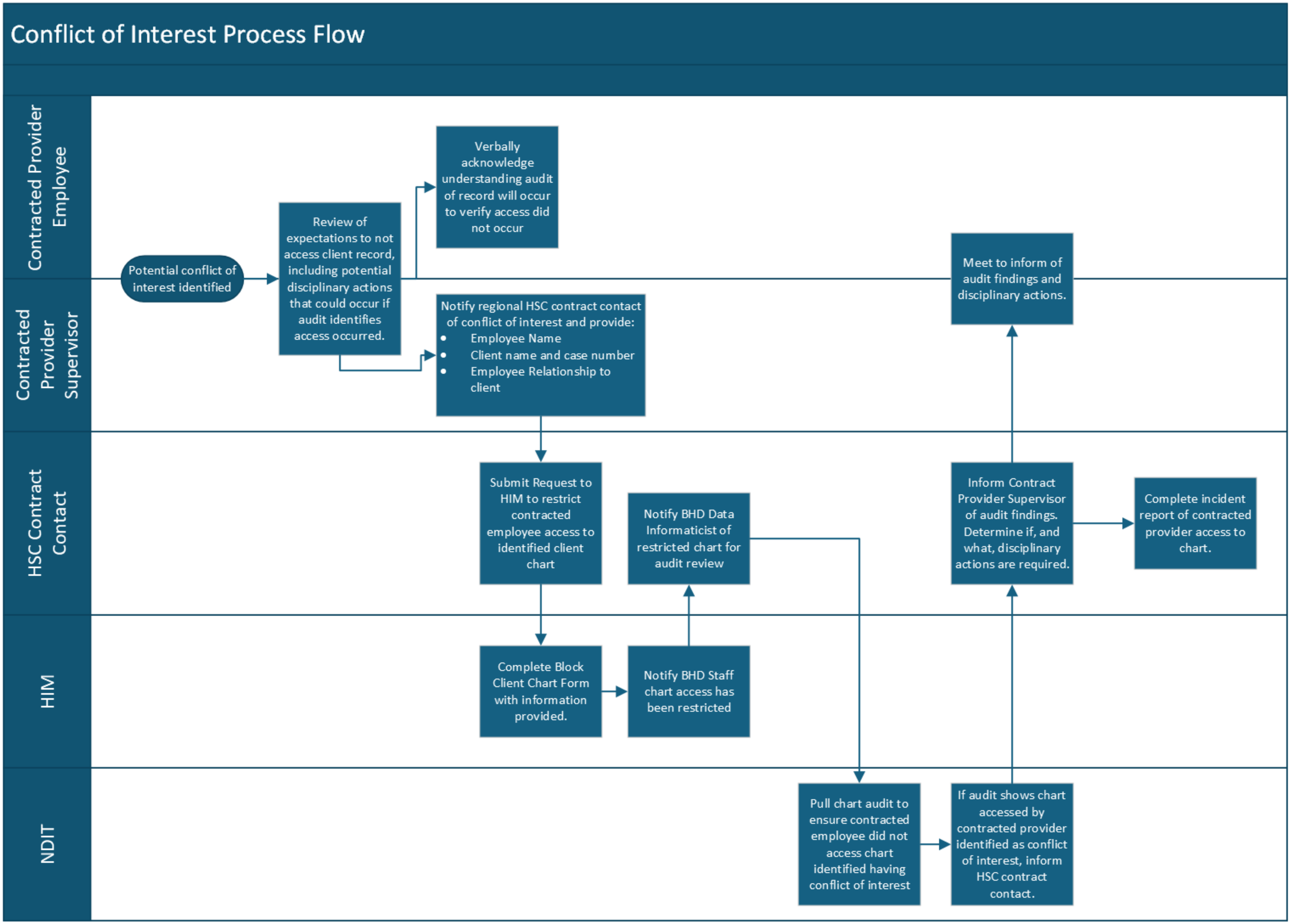
myAvatarNX- COWS

myAvatarNX- Stanley Brown Safety Plan Report

Contracted Provider Conflict of Interest

This swim lane diagram on the following page outlines the steps taken to address potential conflicts of interest when a contracted provider employee may have access to a client's medical record due to a personal relationship. Below are the specific steps for managing a conflict of interest.

1. **Potential Conflict of Interest Identified:** The process starts when a potential conflict of interest is identified. This could happen through various means, such as a supervisor noticing a personal relationship between an employee and a client.
2. **Review of Expectations and Acknowledgement:** The contracted provider employee is informed about the expectations regarding accessing client records and the potential disciplinary actions that could occur if access is found to have taken place.
   The employee verbally acknowledges their understanding and that an audit of their access will be conducted.
3. **Notification of Regional HSC Contract Contact:** The contracted provider supervisor notifies the regional HSC contract contact about the potential conflict of interest. The supervisor provides the employee name, client name and case number, and the employee's relationship to the client.
4. **Restricting Employee Access to Identified Client Chart:** The HSC contract contact submits a request to the Health Information Management (HIM) department to restrict the contracted employee's access to the identified client's chart. The HIM department completes a "Block Client Chart" form with the provided information. The HIM department notifies the BHD Data Informaticist of the restricted chart for audit review.
5. **Chart Audit:** The BHD Data Informaticist pulls the chart audit to ensure the contracted employee did not access the chart.
6. **Audit Findings and Disciplinary Actions:** If the audit shows the chart was not access by the contracted employee, the process ends. If the audit shows the chart was accessed, the supervisor is informed of the audit findings. The supervisor determines if and what disciplinary actions are required. The supervisor informs the HSC contract contact of the audit findings and any disciplinary actions taken.
7. **Completing Incident Report:** The supervisor completes an incident report of the contracted provider's access to the chart.


Conflict of Interest Process Flow
Contracted Provider Employee
Contracted Provider Supervisor
HSC Contract Contact
HIM
NDIT
Potential conflict of interest identified
Review of expectations to not access client record, including potential disciplinary actions that could occur if audit identifies access occurred.
Verbally acknowledge understanding audit of record will occur to verify access did not occur
Notify regional HSC contract contact of conflict of interest and provide:
• Employee Name
• Client name and case number
• Employee Relationship to client
Submit Request to HIM to restrict contracted employee access to identified client chart
Complete Block Client Chart Form with information provided.
Notify BHD Staff chart access has been restricted
Notify BHD Data Informaticist of restricted chart for audit review
Pull chart audit to ensure contracted employee did not access chart identified having conflict of interest
If audit shows chart accessed by contracted provider identified as conflict of interest, inform HSC contract contact.
Inform Contract Provider Supervisor of audit findings. Determine if, and what, disciplinary actions are required.
Complete incident report of contracted provider access to chart.
Meet to inform of audit findings and disciplinary actions.

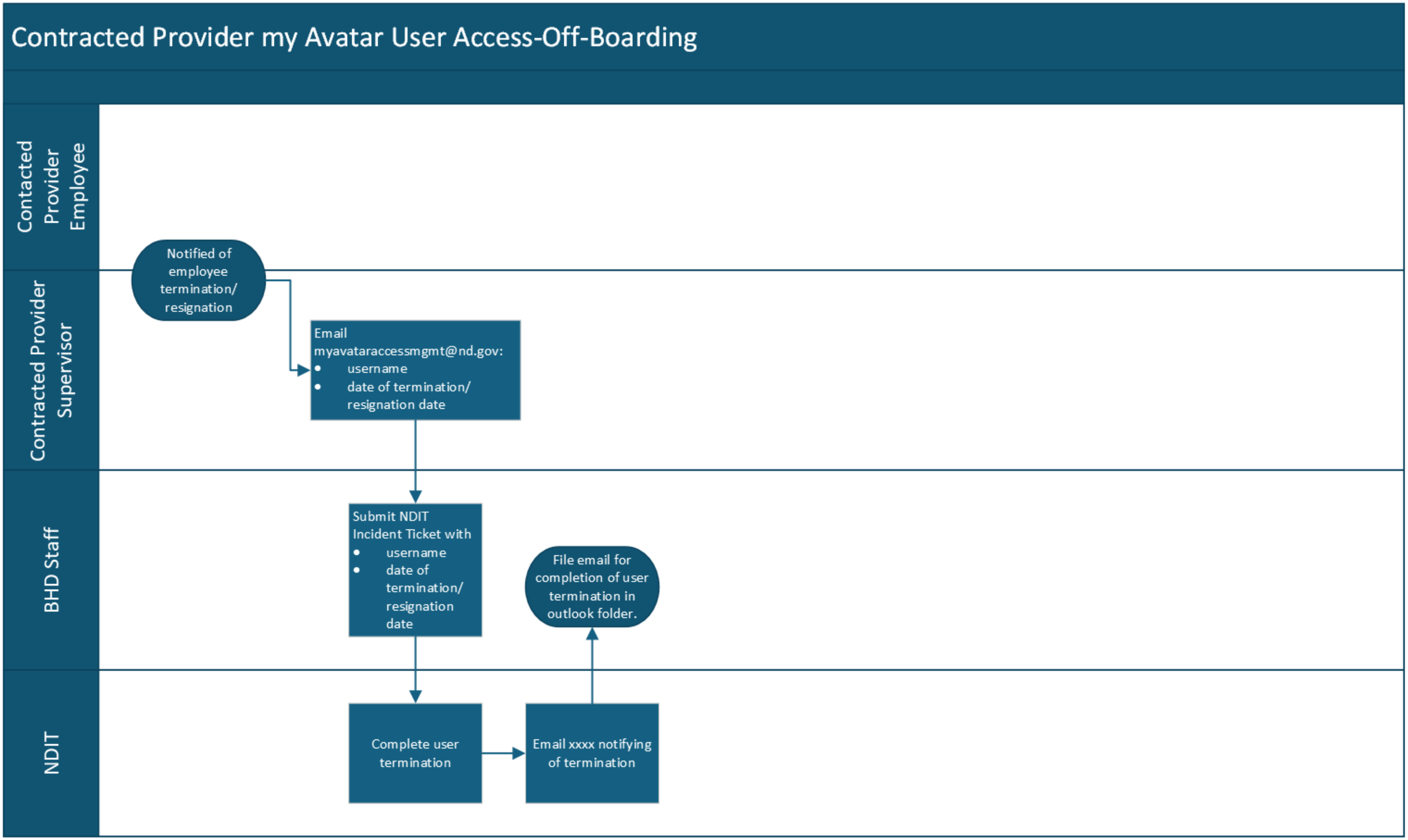
Contracted Provider User Access Off-Boarding

The process flow steps for removing access to myAvatar when a staff member leaves employment are provided ont eh following page. This swim lane diagram outlines the off-boarding process for employees at a contracted provider who have access to the myAvatar system. It details the steps involved, the roles of different individuals, and the sequence of actions when an employee terminates or resigns.

Key Steps in the Off-boarding Process:

1. **Notification of Employee Termination/Resignation:** The process begins when the supervisor is notified of the employee's termination or resignation. Contracting providers must notify the BHD of the termination no later than one (1) business day
2. **Email to myavataraccessmgmt@nd.gov:** The supervisor emails myavataraccessmgmt@nd.gov, including the Agency Name, staff member's name, region they worked in, username and date of termination/resignation.
3. **Submit NDIT Incident Ticket:** The BHD staff submits an incident ticket to NDIT with the username, date of termination/resignation.
4. **Complete User Termination:** The NDIT staff completes the user termination in the MyAvatar system.
5. **Email Notifying of Termination:** The NDIT staff sends an email notifying of the termination.

File Email for Completion of User Termination: The BHD staff files an email for completion of user termination in an Outlook folder


Contracted Provider my Avatar User Access-Off-Boarding
Contacted Provider Employee
Contracted Provider Supervisor
BHD Staff
NDIT
Notified of employee termination/ resignation
Email myavataraccessmgmt@nd.gov:
• username
• date of termination/ resignation date
Submit NDIT Incident Ticket with
• username
• date of termination/ resignation date
File email for completion of user termination in outlook folder.
Complete user termination
Email xxxx notifying of termination