Database Security Application

DATABASE SECURITY APPLICATION (DSA)
APPROVER TRAINING MANUAL

State of Michigan
Department of Health and Human Services

Last Updated: August 2020

Table of Contents

1   Introduction

1.1 About the DSA

The Database Security Application (DSA) allows users to securely request access to Michigan Department of Health and Human Services (MDHHS) applications [e.g., CareConnect360, Data Warehouse, Community Health Automated Medicaid Processing System (CHAMPS)]. All application access requests progress through a review and approval cycle* (*Figure 1.1.1*), with each phase and outcome tracked within the DSA.
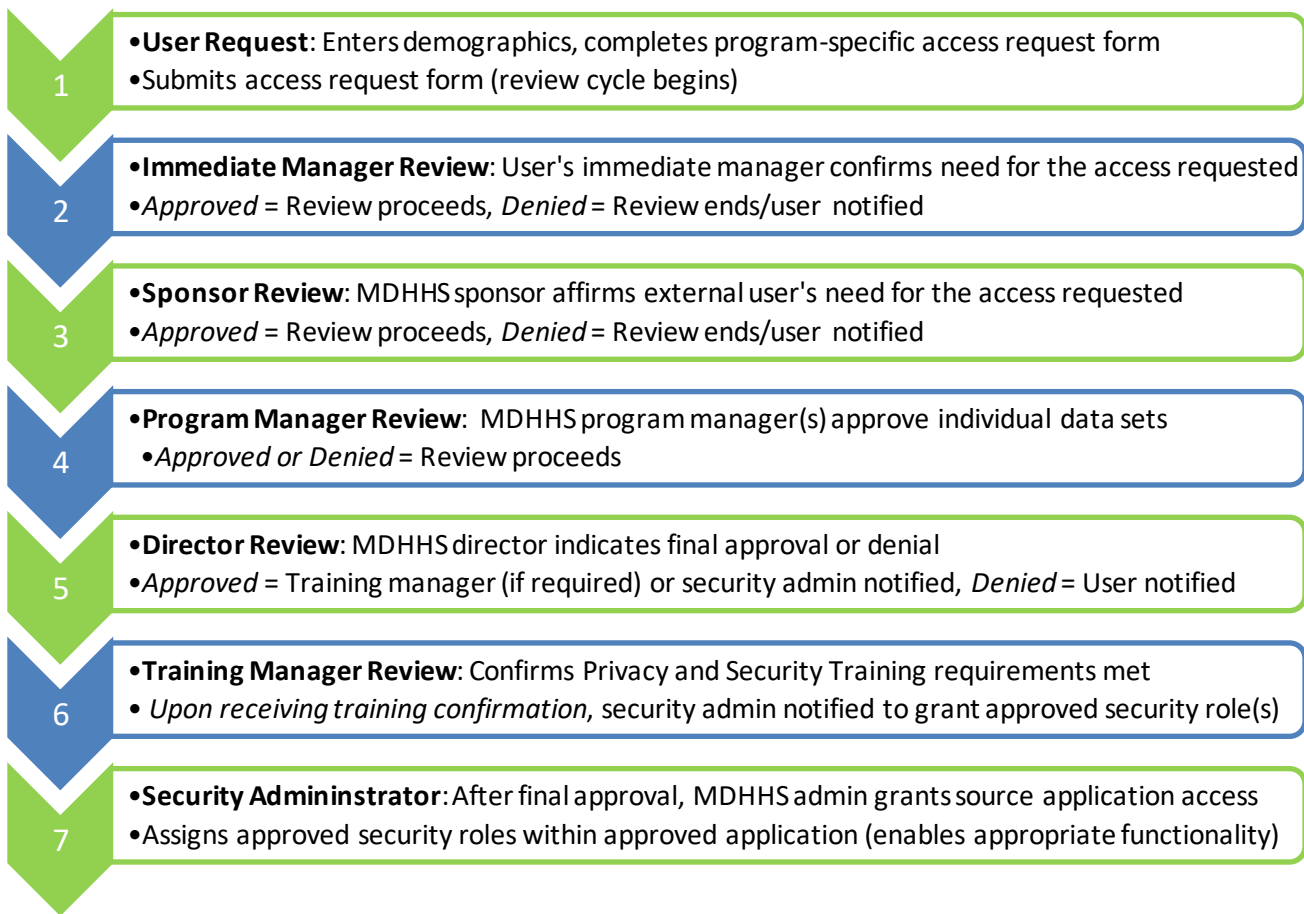
1
- **User Request**: Enters demographics, completes program-specific access request form
- Submits access request form (review cycle begins)

2
- **Immediate Manager Review**: User's immediate manager confirms need for the access requested
- *Approved* = Review proceeds, *Denied* = Review ends/user notified

3
- **Sponsor Review**: MDHHS sponsor affirms external user's need for the access requested
- *Approved* = Review proceeds, *Denied* = Review ends/user notified

4
- **Program Manager Review**: MDHHS program manager(s) approve individual data sets
- *Approved or Denied* = Review proceeds

5
- **Director Review**: MDHHS director indicates final approval or denial
- *Approved* = Training manager (if required) or security admin notified, *Denied* = User notified

6
- **Training Manager Review**: Confirms Privacy and Security Training requirements met
- *Upon receiving training confirmation*, security admin notified to grant approved security role(s)

7
- **Security Admininstrator**: After final approval, MDHHS admin grants source application access
- Assigns approved security roles within approved application (enables appropriate functionality)

Figure 1.1.1: MDHHS Application Access Request – General DSA Review and Approval Cycle

* Not all access requests require all review levels, and some applications use different terminology for their review levels.

An application access request automatically advances through the workflow as each reviewer records approval or denial. These actions trigger email notifications which are sent to alert the next required reviewer, or inform the user when denied. Users are able to check the status of their request at any point during the process. Access is granted by the Security Admin only after MDHHS final approval.

OPTUM™

1.2 MDHHS Applications Requested Through the DSA

Users request access to the following MDHHS applications using the DSA access request process.

- Benefits Monitoring Program (BMP)
- Business Objects Community (BOC)
- CareConnect360 (CC360)
- Community Health Automated Medicaid Processing System (CHAMPS)
- Children's Special Health Care Services (CSHCS)
- CMS Waiver Applications Portal
- Departmental Work Intake Process (DWIP)
- Master Person Index (MPI)
- MDHHS Document Management System (DMS/FileNet)
- MDHHS-Health Data Warehouse (DW)
- Medicaid Statistical Information System (MSIS)
- Michigan Adult Integrated Management System (MiAIMS)
- Michigan Care Improvement Registry (MCIR)
- Michigan Statewide Automated Child Welfare Information System (MiSACWIS)
- Pharmacy Cross-Reference Application (XDR)
- Siebel CRM
- Waiver Support Application (WSA)

1.3 Access Approval Levels

Approvers are responsible for reviewing user-submitted requests for access to the MDHHS applications identified in 1.2 MDHHS Applications Requested Through the DSA. All approvers should have at least one backup approver assigned for each approval level for which they are responsible. Please reference 7.3 Assign Backup Approvers and 7.4 Review Backup Approver Assignments for details.

Note: While the basic steps remain the same, some MDHHS applications use different titles for the access approval levels listed below. For example, MiSACWIS approvers are known as Authorized Requestors, Secondary Approvers, Local Office Security Coordinators, Application Security, Exception Reviewers, and Exception Managers.

Immediate Manager

The Immediate Manager works closely with the user requesting access to the MDHHS application, and understands the user's business needs. The Immediate Manager begins the review process by affirming that the user requires access to the requested MDHHS application to complete their job duties.

MDHHS Sponsor

The MDHHS Sponsor works closely with external (non-MDHHS) organizations, and understands the organization's access needs. For these organizations, the MDHHS Sponsor continues the review process by confirming the external user's need for access to the requested MDHHS application.

Program Manager

Individual data sets within an MDHHS application may be approved by different Program Managers (in the DSA known as Data Managers, Profile Managers, Program Managers, Report Managers, Role Managers, etc.). Each Program Manager abides by mandated criteria for allowing users access to specific data, and approves or denies access accordingly.

Director

The Director reviews all previous determinations made during the approval cycle, and indicates final approval or denial as appropriate. Upon approval, the request advances to the Training Manager step (if required) -or- the Security Administrator receives notification to finalize the request.

Training Manager

For applications containing Protected Health Information (PHI), the Training Manager step exists to confirm each user has completed required Privacy and Security Training before any approved security role(s) can be granted. Generally, this check is completed automatically during overnight batch processing. Occasionally the Training Manager needs to take manual action. Once training confirmation is received, the Security Administrator receives notification to finalize the request.

Security Administrator

The Security Administrator performs the final step to complete the access request. The Security Administrator does not make any access decisions, but rather, grants the already-approved access in the source application. First, the Security Administrator assigns the user's approved security role(s) within the source application. Then, the Security Administrator returns to the DSA and marks the user's access request as 'Complete', at which point the user is notified that their access has been granted.

1.4 Accessing the DSA

All users access the DSA through MILogin, the SOM single sign-on portal. MILogin is accessed one of two ways:

★ MDHHS users/contractors with a michigan.gov email use https://miloginworker.michigan.gov
★ All others use https://milogintp.michigan.gov

Complete the following steps to access the DSA:

1. Log into MILogin. The MILogin Home page displays (*Figure 1.4.1*).
2. Click **Database Security Application (DSA)**. The DSA Terms & Conditions display.
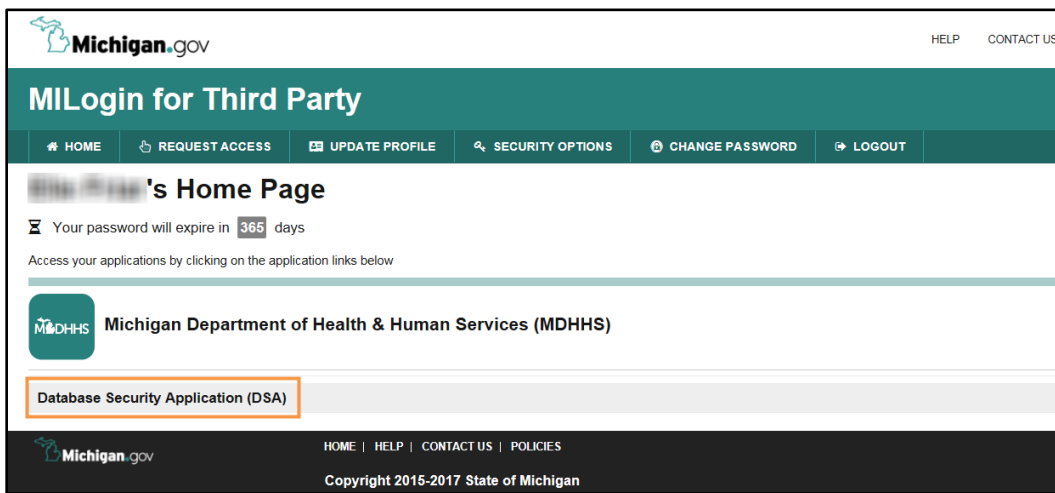
Figure 1.4.1: MILogin Home

3. Review the DSA Terms & Conditions and click **Acknowledge/Agree** (*Figure 1.4.2*). The Home page displays (*Figure 1.4.3, next page*).
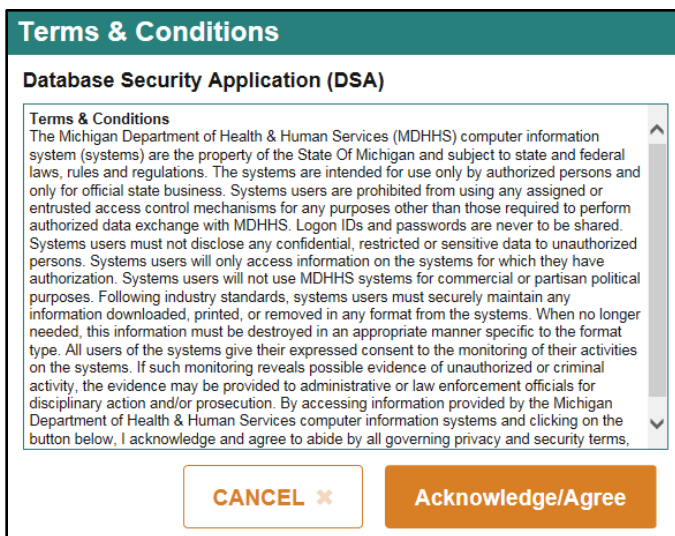
Figure 1.4.2: DSA Terms & Conditions

Figure 1.4.3: Home

1.5 Mozilla Firefox Warning

ATTENTION Mozilla Firefox users: To ensure optimal DSA performance, complete the following.

1. Access Mozilla Firefox.
2. In the address bar, enter **about:config**.
3. Press the keyboard **Enter** key.

   Note: A "This might void your warranty!" message may display. Click **I'll be careful, I promise!** to continue.

4. Locate **dom.allow_scripts_to_close_windows** in the *Preference Name* list.

   Note: Enter "dom.allow" in the *Search* field to easily locate.

5. Double-click the **dom.allow_scripts_to_close_windows** line to update the *Value* to 'true'; the default *Value* is 'false'.

   Note: The use of Internet Explorer is highly recommended for accessing the DSA; even after performing the above steps, some application links may not work with Mozilla Firefox.

2   Understanding DSA Functionality

2.1 Main Menu

All navigation begins in the DSA main menu. Selecting a main menu item such as ***Demographics*** navigates directly to the Demographics page. A main menu item containing a right-facing arrow (e.g., ***Review***) contains multiple sub-menu options; to display the sub-menu options, hover your cursor over the main menu item (*Figure 2.1.1*).

Figure 2.1.1: DSA Main Menu example

Main Menu Option	Function
Home	Returns the user to the DSA Home page
Demographics	Allows the user to enter organization and contact information
Request ▸	Provides access to application access request forms, the immediate manager role and organization manager role request forms, and My Backup Users where approvers set up their backup approvers
Review ▸	Accesses the approver's list of requests awaiting review, list of completed reviews, and if applicable, the approver's list of backup users to review
Manager ▸	Provides access to the options used to approve the immediate manager or organization manager role
Training ▸	Provides access to the most current DSA training materials such as step-by-step videos, job aids, frequently asked questions, and training manuals
Contact Email ▸	Provides a means for users to contact the administrator of each application requested through the DSA
Exit	Logs the user out of the DSA

Table 2.1.1: Main Menu Options

OPTUM™

2.2 Common DSA Functions

The DSA displays confirmation messages in green text when system actions are successfully performed. In contrast, error messages display in red text. In addition, the following common functions are found throughout the access review and approval process.

Common DSA Function	Purpose
Cancel	Navigates away from the current page without performing any action
Cancel-Return-Request-List	Returns the approver to the Reviewer Request List page without performing any action
Help	Accesses a window containing information explaining the page fields and functionality
Return-Some	During a review, allows the Director to return part(s) of the access request to the Program Manager(s) for additional consideration
Save-Goto-List	Saves a review determination and returns to the Reviewer Request List page
Save-Goto-Next	Saves a review determination and automatically advances to/opens the next access request on the Reviewer Request List page
Video Help	Accesses a video containing step-by-step instructions for reviewing the current access request form

Table 2.2.1: Common DSA Review/Approval Functions

2.3 DSA Email Notifications

Application Access Request

Throughout the access request review and approval cycle, email notifications are automatically generated and sent to the user and/or approver. In addition to providing important details, each email notification directs the recipient to access the DSA to check the request status or to take action.

Access Request Email Notification	Email Recipient
Request Submitted: Confirmation the application access request was submitted	User requesting access
Reviewer Notified: Alert informing the approver that an access request is awaiting their review *Note*: The recipient is automatically determined according to the most recent step completed in the review cycle (see Figure 1.1.1)	Immediate Manager, MDHHS Sponsor, Program Manager, Director, or Security Administrator
Request Approved: Notification that the access request was approved	User requesting access
Request Denied: Notification that the access request was denied	User requesting access

Table 2.3.1: Email Notifications – Application Access Request

Immediate Manager Request

Users request the Immediate Manager role using the DSA. Upon submitting the request, email notifications are automatically generated and sent to the user and/or approver.

Immediate Manager Request Email Notification	Email Recipient
Request Submitted: Confirmation the Immediate Manager role request was submitted	User requesting Immediate Manager role
Reviewer Notified: Alert informing the Organization Manager that an Immediate Manager role request is awaiting their review	Organization Manager
Request Approved: Notification that the Immediate Manager role request was approved/granted	User requesting Immediate Manager role
Request Denied: Notification that the Immediate Manager role request was denied	User requesting Immediate Manager role

Table 2.3.2: Email Notifications – Immediate Manager Request

Organization Manager Request

Users request the Organization Manager role using the DSA. Upon submitting the request, email notifications are automatically generated and sent to the user and/or approver.

Organization Manager Request Email Notification	Email Recipient
Request Submitted: Confirmation the Organization Manager role request was submitted	User requesting Organization Manager role
Reviewer Notified: Alert informing the organization's MDHHS Sponsor that an Organization Manager role request is awaiting their review	MDHHS Sponsor
Request Approved: Notification that the Organization Manager role request was approved/granted	User requesting Organization Manager role
Request Denied: Notification that the Organization Manager role request was denied	User requesting Organization Manager role

Table 2.3.3: Email Notifications – Organization Manager Request

3   Reviewing Application Access Requests

Steps outlining the general review process for all access approvers are included in this training manual. Application-specific review instructions are included in the training videos referenced below. A general review and approval cycle begins with the Immediate Manager Review, progresses through the MDHHS Sponsor Review (for external, non-MDHHS organizations), the Program Manager Review, and finally the Director Review.

Upon Director (final) approval, certain access requests advance to the Training Manager step to confirm Privacy and Security Training requirements have been met. Otherwise, the Security Administrator is notified to finalize the access request.

Note: *The Immediate Manager Review steps are the same for all access requests*. Please reference 3.1 Immediate Manager Review and the **Completing an Immediate Manager or Authorized Requestor Review** video for additional information.

The Security Administrator finalization steps are also the same for all access requests. Please reference 4 Finalizing the Access Request: Security Admin and the **Completing the Access Request – Security Administrator** video for additional information.

The remaining review levels and instructions differ for each application. Please reference the access request form-specific review steps in the training videos.

All training videos and transcripts are located in the **Training** menu under **Training View**. Select a **Form** from the list to access training materials for that specific access request form. Select '**General DSA**' in the **Form** list to locate the Immediate Manager/Authorized Requestor and Security Administrator training videos and transcripts.

Please reference the following training videos for application-specific access request review instructions:

- **Reviewing the BMP Access Request –** Approver & Director versions
- **Reviewing the BOC Access Request –** Approver & Director versions
- **Reviewing the CC360 Access Request –** Approver & Director versions
- **Reviewing the CHAMPS Access Request –** Approver & Director versions
- **Reviewing the CMS Access Request –** one version for ALL reviewers
- **Reviewing the CRM Access Request –** Approver & Director versions
- **Reviewing the CSHCS Access Request –** Approver & Director versions
- **Reviewing the DMS Access Request –** Approver & Director versions

- **Reviewing the DW Access Request –** Approver & Director versions
- **Reviewing the DWIP Access Request –** Approver & Director versions
- **Reviewing the MCIR Access Request –** Approver & Director versions
- **Reviewing the MiAIMS Access Request** – Immediate Manager & Sponsor versions
- **Reviewing the MiSACWIS Access Request –** Secondary Approver, LOSC, Application Security, Exception Reviewer, & Exception Manager versions
- **Reviewing the MPI Access Request –** Approver & Director versions
- **Reviewing the MSIS Access Request –** one version for ALL reviewers
- **Reviewing the WSA-AUT Access Request –** Approver & Director versions
- **Reviewing the WSA-B3W Access Request –** Approver & Director versions
- **Reviewing the WSA-CWP Access Request –** Approver & Director versions
- **Reviewing the WSA-HAB Access Request –** Approver & Director versions
- **Reviewing the WSA-HHB Access Request –** Approver & Director versions
- **Reviewing the WSA-ICO Access Request –** Approver & Director versions
- **Reviewing the WSA-MIC Access Request –** Approver & Director versions
- **Reviewing the WSA-SED Access Request –** Approver & Director versions
- **Reviewing the XDR Access Request –** one version for ALL reviewers

---

VIDEO TIPS: For your convenience, a written transcript accompanies each training video.

In addition all videos have user controls available including pause, stop, rewind, and fast forward. Note that you may need to maximize the video window and/or scroll to see the controls (and to see the Close link).

Press the ESC (escape) keyboard key or click Close to exit a video.

3.1 Immediate Manager Review

The Immediate Manager (a.k.a. Authorized Requestor) works closely with the user requesting application access, and understands the user's business needs. The Immediate Manager begins the review process by affirming that the user requires access to the requested MDHHS application to complete their job duties.

Complete the following steps to perform a review as an Immediate Manager:

1. Complete the steps in 1.4 Accessing the DSA.
2. Select **Review Requests** from the **Review** sub-menu (*Figure 3.1.1*).
    -or-
    Click Go To Review in the Request Pending Review(s) dashboard.
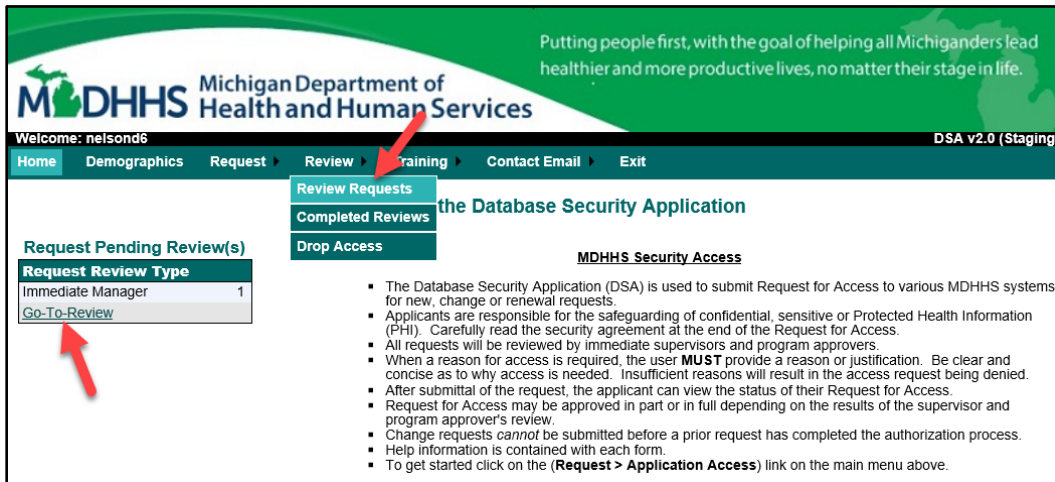
Figure 3.1.1: Home

3. Click Review beside the request to be reviewed (*Figure 3.1.2*). The Immediate Manager Review page displays.
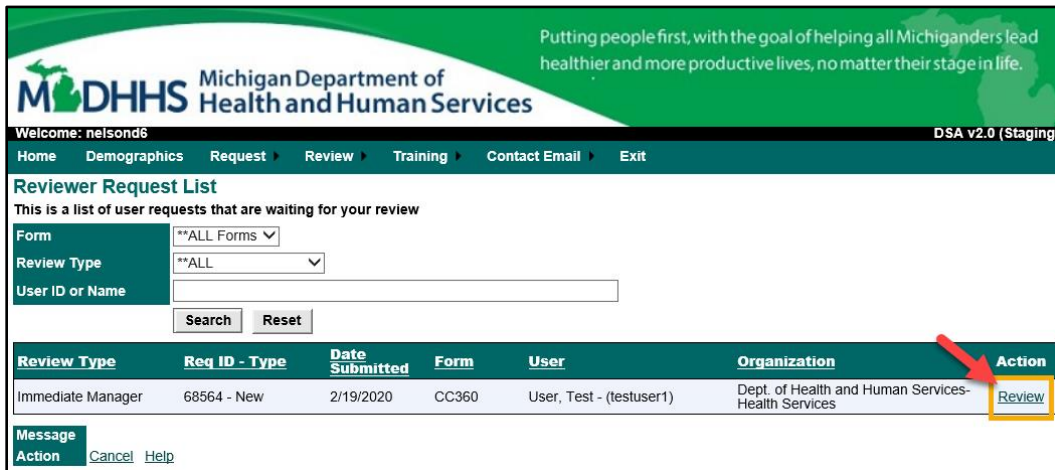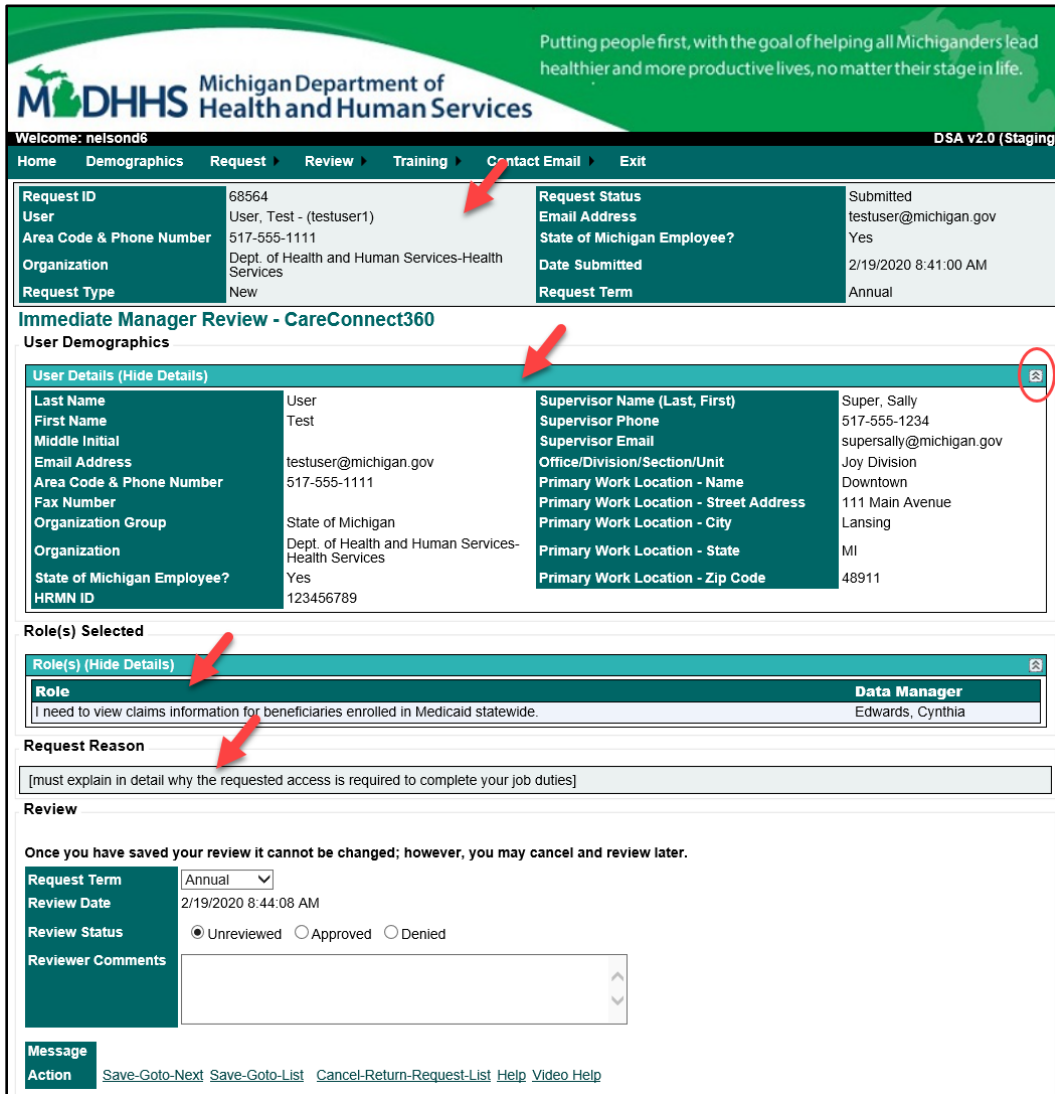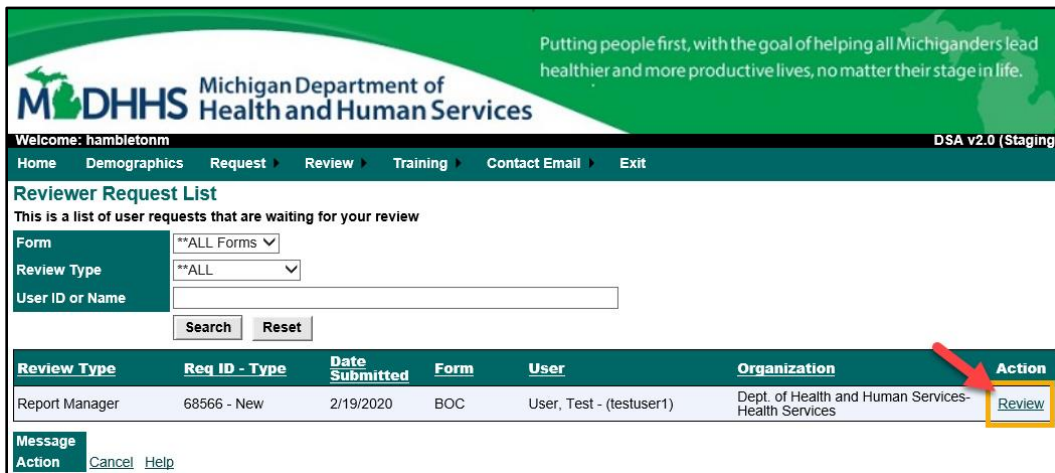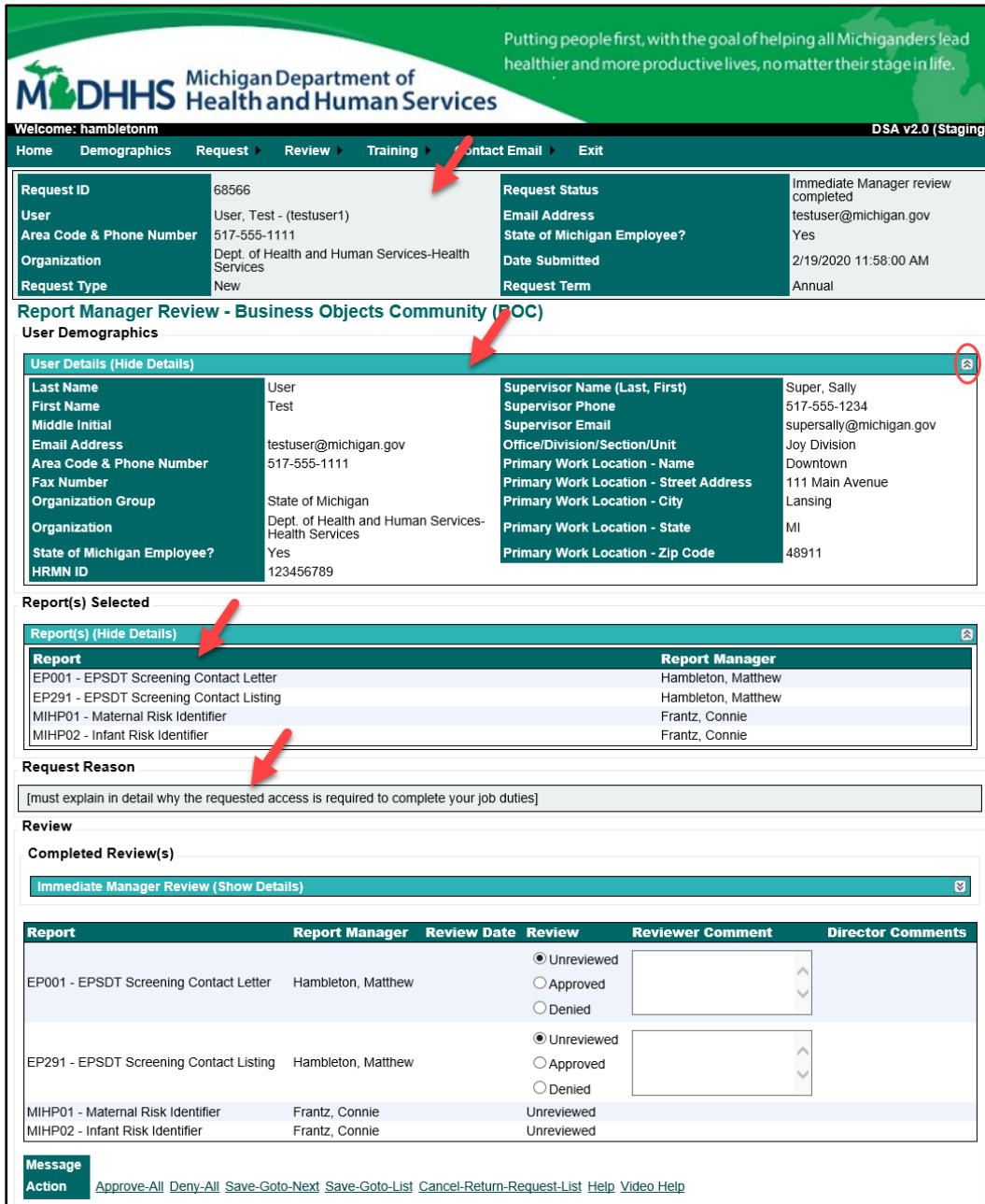

Figure 3.1.2: Reviewer Request List – Immediate Manager

Note: Use the search fields (*Figure 3.1.2, above*) to locate the request, if necessary.

4. Verify the user information (*Figure 3.1.3*).

5. Click the arrow beside **User Details** to expand and review additional user demographics.

6. Verify the requested documents/profiles/programs/reports/roles/user groups, and confirm the **Request Reason** explains the need.

Figure 3.1.3: Immediate Manager Review

7. Some applications allow for short-term access. If so, the ***Request Term*** field displays (*Figure 3.1.4*). To define the short-term request:

   a. Select 'ShortTerm' (default value is 'Annual'). The ***End Date*** field appears.

   b. Enter the ***End Date*** to indicate the length of short-term access being approved.
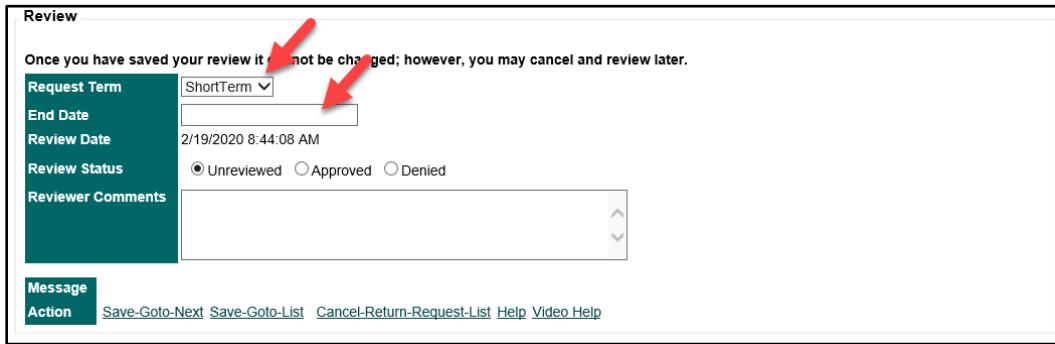
Figure 3.1.4: Immediate Manager Review – Short Term Access

8. To approve the access request, select the ***Approved*** radio button (*Figure 3.1.5*).

9. To deny the access request, select the ***Denied*** radio button.

10. Enter ***Reviewer Comments*** as appropriate. *Comments are required when denying*.

11. Click Save Goto Next to save the review, advance to the next access request awaiting review.
    -or-
    Click Save Goto List to save the review and return to the list of requests awaiting review.
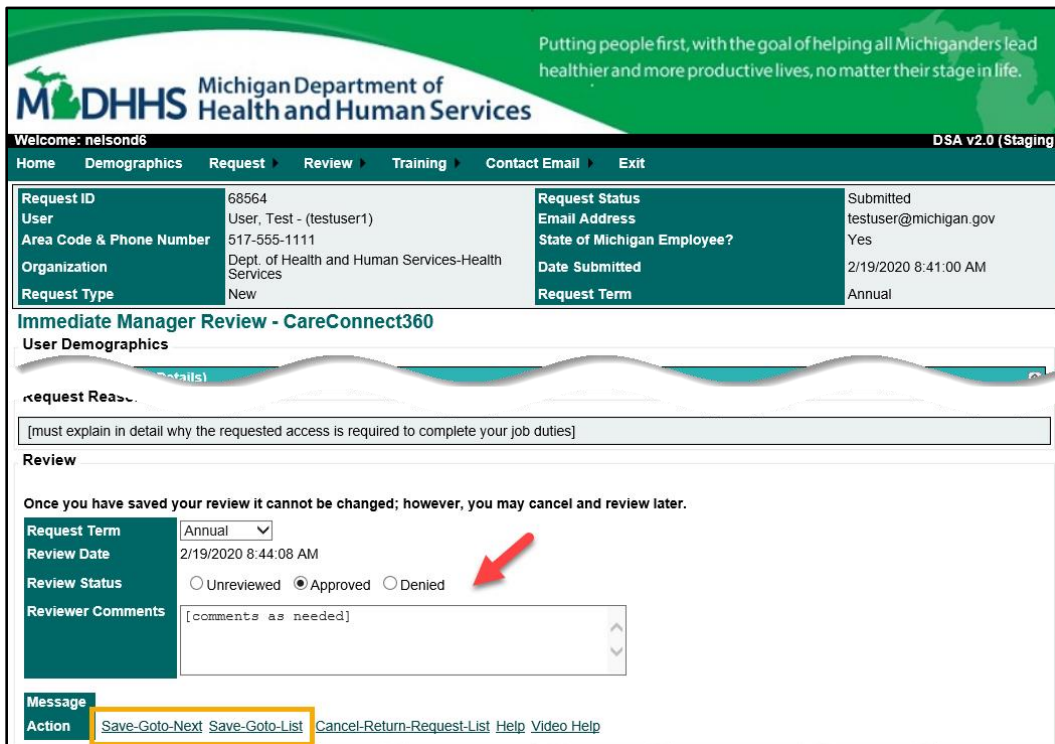
Figure 3.1.5: Immediate Manager Review

Note: **When approved**, the request automatically advances to the next required approver, and an email notification is sent informing the approver that an access request is awaiting review. **When denied**, the review ends and the user receives email notification.

OPTUM™

3.2 MDHHS Sponsor Review

The MDHHS Sponsor works closely with the external (non-MDHHS) organization, and understands the organization's access needs. The MDHHS Sponsor continues the review process by confirming the external user's need for access to the requested MDHHS application.

Complete the following steps to perform a review as an MDHHS Sponsor:

1. Complete the steps in 1.4 Accessing the DSA.
2. Select **Review Requests** from the **Review** sub-menu (*Figure 3.2.1*).
   -or-
   Click Go To Review in the Request Pending Review(s) dashboard.
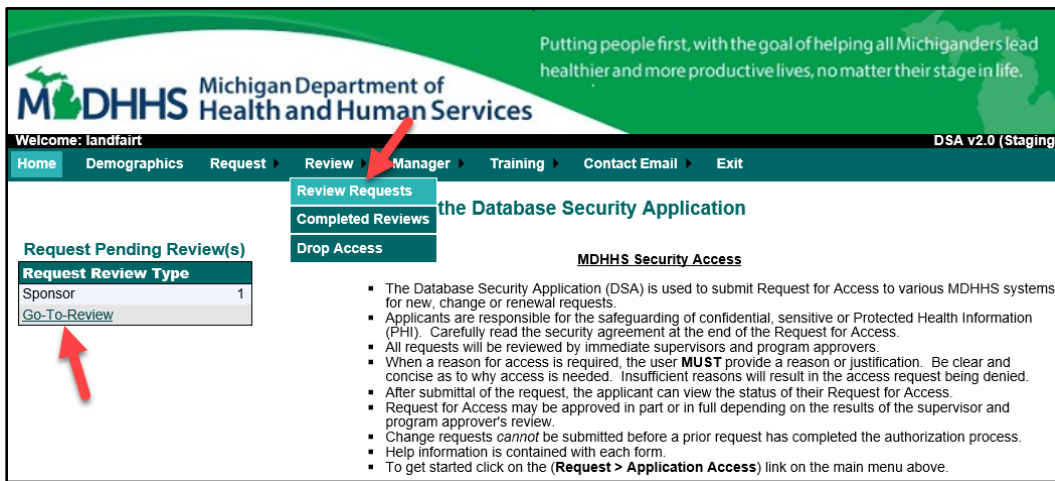
Figure 3.2.1: Home

3. Click Review beside the request to be reviewed (*Figure 3.2.2*). The Sponsor Review page displays.

> *Note*: Use the search fields to locate the request, if necessary.
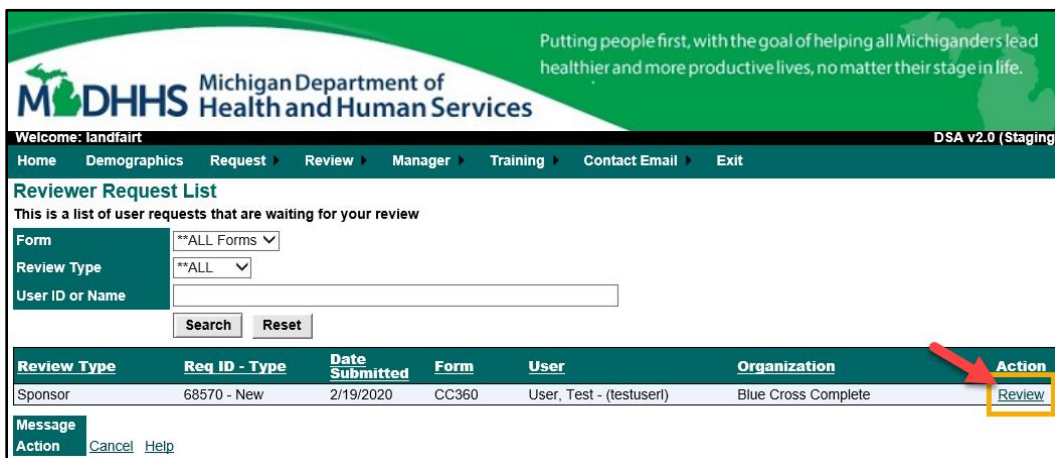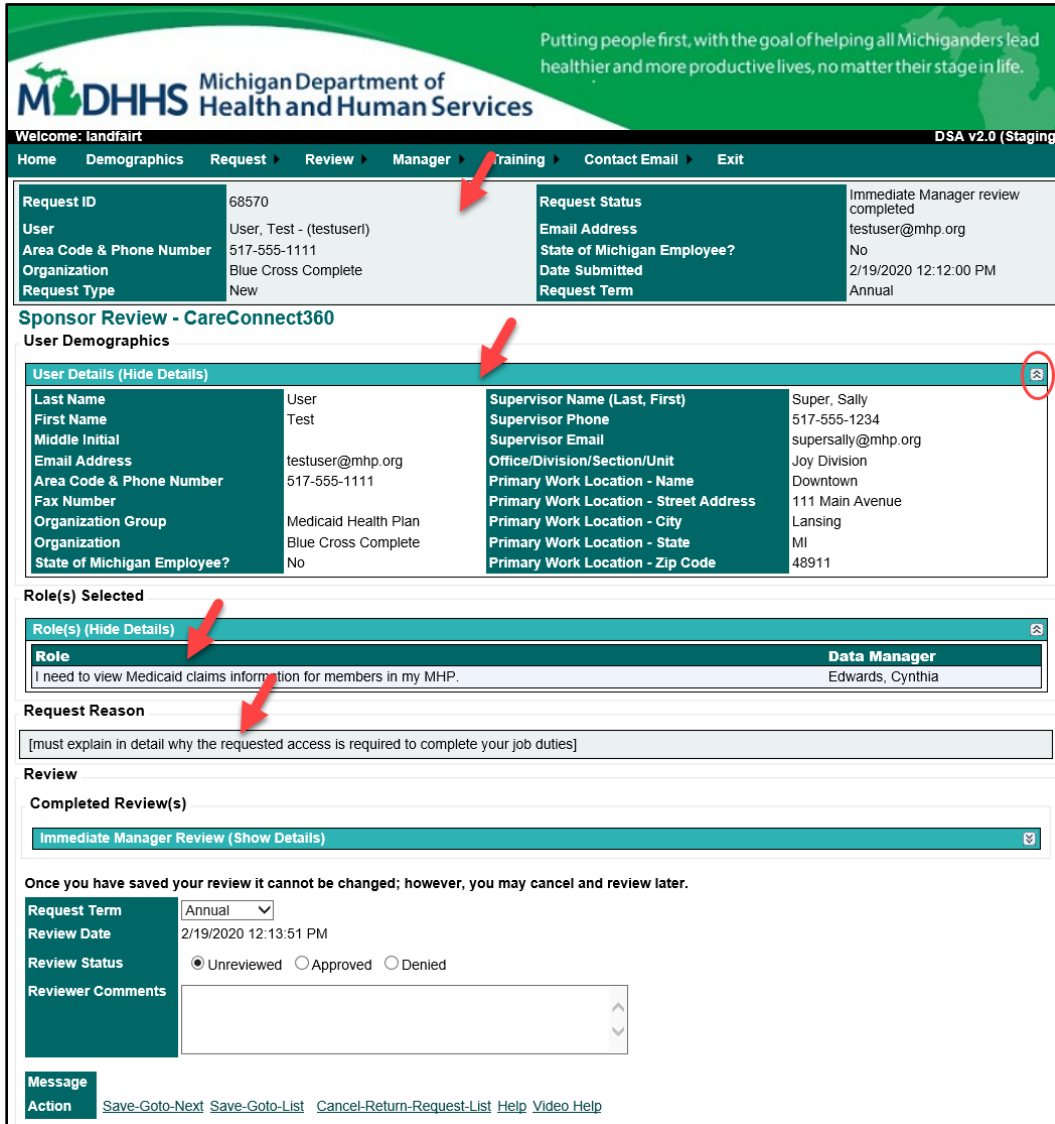
Figure 3.2.2: Reviewer Request List – Sponsor

4. Verify the user information (*Figure 3.2.3*).

5. Click the arrow beside **User Details** to expand and review additional user demographics.

6. Verify the requested documents/profiles/programs/reports/roles/user groups, and confirm the **Request Reason** explains the need.

Figure 3.2.3: Sponsor Review

7. Under **Completed Review(s)**, click the arrow beside **Immediate Manager Review** (or **Authorized Requestor Review**) to expand and review the Immediate Manager's determination (*Figure 3.2.4*).

Note: If there are any questions for the Immediate Manager, the name is a link. Click the link to email your questions.

Figure 3.2.4: Sponsor Review

7. Some applications allow for short-term access. If so, the ***Request Term*** field displays (*Figure 3.2.5*). To define the short-term request:

   a. Select or confirm 'ShortTerm' (default value is 'Annual').

   b. Enter or confirm the ***End Date*** to indicate the length of the short-term access being approved.

Figure 3.2.5: Sponsor Review – Short Term Access

8. To approve the access request, select the ***Approved*** radio button (*Figure 3.2.6*).

9. To deny the access request, select the ***Denied*** radio button.

10. Enter *Reviewer Comments* as appropriate. *Comments are required when denying*.

11. Click Save Goto Next to save the review, advance to the next access request awaiting review.
    -or-
    Click Save Goto List to save the review and return to the list of requests awaiting review.
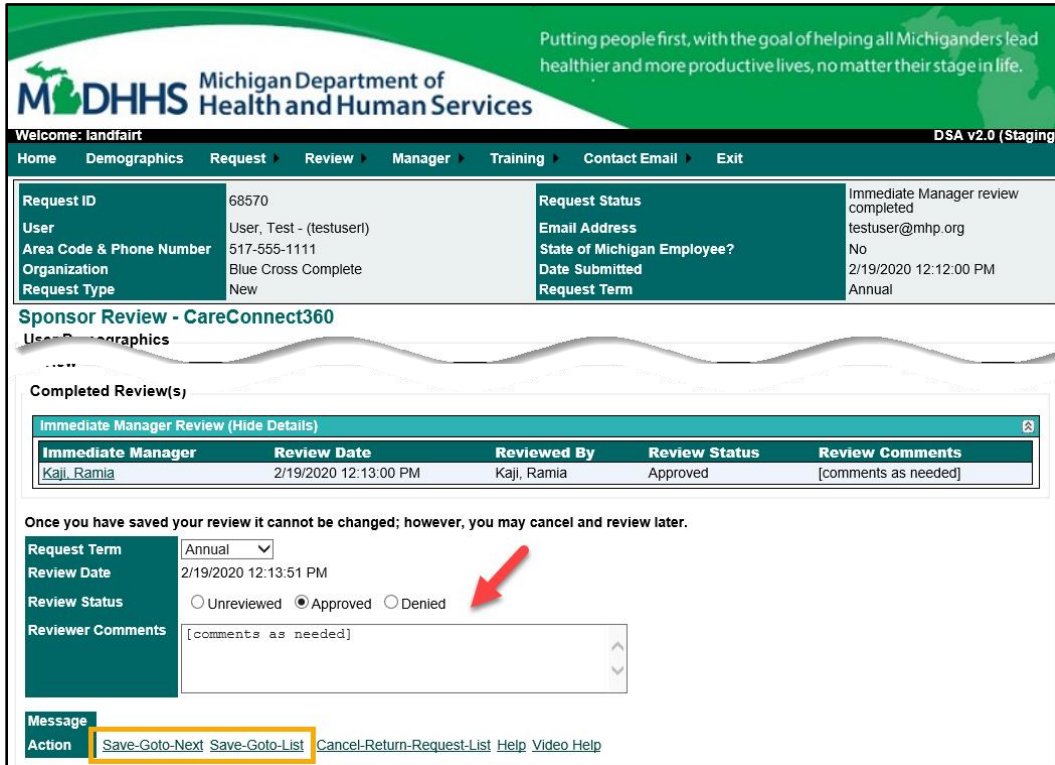
Figure 3.2.6: Sponsor Review

Note: **When approved**, the request automatically advances to the next required approver, and an email notification is sent informing the approver that an access request is awaiting review. **When denied**, the review ends and the user receives email notification.

3.3 Program Manager Review

Individual data sets within an application may be approved by different Program Managers (also known as Data Managers, Profile Managers, Program Managers, Report Managers, Role Managers, etc.). Each Program Manager abides by mandated criteria for allowing users access to specific data, and approves or denies access accordingly.

Complete the following steps to perform a review as a Program Manager:

1. Complete the steps in 1.4 Accessing the DSA.
2. Select **Review Requests** from the **Review** sub-menu (*Figure 3.3.1*).
    -or-
   Click Go To Review in the Requests Pending Review(s) dashboard.
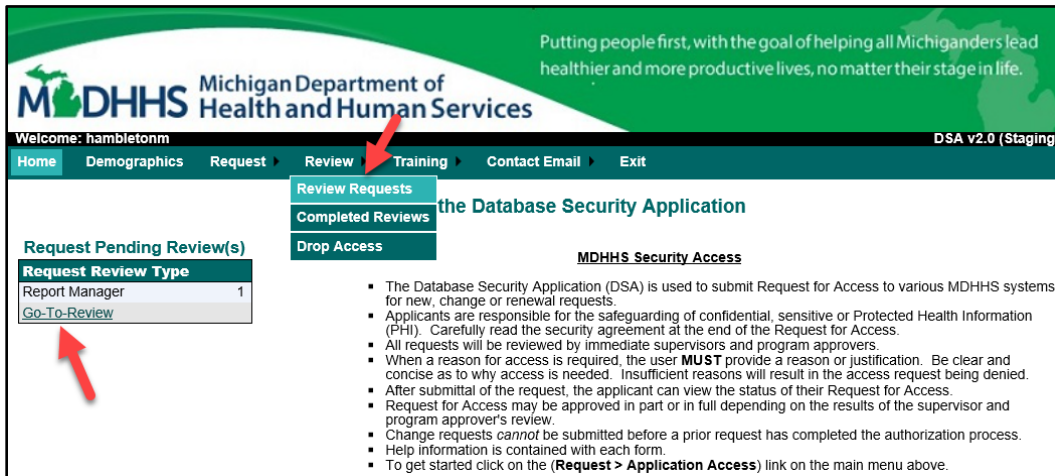
Figure 3.3.1: Home

3. Click Review beside the request to be reviewed (*Figure 3.3.2*). The Program Manager Review page displays.

Figure 3.3.2: Reviewer Request List – Program Manager (a.k.a. Report Manager, etc.)
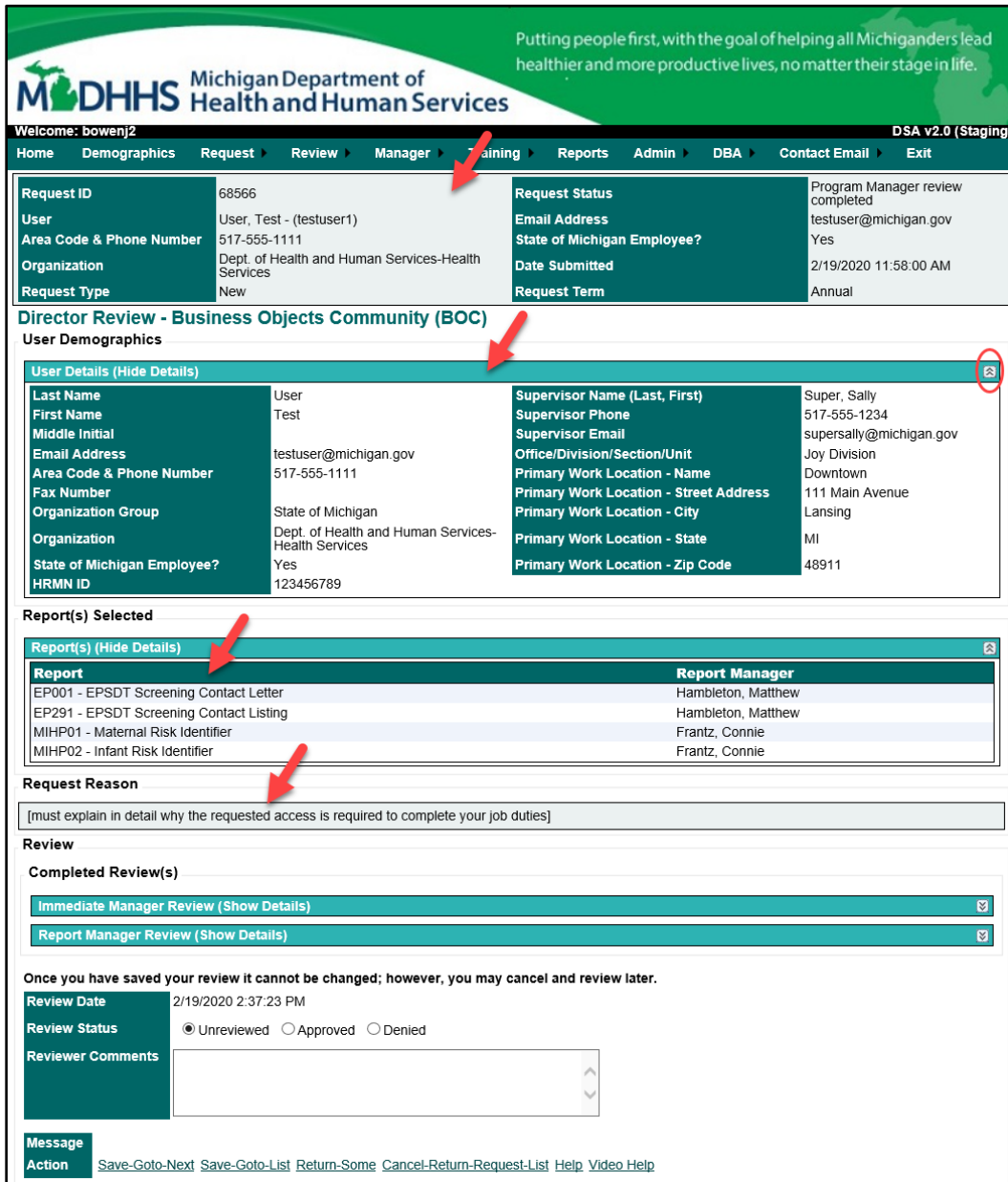
Note: Use the search fields (*Figure 3.3.2, above*) to locate the request, if necessary.

4. Verify the user information (*Figure 3.3.3*).

5. Click the arrow beside **User Details** to expand and review additional user demographics.

6. Verify the requested documents/profiles/programs/reports/roles/user groups, and confirm the **Request Reason** explains the need.

Figure 3.3.3: Program Manager Review

7. Under **Completed Review(s)**, click the arrow beside **Immediate Manager Review**, and **Sponsor Review** if applicable, to expand and review the Immediate Manager's and MDHHS Sponsor's determinations (*Figure 3.3.4*).

> *Note*: If there are any questions for the Immediate Manager, the name is a link. Click the link to email your questions.

Figure 3.3.4: Program Manager Review

> *Note*: In some instances, multiple Program Managers are responsible for approving the different data sets requested. This is indicated by the *Approved* and *Denied* radio buttons only appearing as active and available for the current approver.

8. To approve access to the document/profile/program/report/role/user group, select the **Approved** radio button (*Figure 3.3.5*).

9. To deny access to the document/profile/program/report/role/user group, select the **Denied** radio button.

10. Enter **Reviewer Comments** as appropriate. *Comments are required when denying*.

11. Click <u>Save Goto Next</u> to save the review, advance to the next access awaiting review.
    -or-
    Click <u>Save Goto List</u> to save the review and return to the list of requests awaiting review.

Figure 3.3.5: Program Manager Review

> *Note*: **Regardless of approval or denial**, once all Program Managers have completed their review the request automatically advances to the Director for final review and approval. An email notification is sent informing the Director that a request is awaiting review.

3.4 Director Review

The Director reviews all previous determinations made during the approval cycle, and indicates final approval or denial as appropriate. This action completes the review and approval portion of the access request process.

Upon final Director approval, the Security Administrator receives notification to finalize the access request (complete the process).

Note: For applications containing Protected Health Information (PHI), there is a Training Manager step prior to the Security Administrator step. The Training Manager step exists to confirm each user has completed required Privacy and Security Training before any approved security role(s) can be granted.

Complete the following steps to perform a review as a Director:
1. Complete the steps in 1.4 Accessing the DSA.
2. Select *Review Requests* from the *Review* sub-menu (*Figure 3.4.1*).
   -or-
   Click Go To Review in the Requests Pending Review(s) dashboard.

Figure 3.4.1: Home

OPTUM™
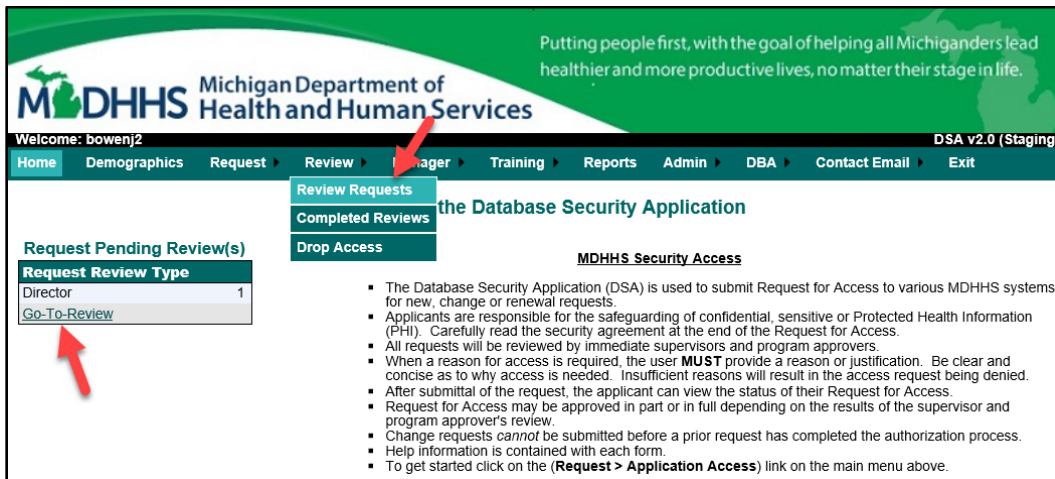
3. Click <u>Review</u> beside the request to be reviewed (*Figure 3.4.2*). The Director Review page displays.

> *Note*: Use the search fields to locate the request, if necessary.
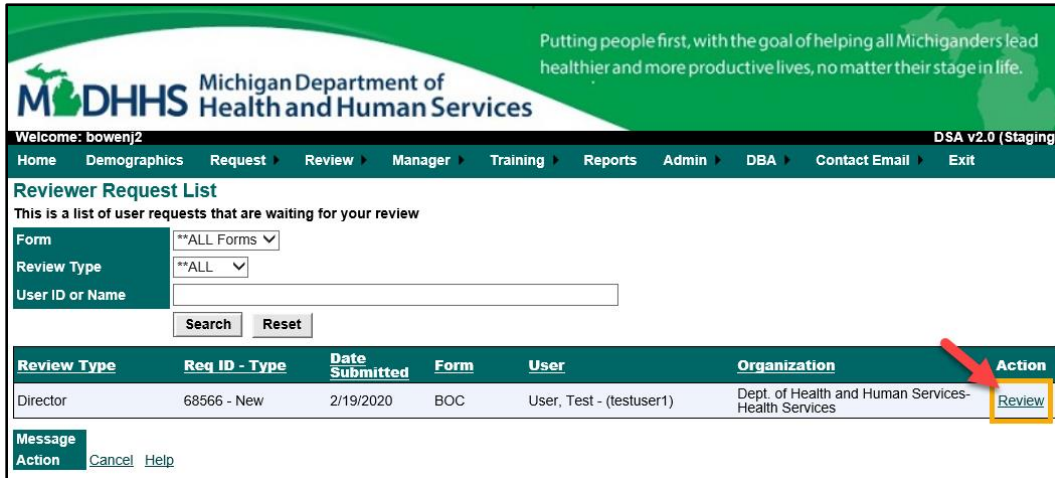
Figure 3.4.2: Reviewer Request List – Director

4. Verify the user information (*Figure 3.4.3*).
5. Click the arrow beside **User Details** to expand and review additional user demographics.
6. Verify the requested documents/profiles/programs/reports/roles/user groups, and confirm the **Request Reason** explains the need.

Figure 3.4.3: Director Review

7. Under **Completed Review(s)**, click the arrow beside **Immediate Manager Review** to expand and review the Immediate Manager's determination (*Figure 3.4.4*).

> *Note*: If there are any questions for the Immediate Manager, the name is a link. Click the link to email your questions.

8. Click the arrow beside **Sponsor Review**, if applicable, and beside **Program Manager Review** (**Report Manager Review** in *Figure 3.4.4* example) to expand and review the MDHHS Sponsor's and Program Manager's determinations.

Figure 3.4.4: Director Review

9. To return some or all of the access request to a Program Manager for reconsideration:

   a. Click <u>Return Some</u> at the bottom (*Figure 3.4.5*). The Return Some window displays.

Figure 3.4.5: Director Review

b. Select the **Send Back?/Update** check box(es) (*Figure 3.4.6*) beside the item(s) to be returned to the Program Manager(s).

c. Enter a **Director Comment** for each item to be returned, explaining why it is being returned. *Comments are required*.

d. Click <u>Save</u>. The Program Manager receives an email notification indicating the return.

Figure 3.4.6: Return Some

10. To approve the access request, select the **Approved** radio button (*Figure 3.4.7*).

11. To deny the access request, select the **Denied** radio button.

12. Enter **Reviewer Comments** as appropriate. *Comments are required when denying*.

13. Click <u>Save Goto Next</u> to save the final determination, advance to the next access request awaiting review.
   -or-
   Click <u>Save Goto List</u> to save the final determination and return to the list of requests awaiting review.

> *Note*: For applications containing PHI, **when approved** the request advances to the Training Manager step to confirm the user has completed required Privacy and Security training before any approved security role(s) can be granted. Upon receiving training confirmation, the Security Administrator receives email notification to finalize the access request.
>
> Otherwise, **when approved** the Security Administrator receives an email notification instructing them to grant the approved access and assign the user's security role within the source application.
>
> **When denied**, the review ends and the user is notified.

Figure 3.4.7: Director Review

4   Finalizing the Access Request: Security Admin

The Security Administrator performs the final step to complete the access request. The Security Administrator does not make any access decisions, but rather, grants the already-approved access in the source application. First, the Security Administrator assigns the user's approved security role(s) within the source application. Then, the Security Administrator returns to the DSA and marks the user's access request as 'Complete', at which point the user is notified that their access has been granted.

Perform the following steps to complete the access request as the Security Administrator:

1. Complete the steps in 1.4 Accessing the DSA.
2. Select **Review Requests** from the **Review** sub-menu (*Figure 4.1*).
   -or-
   Click Go To Review in the Requests Pending Review(s) dashboard.
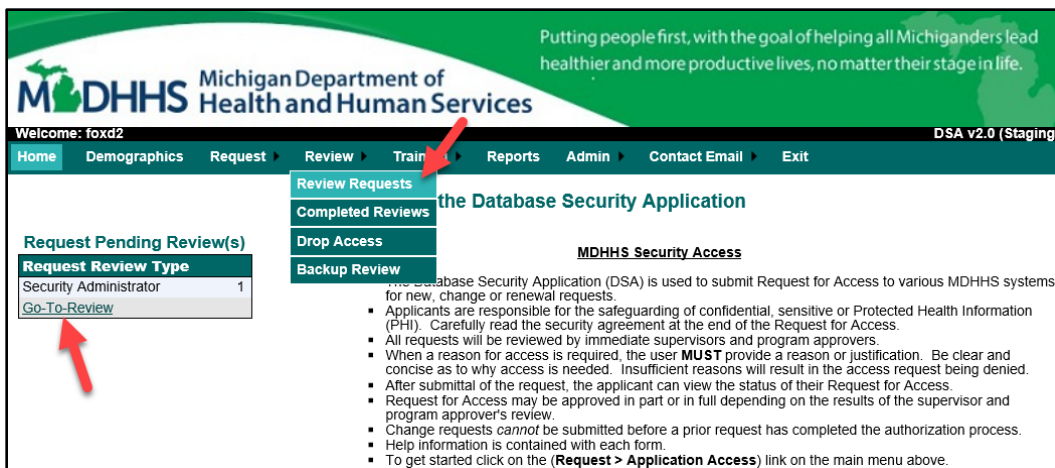
Figure 4.1: Home

3. Click Review beside the request to be reviewed (*Figure 4.2*). The Security Administrator page displays.
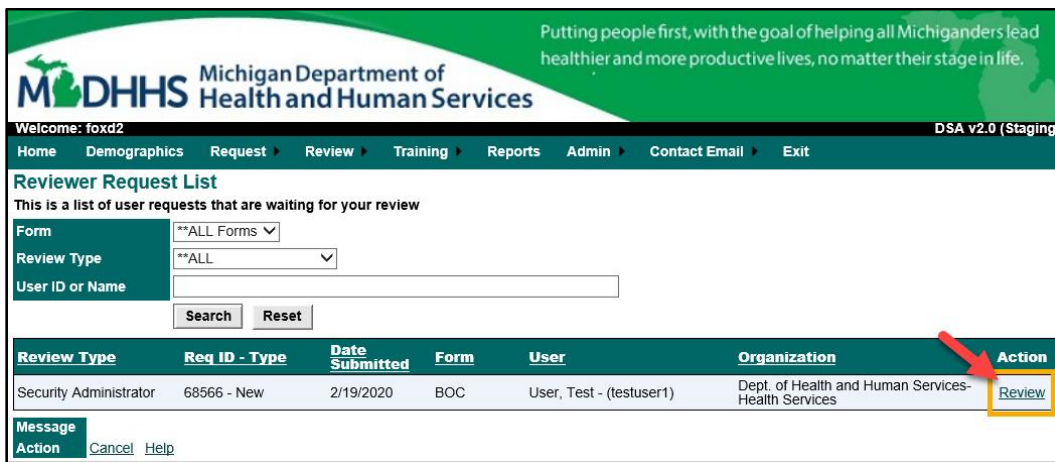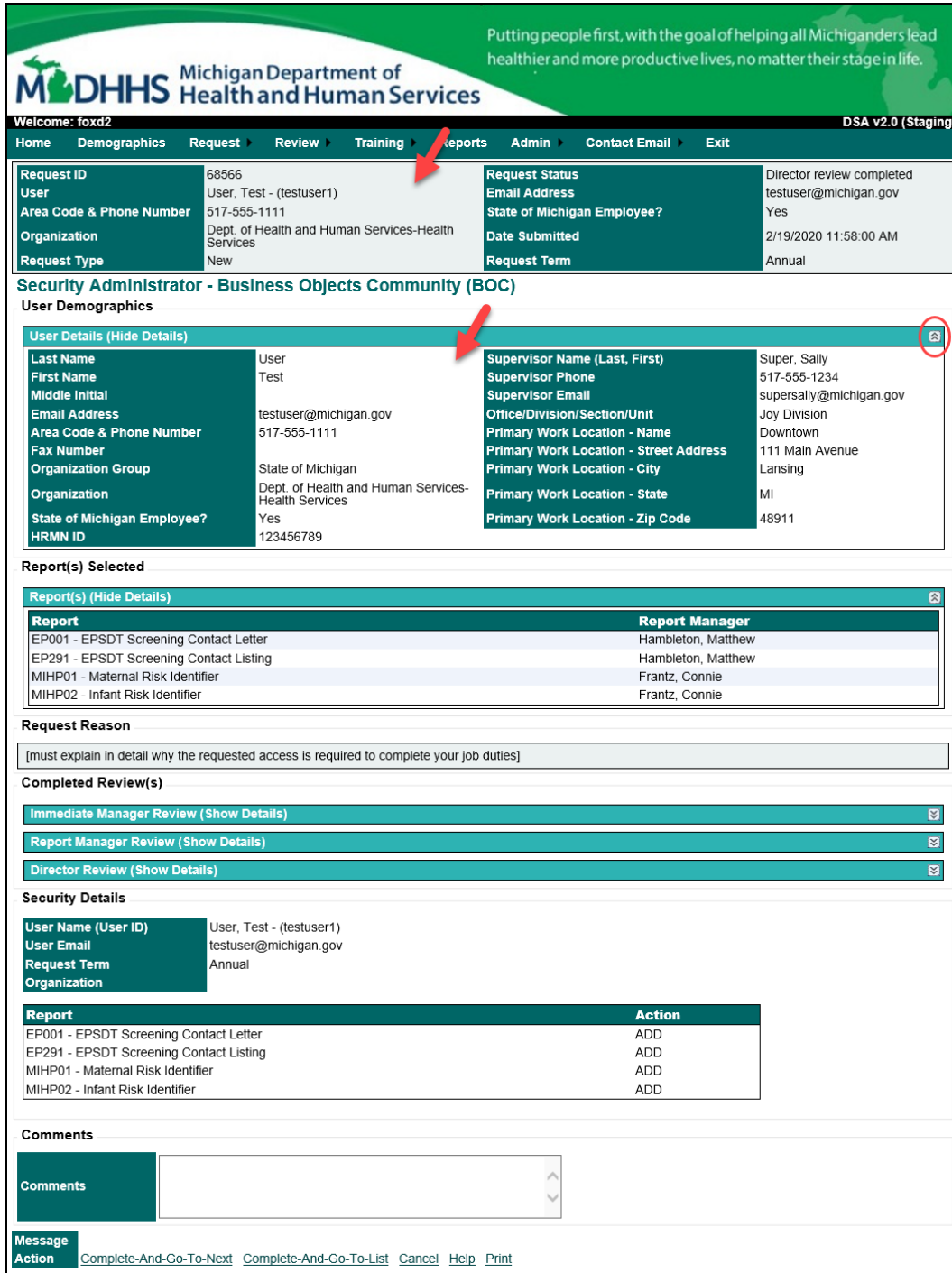

Figure 4.2: Reviewer Request List – Security Administrator

> *Note*: Use the search fields (*Figure 4.2, above*) to locate the request, if necessary.

4. Verify the user information (*Figure 4.3*).
5. Click the arrow beside **User Details** to expand and review additional user demographics.

Figure 4.3: Security Administrator

> **IMPORTANT**: The details crucial to finalizing the access request are located at the bottom in the **Security Details** section.

6. Under **Security Details** take note of the *User Name* and *User ID*, along with the security roles that were approved for the user (*seen as **Reports** in Figure 4.4 example*).

Figure 4.4: Security Administrator

7. Grant the approved access in the source application (e.g., CareConnect360, CHAMPS):

   a. Access the source application for which the security access was approved.

   b. Follow the source application's procedures for granting access and assigning approved security roles.

   c. When complete, return to the DSA.

8. Only after the access has been granted in the source application, enter detailed *Comments* (*Figure 4.5*) *about completing the access assignment in the source application*.

9. Click Complete And Go To Next to mark the access request complete, then advance to the next request awaiting finalization.
   -or-
   Click Complete And Go To List to mark the access request complete and return to the list of requests awaiting finalization.
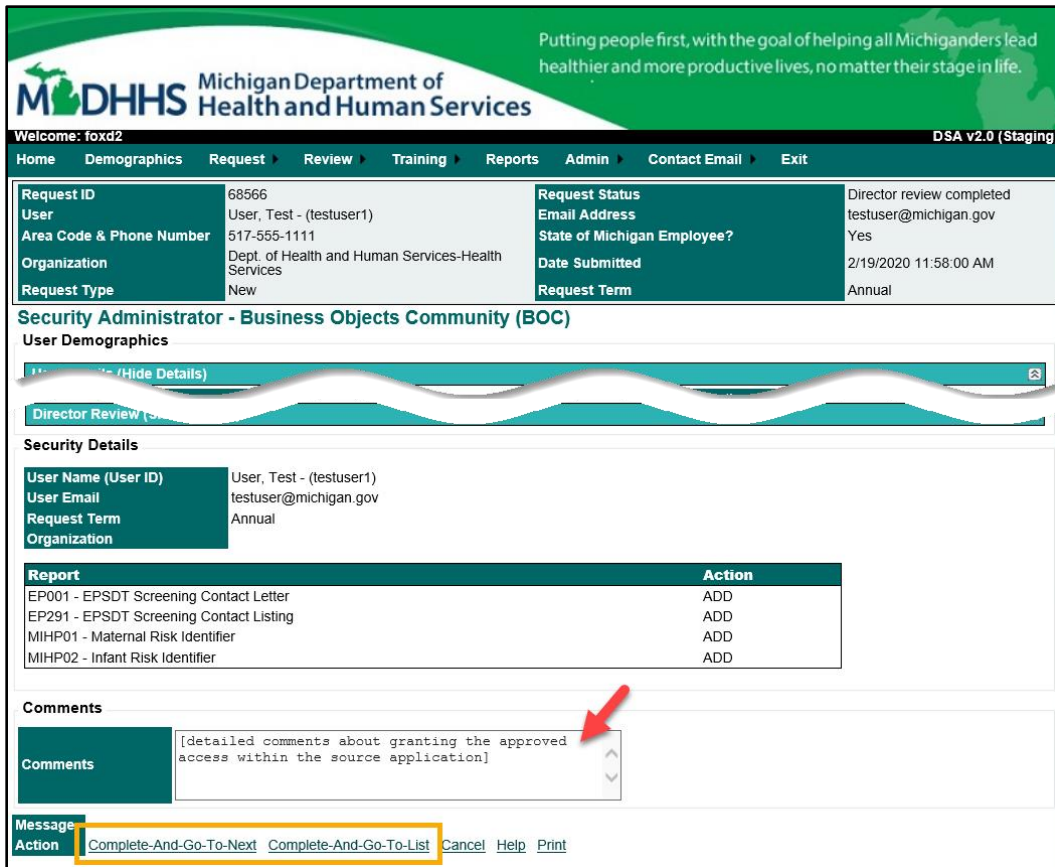

Figure 4.5: Security Administrator

Note: Upon completion, the user receives notification of their approved access being granted.

5 Periodically Reviewing Privileged Access

Some application access is considered Privileged Access and requires increased security protocol including periodic access reviews (PARs). Each application's access request Form Administrator determines which Privileged Access roles exist.

The Privileged Access roles are then communicated and coordinated between the Form Administrator and Optum, who perform the necessary actions to mark the role as 'privileged' within the Database Security Application (DSA). Please contact Optum for further coordination information. In limited instances, Privileged Access roles are identified by the Immediate Manager or Sponsor by selecting **Force PAR** during the review and approval cycle.

5.1 Periodic Access Reviews: Immediate Manager

Once marked, if a Privileged Access role requires a six-month (for example) periodic access review, the PAR is automatically created at the five-month mark and an email notification is sent to the Immediate Manager who approved the current privileged access.

The Immediate Manager is required to access the PAR request and re-approve the privileged access if still valid, or deny if the privileged access is no longer needed. If denied or not re-approved within an appropriate amount of time, a Drop Access request is automatically created to remove the privileged access.

> *Note*: Detailed instruction for completing a periodic access review as the Immediate Manager begins on the next page.

Perform the following steps to complete a Periodic Access Review (PAR) as the Immediate Manager:

1. Complete the steps in <u>1.4 Accessing the DSA</u>.
2. Select **Review Requests** from the **Review** sub-menu (*Figure 5.1.1*).
   -or-
   Click <u>Go To Review</u> in the Request Pending Review(s) dashboard.

   > *Note*: The Immediate Manager's Request Pending Review(s) dashboard also includes a 'PAR Immediate Manager' **Request Review Type** and displays the associated number of PAR reviews pending (*Figure 5.1.1*).
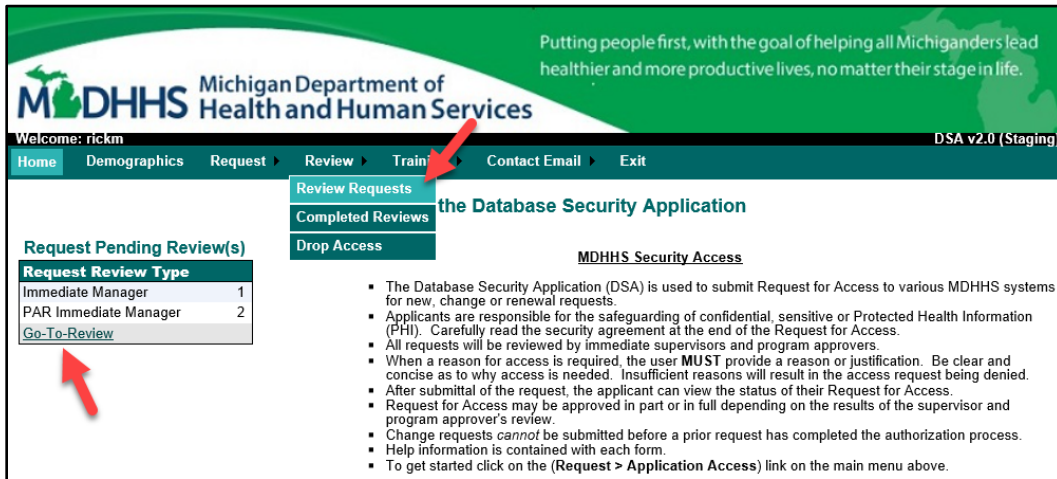
Figure 5.1.1: Home – Immediate Manager

3. Click <u>Review</u> beside the PAR request to be reviewed (*Figure 5.1.2*). The Immediate Manager Periodic Access Review page displays.
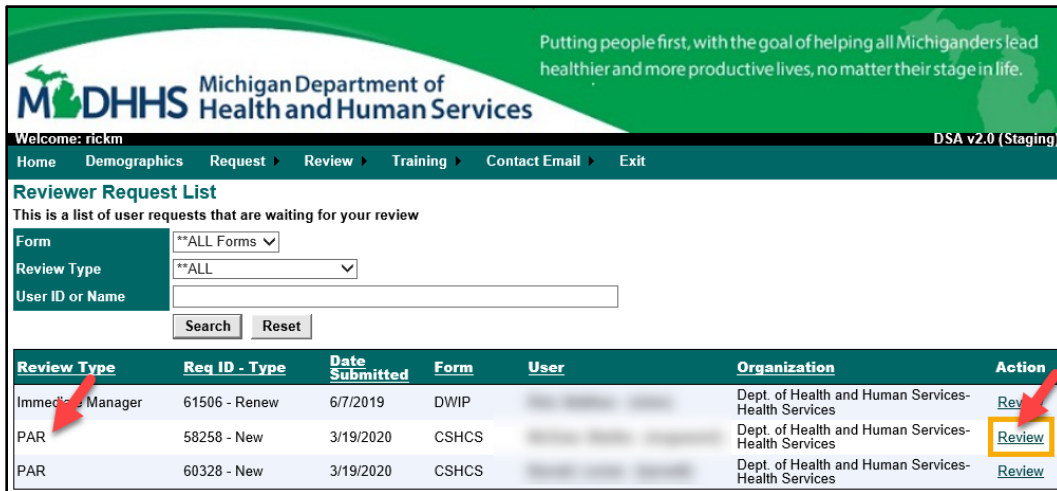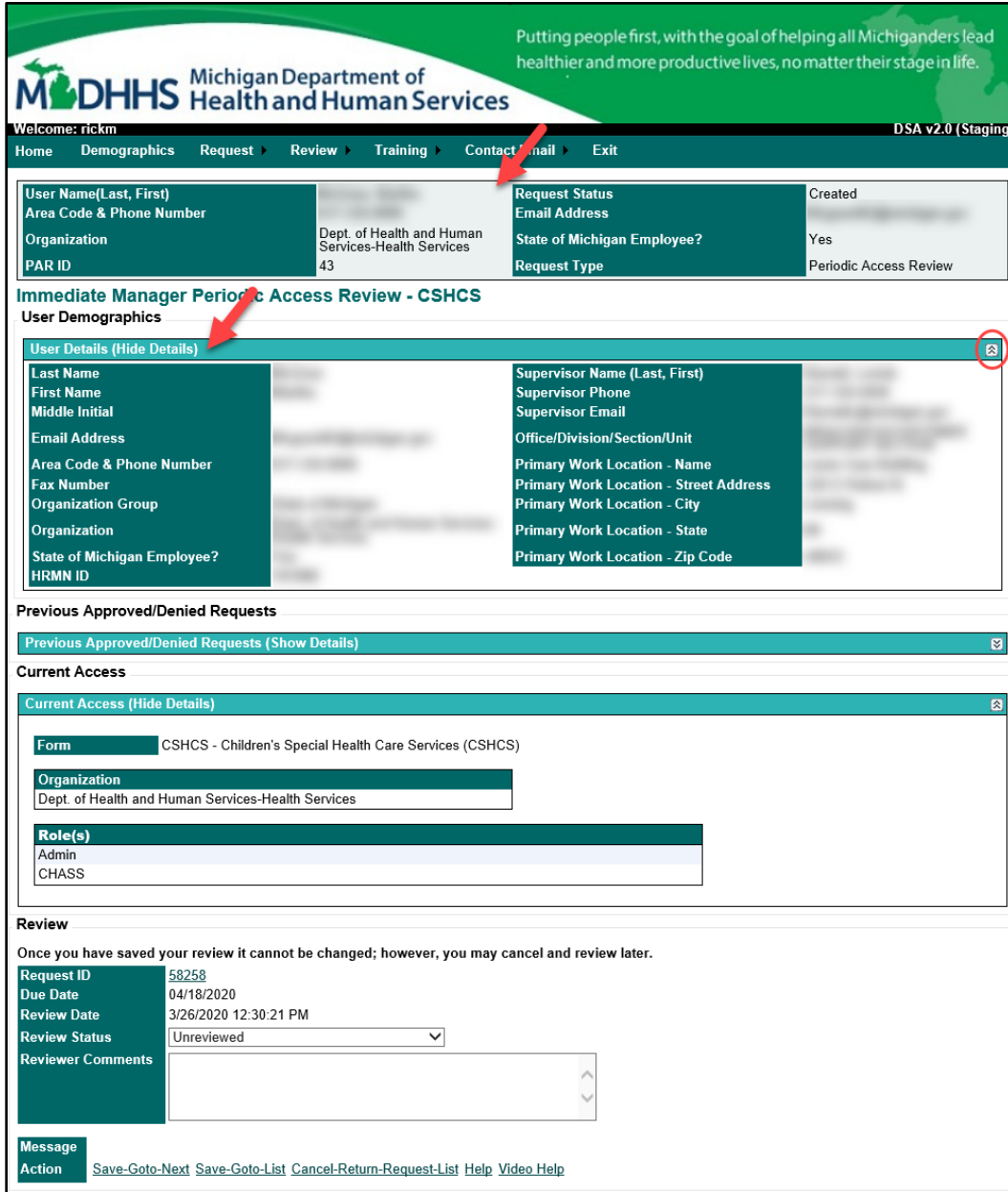

Figure 5.1.2: Reviewer Request List – Immediate Manager

4. Verify the user information (*Figure 5.1.3*).
5. Click the arrow beside **User Details** (*red circle*) to expand and review additional user demographics.

Figure 5.1.3: Immediate Manager Periodic Access Review

6. Under **Current Access** take note of the user's current approved Privileged Access details (*Figure 5.1.4*).

7. Under **Review** the *Request ID* is a link. Click the link to review the original request and review/approval cycle for the Privileged Access role (*see Figure 5.1.5, next page*).

Figure 5.1.4: Immediate Manager Periodic Access Review

8. In the original request (*Figure 5.1.5*), click the arrow beside each review level to expand the details and review the previous Privileged Access role approvals as needed.

9. When complete, click <u>Return To Previous Page</u> to return to the PAR request.

Figure 5.1.5: Original Privileged Access Role Request

10. To complete the PAR request, select the **Review Status** (*Figure 5.1.6*). Please see Table 5.1.1 for the resulting actions. Review statuses include:

- Access is appropriate
- Access needs have changed
- Remove access – Retired

- Remove access – No longer my employee

- Remove access – Job duties changed

- Reassign – Transfer

- Reassign – Transfer Not Found

11. Enter detailed **Reviewer Comments** about the status selected.

Figure 5.1.6: Immediate Manager Periodic Access Review

12. Click <u>Save Goto Next</u> to save the PAR, advance to the next request awaiting review.
    -or-
    Click <u>Save Goto List</u> to save the PAR and return to the list of requests awaiting review.

PAR Review Status Selected	Resulting Action
Access is appropriate	No change to the user's current Privileged Access role, the privileged access continues
Access needs have changed	Automatically generates a Change request which the user must complete according to their new access needs
Remove access – Retired	Automatically generates a Drop Access request informing the Security Administrator to terminate the Privileged Access in the source system
Remove access – No longer my employee	Automatically generates a Drop Access request informing the Security Administrator to terminate the Privileged Access in the source system
Remove access – Job duties changed	Automatically generates a Drop Access request informing the Security Administrator to terminate the Privileged Access in the source system
Reassign – Transfer	Allows selection of the new **Immediate Manager**, then transfers the PAR and sends email notification to the new Immediate Manager
Reassign – Transfer Not Found	When the new Immediate Manager cannot be found allows selection of the **Form Administrator**, then transfers the PAR and sends email notification to the Form Administrator for PAR resolution

Table 5.1.1: PAR Review Statuses

5.2 Periodic Access Reviews: Form Administrator

Form Administrators can manage their application's PARs using the Request Maintenance page. In addition to the statuses available to the Immediate Manager, the Form Administrator can select to close a PAR or extend the due date for a PAR.

Complete the following steps to manage Periodic Access Requests (PARs) as the Form Administrator:
1. Complete the steps in 1.4 Accessing the DSA.
2. Select **Request Maintenance** from the **Admin** sub-menu (*Figure 5.2.1*).
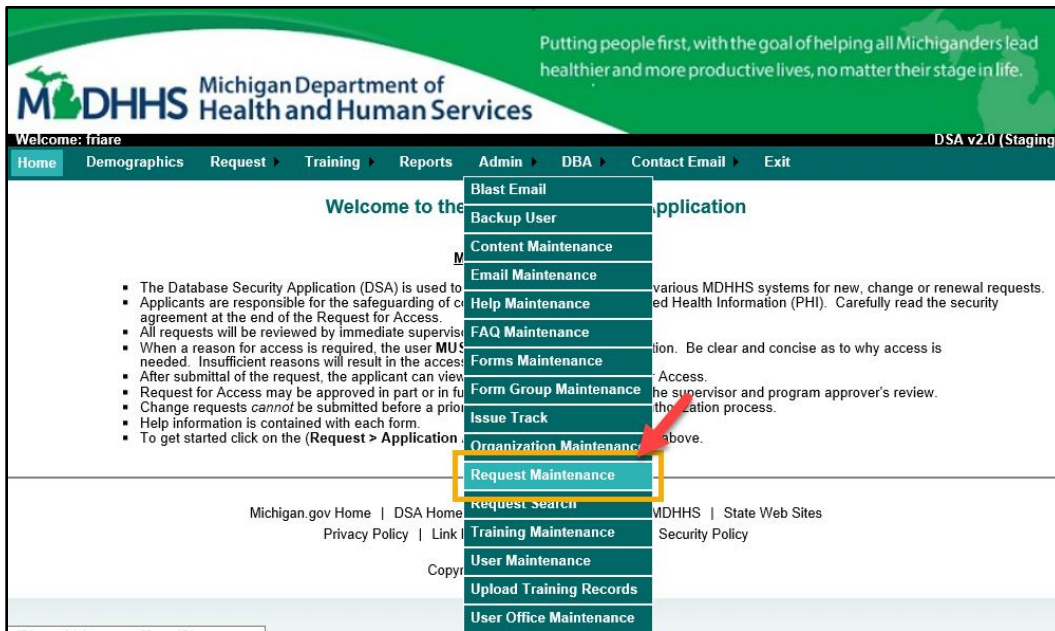
Figure 5.2.1: Admin – Request Maintenance

3. Click the **Periodic Access Reviews** tab (*Figure 5.2.2*).

4. Click <u>View</u> beside the PAR request to be reviewed. The Periodic Access Review page displays.
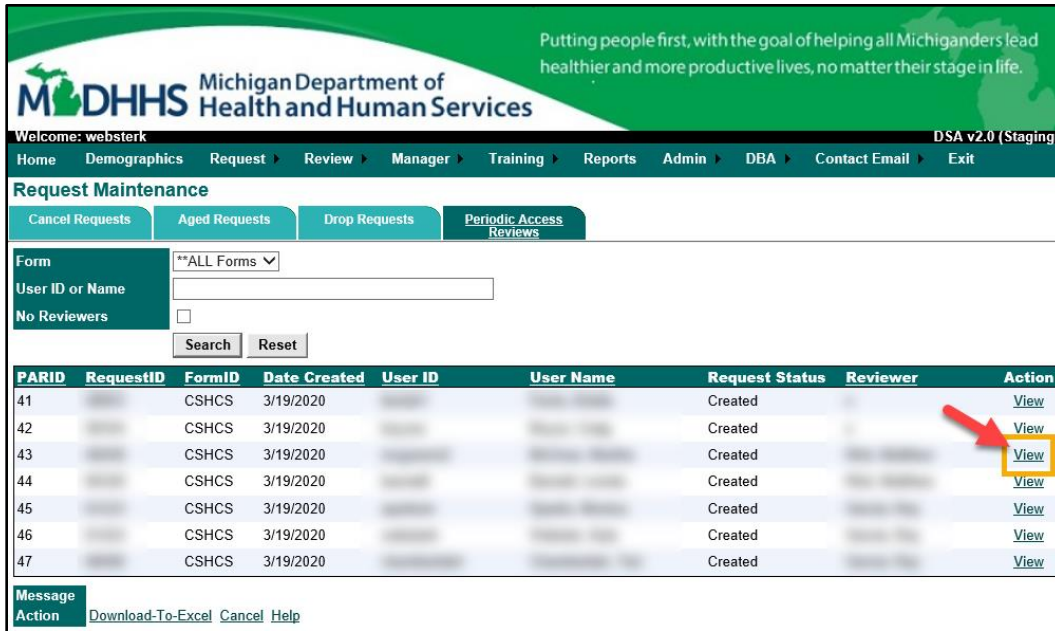
Figure 5.2.2: Request Maintenance – Periodic Access Reviews

5. Verify the user information (*Figure 5.2.3*).

6. Click the arrow beside **User Details** (*red circle*) to expand and review additional user demographics.
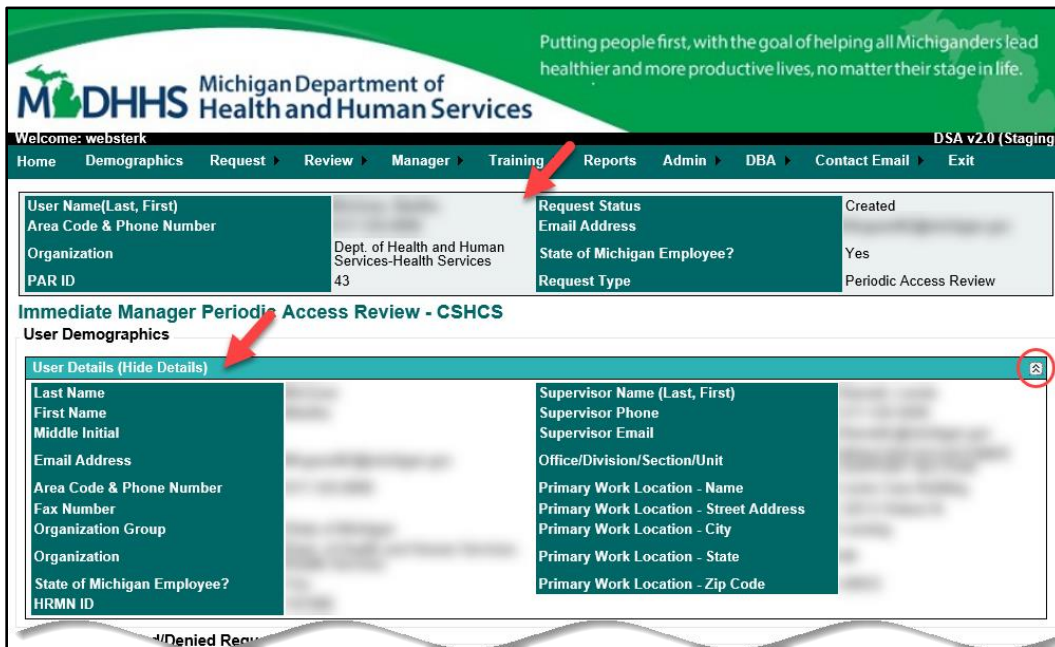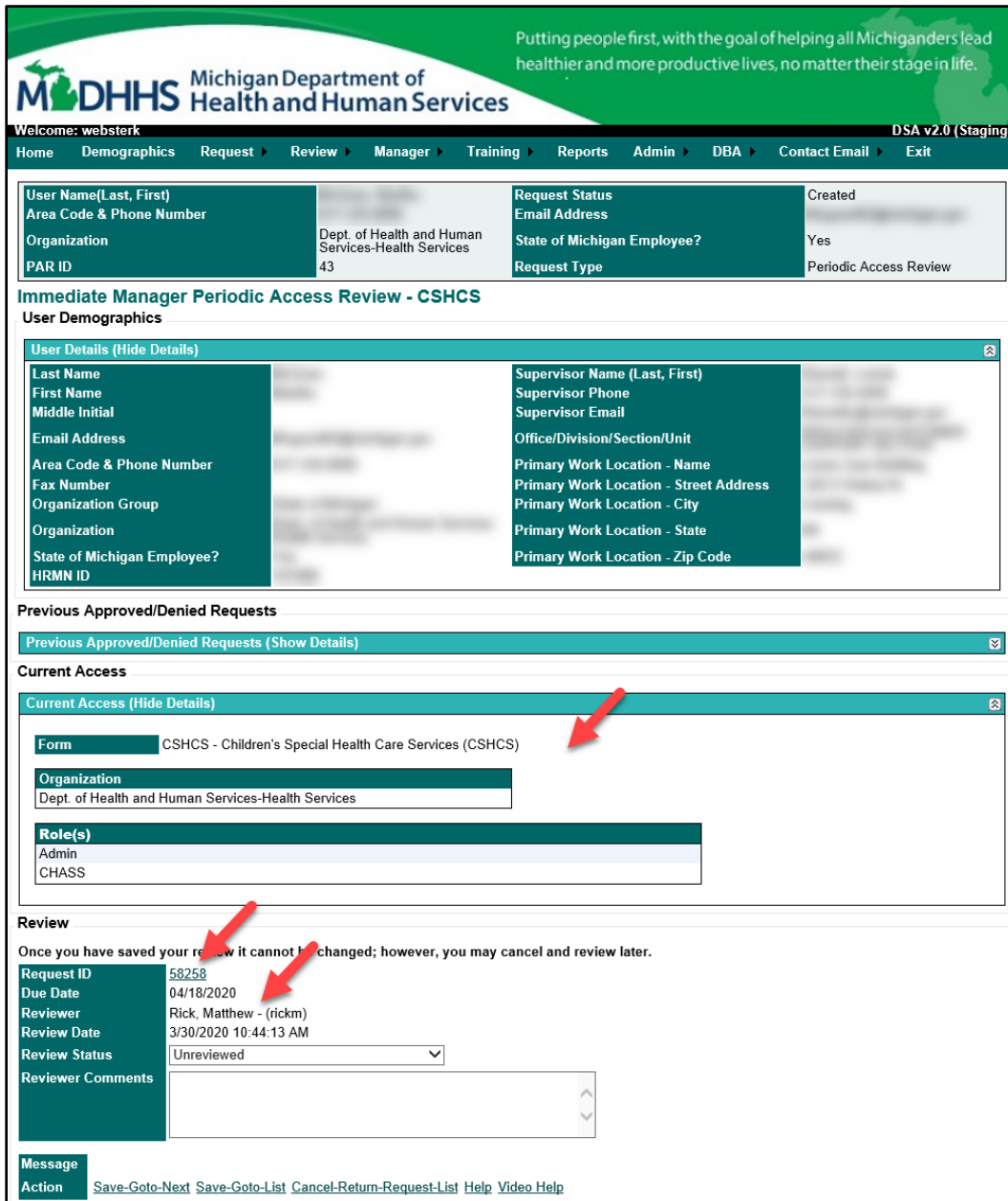
Figure 5.2.3: Periodic Access Review – Form Administration

7. Under **Current Access** take note of the user's current approved Privileged Access details (*Figure 5.2.4*).

8. Under **Review** the *Request ID* is a link. If necessary, click the link to review the original Privileged Access role request and review/approval cycle.

9. Note the PAR's *Due Date* and *Reviewer*. The Reviewer is the Immediate Manager who originally approved the privileged access.

Figure 5.2.4: Periodic Access Review – Form Administrator

10. To complete the PAR request or extend the PAR's due date, select the appropriate ***Review Status*** (*Figure 5.2.5*). Please see Table 5.2.1 for the resulting actions. Statuses include:

- Access is appropriate
- Access needs have changed
- Remove access – Retired
- Remove access – No longer my employee
- Remove access – Job duties changed
- Reassign – Transfer
- Reassign – Transfer Not Found
- Close PAR
- Extend Due Date for PAR

11. If selecting the ***Review Status***:

a. 'Reassign – Transfer' select the new ***Immediate Manager*** to which the PAR is to be transferred.

b. 'Reassign – Transfer Not Found' select the ***Form Administrator*** to perform the PAR resolution.

c. 'Extend Due Date for PAR' ***Select*** *(the new)* ***Due Date*** for the PAR.

12. Enter detailed ***Reviewer Comments*** about the status selected.

Figure 5.2.5: Periodic Access Review – Form Administration

13. Click <u>Save Goto Next</u> to save the PAR, advance to the next request awaiting review.
    -or-
    Click <u>Save Goto List</u> to save the PAR and return to the list of requests awaiting review.

PAR Review Status Selected	Resulting Action
Access is appropriate	No change to the user's current Privileged Access role, the privileged access continues
Access needs have changed	Automatically generates a Change request which the user must complete according to their new access needs
Remove access – Retired	Automatically generates a Drop Access request informing the Security Administrator to terminate the Privileged Access in the source system
Remove access – No longer my employee	Automatically generates a Drop Access request informing the Security Administrator to terminate the Privileged Access in the source system
Remove access – Job duties changed	Automatically generates a Drop Access request informing the Security Administrator to terminate the Privileged Access in the source system
Reassign – Transfer	Allows selection of the new *Immediate Manager*, then transfers the PAR and sends email notification to the new Immediate Manager
Reassign – Transfer Not Found	When the new Immediate Manager cannot be found allows selection of the *Form Administrator*, then transfers the PAR and sends email notification to the Form Administrator for PAR resolution
Close PAR	No change to the user's current Privileged Access role, the privileged access continues
Extend Due Date for PAR	Allows the Form Administrator to *Select (a) Due Date* to extend a PAR that cannot be completed by the initially-assigned due date

Table 5.2.1: PAR Review Statuses

6   Dropping Users: Access Termination

When a user's need for access to an application ceases the Immediate Manager, the Organization Manager, and the application's access request Form Administrator have the ability to generate a drop access request within the DSA. This action notifies the application's Security Administrator to review the drop access request and terminate the user's access in the source application (e.g., CareConnect360, CHAMPS, MiSACWIS).

At times it may be necessary to generate drop access requests for multiple users at once. The application's Form Administrator has the added ability to upload a Microsoft Excel © spreadsheet containing multiple users that need their access terminated. Uploading the file generates drop access requests for each user on the spreadsheet.

6.1 Generate a Drop Access Request

Complete the following steps to generate a drop access request:
1. Complete the steps in 1.4 Accessing the DSA.
2. Select **Drop Access** from the **Review** sub-menu (*Figure 6.1.1*). The Drop User Access page displays.
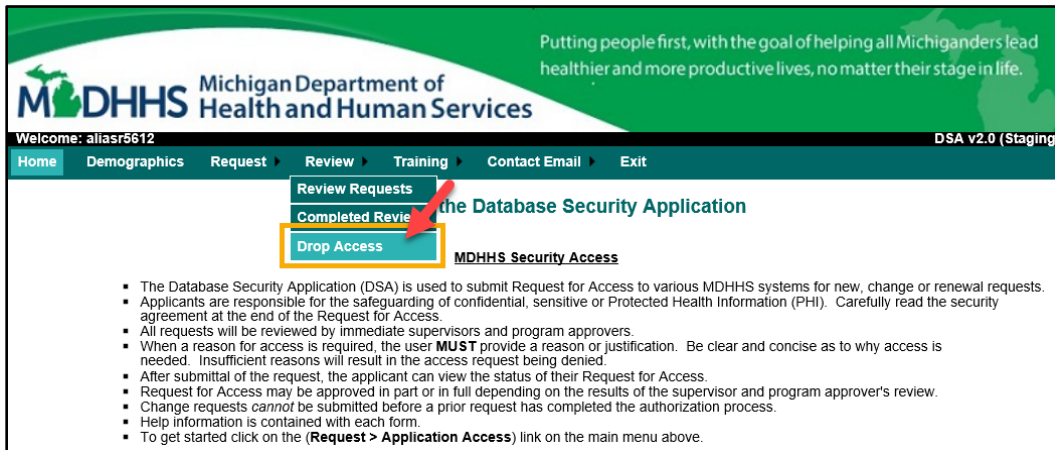
Figure 6.1.1: Home

3. Click Generate Drop Access Request (*Figure 6.1.2*). The Drop Access Confirmation window displays.
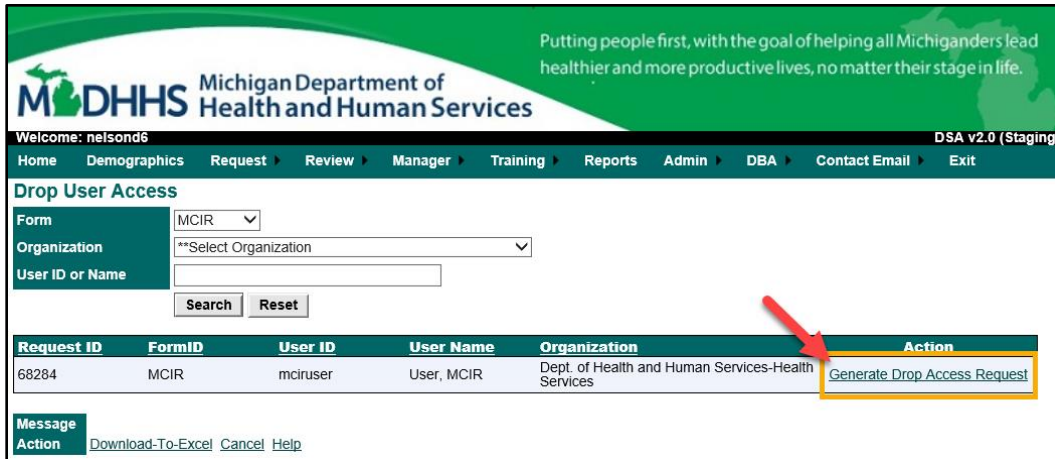
Figure 6.1.2: Drop User Access

4. Enter a detailed ***Reason*** for terminating/dropping the user's access (*Figure 6.1.3*).

5. Click Confirm. The application's Security Administrator is notified by email to review the drop access request and terminate the user's access in the source application.
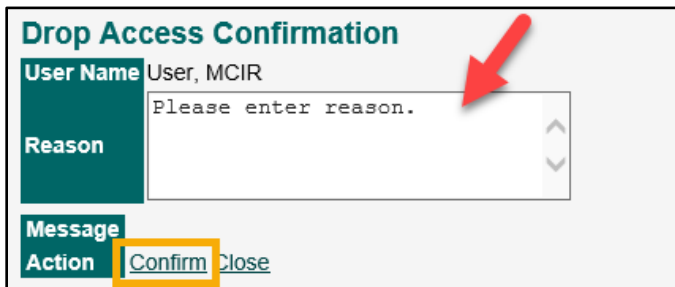
Figure 6.1.3: Drop Access Confirmation

6.2 Complete a Drop Access Request

When an Immediate Manager, Organization Manager, or the application's access request Form Administrator generates a drop access request within the DSA, the application's Security Administrator receives email notification with the subject line: **Drop Access - <application name> Request to Review as Security Administrator**. This email instructs them to review the drop access request, and terminate the user's access as appropriate.

To carry out the request, the Security Administrator first terminates the user's access in the source application (e.g., CareConnect360, CHAMPS, MiSACWIS). *After completing the termination in the source application, the Security Administrator returns to the DSA to document the termination* thus completing the drop access process.

Complete the following steps to drop a user's access as the Security Administrator:

1. Complete the steps in <u>1.4 Accessing the DSA</u>.
2. Select *Review Requests* from the *Review* sub-menu (*Figure 6.2.1*).
   **-or-**
   Click <u>Go To Review</u> in the Request Pending Review(s) dashboard.
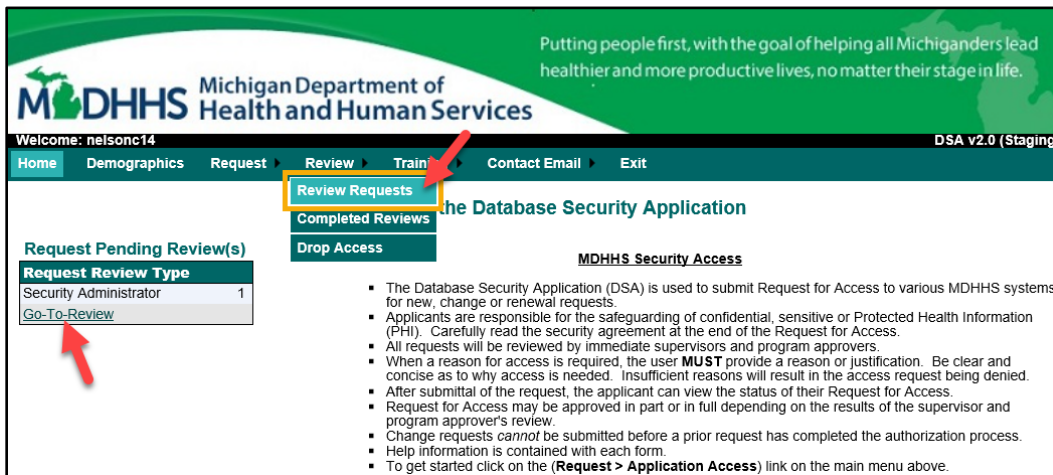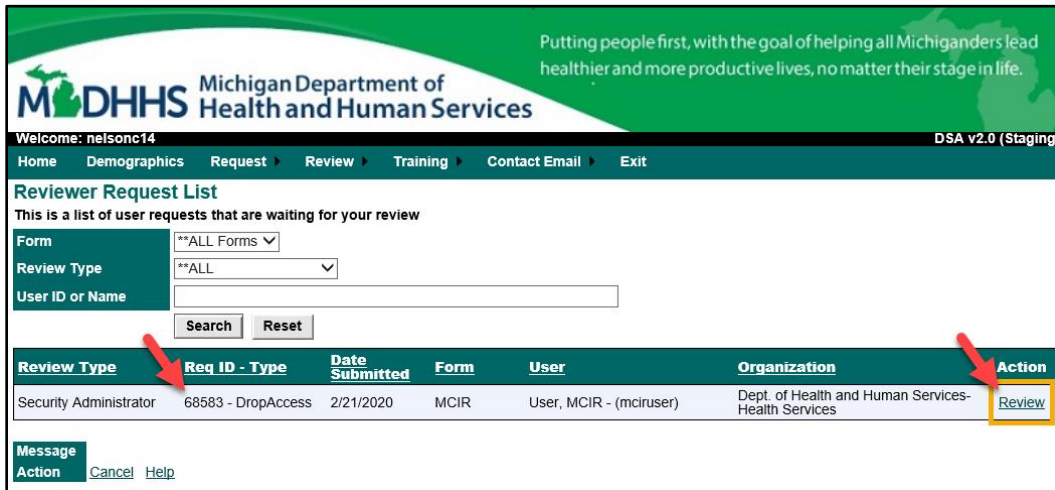

Figure 6.2.1: Home – Review – Review Requests

3. Click <u>Review</u> beside the 'DropAccess' request to be reviewed (*Figure 6.2.2*). The Security Administrator page displays.

Figure 6.2.2: Reviewer Request List – Security Administrator

4. Verify the user information (*Figure 6.2.3*). Click the arrow beside **User Details** to expand.

Figure 6.2.3: Security Administrator

> *IMPORTANT*: The details crucial to completing the drop access request are located at the bottom in the **Security Details** section.

5. Review the ***Request Reason*** (*Figure 6.2.4*) to confirm the termination is appropriate.

6. Under **Security Details** take note of the ***User Name*** and ***User ID***, along with the drop access instructions (i.e., "Please drop the user's access from this application").
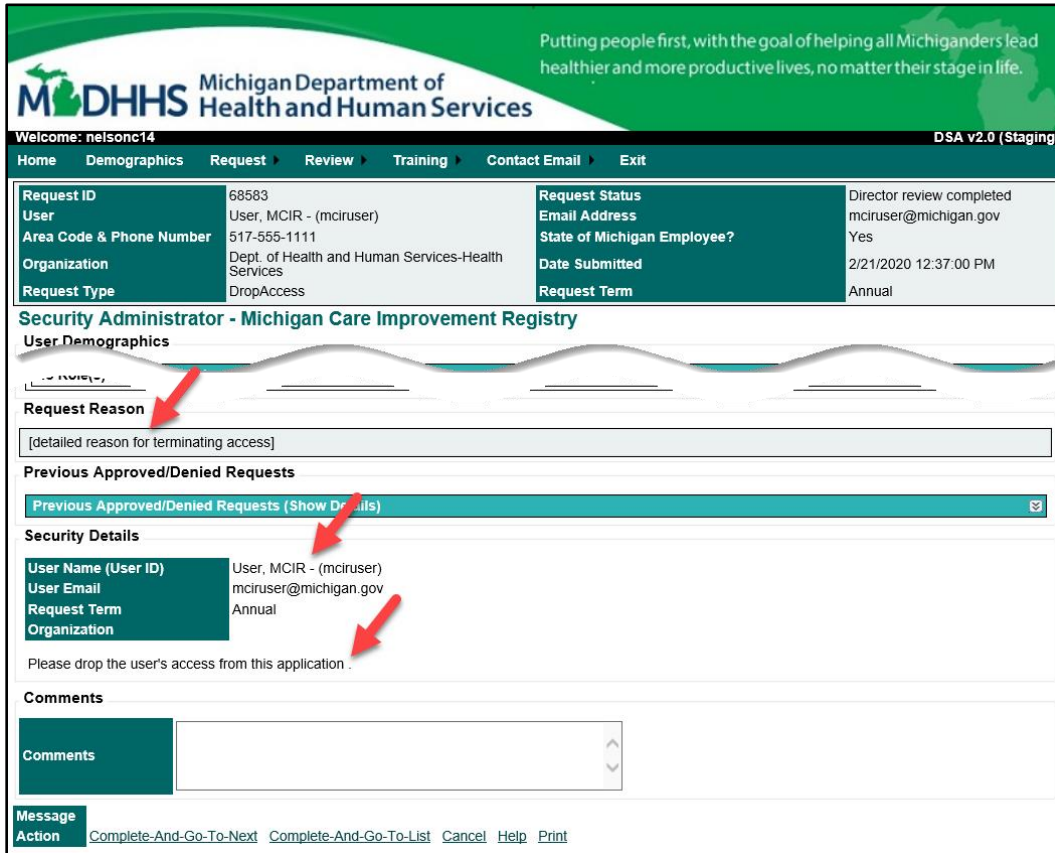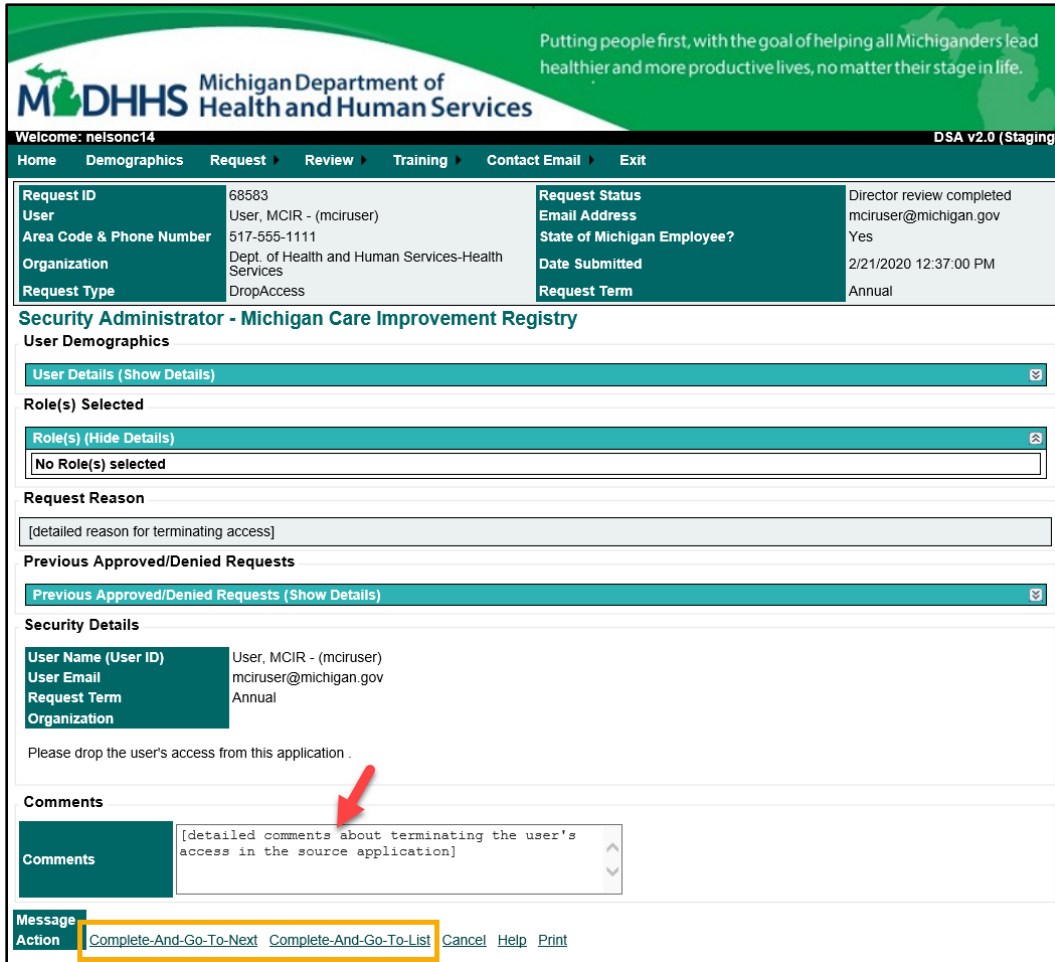
Figure 6.2.4: Security Administrator

7. Terminate the user's access in the source application:

   a. Access the source application for which the access termination is requested (e.g., CareConnect360, CHAMPS, MiSACWIS).

   b. Follow the source application's procedures for terminating the user's access.

   c. When complete, return to the DSA.

8. Only after the access has been terminated in the source application (e.g., CareConnect360, CHAMPS, MiSACWIS), enter detailed *Comments* (*Figure 6.2.5*) *about completing the access termination in the source application*.

9. Click Complete And Go To Next to mark the drop access request complete, then advance to the next request on the list.
   -or-
   Click Complete And Go To List to mark the drop access request complete and return to the list of requests awaiting review.

Figure 6.2.5: Security Administrator

8. Only after the access has been terminated in the source application (e.g., CareConnect360, CHAMPS, MiSACWIS), enter detailed *Comments* (*Figure 6.2.5*) *about completing the access termination in the source application*.

9. Click Complete And Go To Next to mark the drop access request complete, then advance to the next request on the list.
   -or-
   Click Complete And Go To List to mark the drop access request complete and return to the list of requests awaiting review.

Figure 6.2.5: Security Administrator

Page | 52

6.3 Bulk Generate Drop Access Requests

Note: Only the Form Administrator has the added ability to bulk generate drop access requests.

Complete the following steps to generate multiple drop access requests by spreadsheet upload:

1. Complete the steps in 1.4 Accessing the DSA.
2. Select *Request Maintenance* from the *Admin* sub-menu (*Figure 6.3.1*). The Request Maintenance page displays.
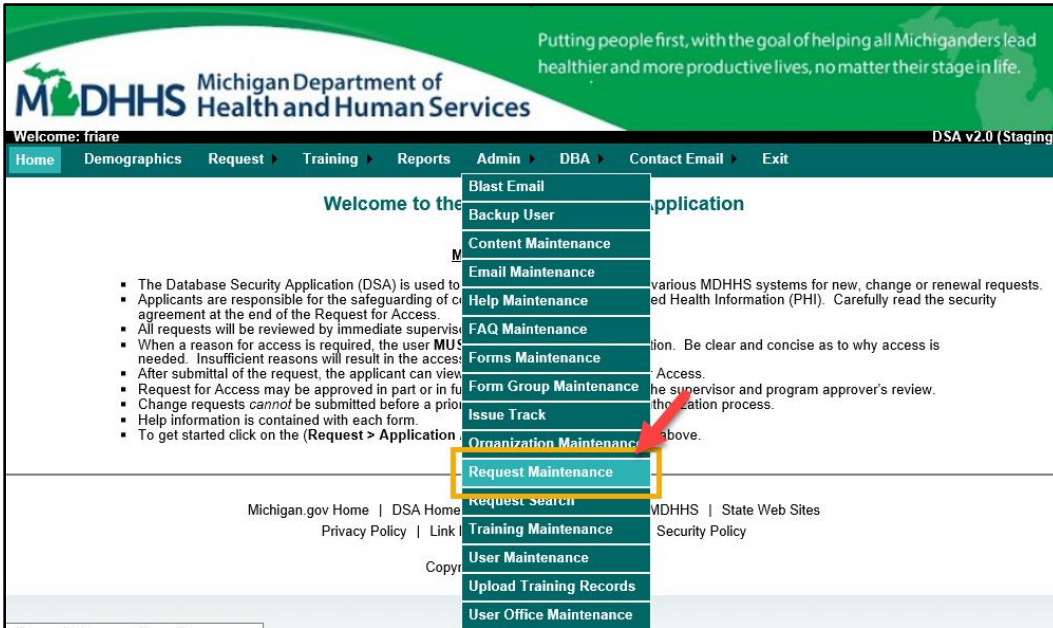
Figure 6.3.1: Admin – Request Maintenance

3. Click the **Drop Requests** tab (*Figure 6.3.2*).
4. Click **Upload From Excel**.
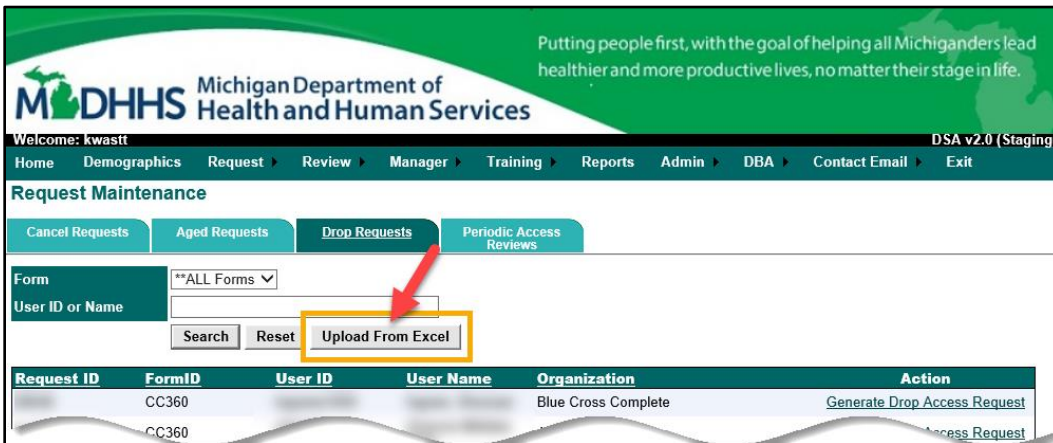
Figure 6.3.2: Request Maintenance – Drop Requests

5. To ensure proper file formatting, click <u>Sample File</u> (*Figure 6.3.3*) to access a sample Excel file to use as your template.

Figure 6.3.3: Request Maintenance – Drop Requests

6. Save the sample Excel file (*Figure 6.3.4*). This is a .csv (comma delimited) file and needs to be saved as a .csv file

> *IMPORTANT*: Do not add, delete, or rename the columns. The Excel spreadsheet must contain exactly three (3) columns titled 'UserID', 'OrganizationName', and 'Reason'. **All three values are required in each row**.
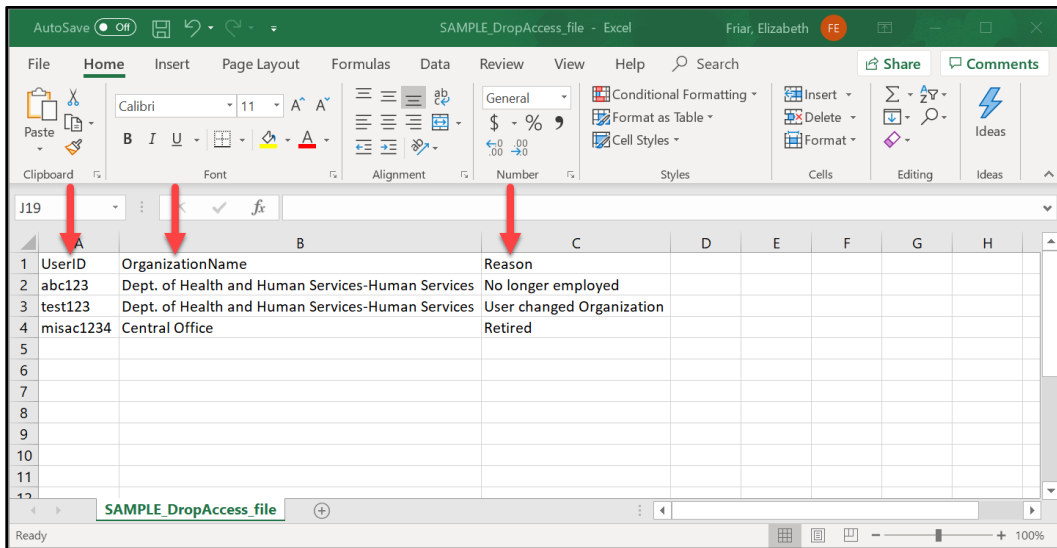
Figure 6.3.4: Sample Excel .csv File

7. To prepare the sample Excel file for upload, complete the following and save:

   a. Begin with row number 2. Do not alter or delete the column titles in row number 1.

   b. Replace the values in the sample file's **UserID** column (e.g., abc123, test123) with each MILogin user ID for whom access needs to be terminated. The maximum number of rows/user IDs allowed is 100.

c. Replace the values in the sample file's **OrganizationName** column (e.g., Dept of Health and Human Services-Human Services, Central Office) with each user's organization. Please see the *IMPORTANT* note below.

d. Replace the values in the sample file's **Reason** column (e.g., No longer employed, Retired) with the reason for each user's termination. Note, the reason entered will display in the generated drop access request's *Reason* field.

> *IMPORTANT*: The organization name must exactly match the organization name as it exists within the DSA. Form Administrators can access the organization name by selecting *Request Search* from the *Admin* sub-menu and clicking View beside the user's current/to-be-terminated access request. The *Organization* name is located at the top (*Figure 6.3.5*).
>
>
>
> **Figure 6.3.5: Request Search – Request Details – Get Organization Name**

8. Once the spreadsheet is saved and ready for upload, select the application name in the *Form* list (*Figure 6.3.6*) for which the drop access requests are being made (e.g., CC360, CHAMPS, MiSACWIS).

Figure 6.3.6: Request Maintenance – Drop Requests

OPTUM™

9. Click **Browse…** to select the Excel file to be uploaded (*Figure 6.3.7*). Once selected, the file name displays in the ***File to upload*** field.

10. Click Upload to submit the Excel file. The 'upload successful' and 'rows inserted: <#>' messages display.
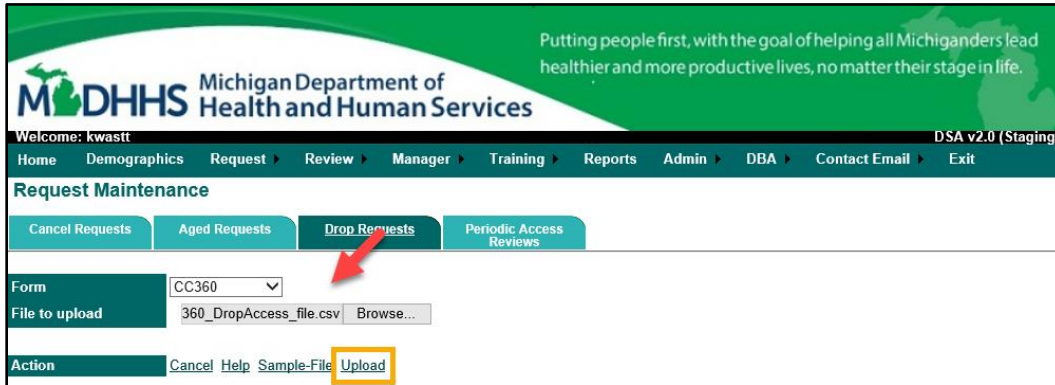
Figure 6.3.7: Request Maintenance – Drop Requests

11. Click Create Drop Requests (*Figure 6.3.8*) to complete the process. The application's Security Administrator is notified by email to review the drop access request and terminate the user's access in the source application. Please reference 6.2 Complete a Drop Access Request for additional information.

    -or-

    Click Create Drop Requests And Complete to create the drop requests *and* mark the requests as complete within the DSA. This option is beneficial when reconciling the DSA with users already terminated in the source application due to reasons such as 60-day inactivity termination.
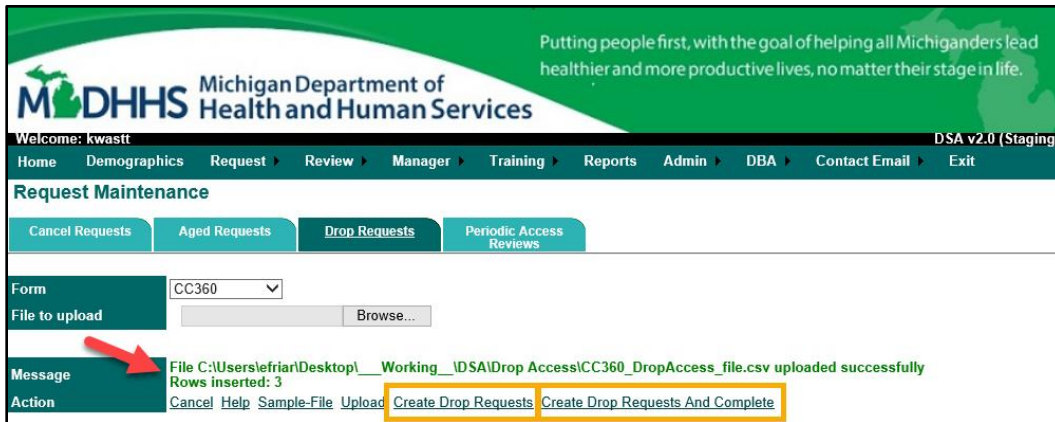
Figure 6.3.8: Request Maintenance – Drop Requests

12. When successful, the request ID numbers display for the drop access requests generated (*Figure 6.3.9*).
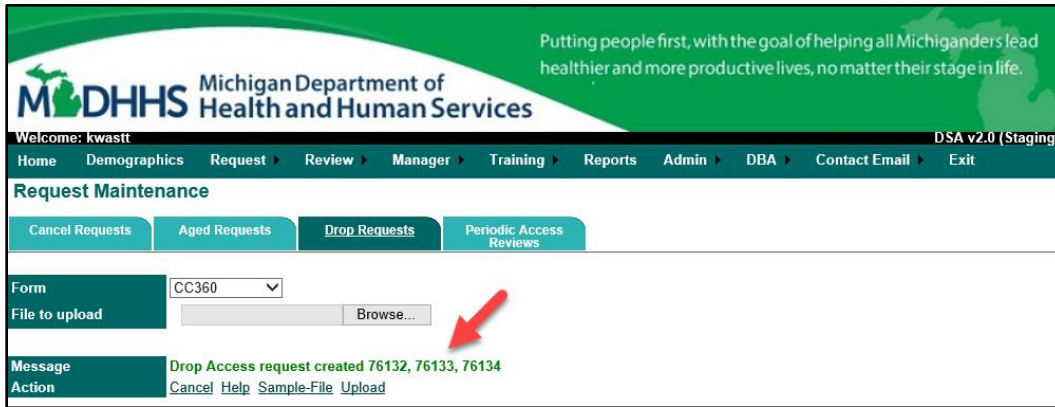
Figure 6.3.9: Request Maintenance – Drop Requests

Note: If a User ID/Organization Name combination does not have a current access request matching the access termination need -or- a drop access request is already in process, the message "**Excel file not processed due to error(s) below. Please address the errors and resubmit.**" displays and specific details are listed (*Figure 6.3.10*). Correct the errors, then repeat steps 8-12 to resubmit the Excel file.

Figure 6.3.10: Request Maintenance – Drop Requests

13. To confirm the creation of your bulk-generated drop access requests, select **Request Search** from the **Admin** sub-menu (*Figure 6.3.11*). The Request Search page displays.

Figure 6.3.11: Admin – Request Search

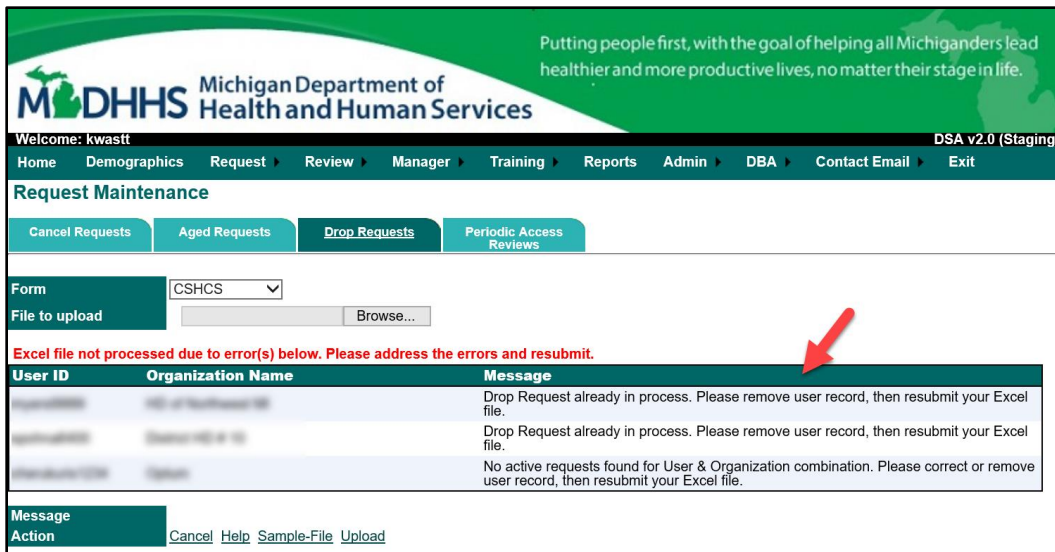14. Use the search fields to narrow the results (*Figure 6.3.12*). For example, select the 'DropAccess' **Request Type** and the application name in the **Form** field, then click **Search**.

15. Note the request IDs corresponding to your bulk upload listed in the results grid.

16. Click <u>View</u> to view the drop access request details.

17. Click <u>Print</u> to print the drop access request details.
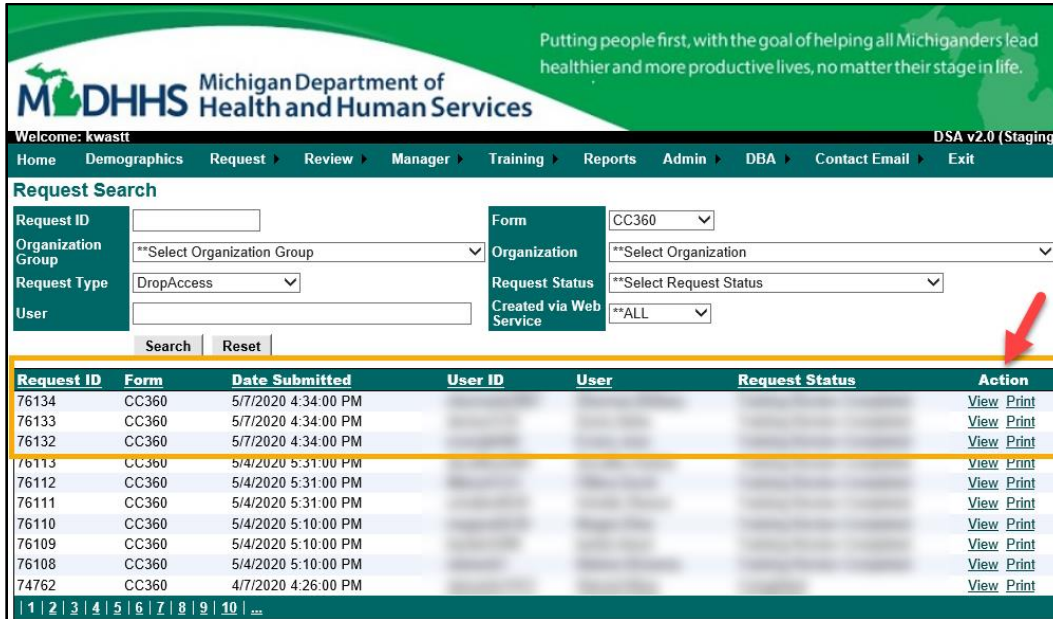

Figure 6.3.12: Request Search

7 Maintaining Approvers: Management

Users who review and approve MDHHS application access requests are called approvers in the DSA. The Immediate Manager and the Organization Manager are DSA approver/management roles available for request within the DSA. These access request management roles must be approved.

In addition, all approvers should have at least one backup approver assigned for each approval level for which they are responsible (e.g., Immediate Manager, Program Manager, Director). Backup approvers are designated for a defined timeframe, and they must also be approved.

7.1 Review Immediate Manager DSA Role Request

A user selects their Immediate Manager while filling out an application access request form. The Immediate Manager works closely with the user, and therefore understands the user's business needs as they relate to application access needs.

Each organization must have at least one individual set up with the Immediate Manager role within the DSA. The Immediate Manager completes the first step in the review and approval process by affirming that the user requires access to the requested application to complete their job duties.
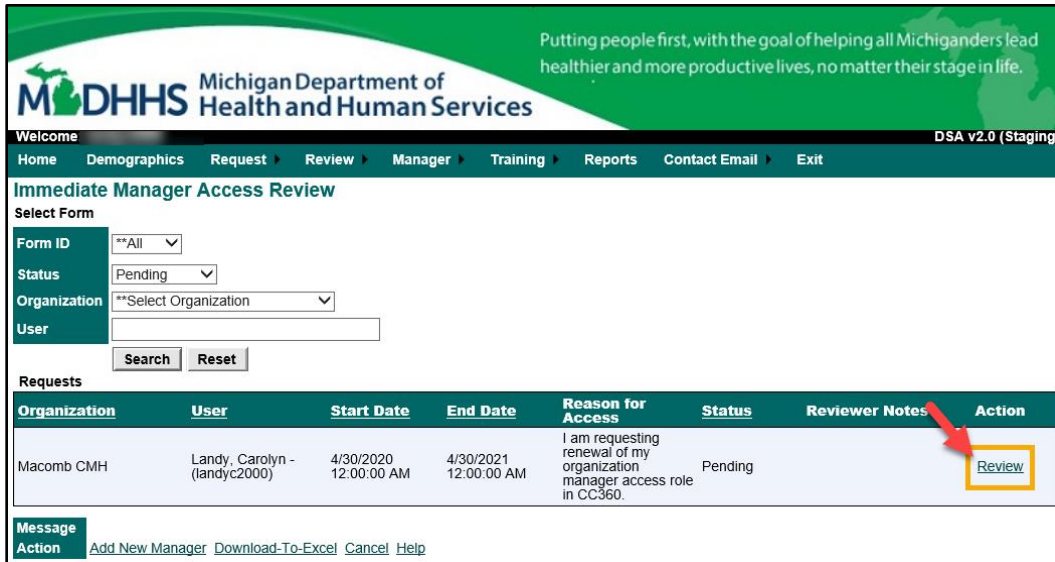
Complete the following steps to review an Immediate Manager DSA role request:

1. Complete the steps in 1.4 Accessing the DSA.
2. Select **Immediate Manager Access** from the **Manager** sub-menu (*Figure 7.1.1*). The Immediate Manager Access Review page displays.

Figure 7.1.1: Home

3. Click Review beside the request to be reviewed (*Figure 7.1.2*). The Review Immediate Manager Access Request window displays.
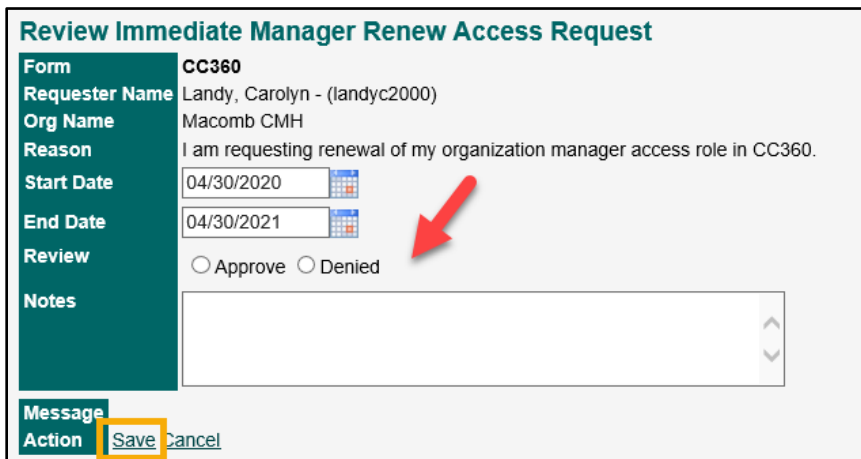
Figure 7.1.2: Immediate Manager Access Review

> *Note*: The Immediate Manager role automatically defaults to a one-year timeframe. Update the *Start Date* and/or *End Date* if appropriate.

4. To approve the Immediate Manager role assignment, select the *Approve* radio button (*Figure 7.1.3*).

5. To deny the Immediate Manager role assignment, select the *Denied* radio button.

6. Enter detailed *Notes* regarding the Immediate Manager role assignment or denial. *Notes are required*.

7. Click Save.
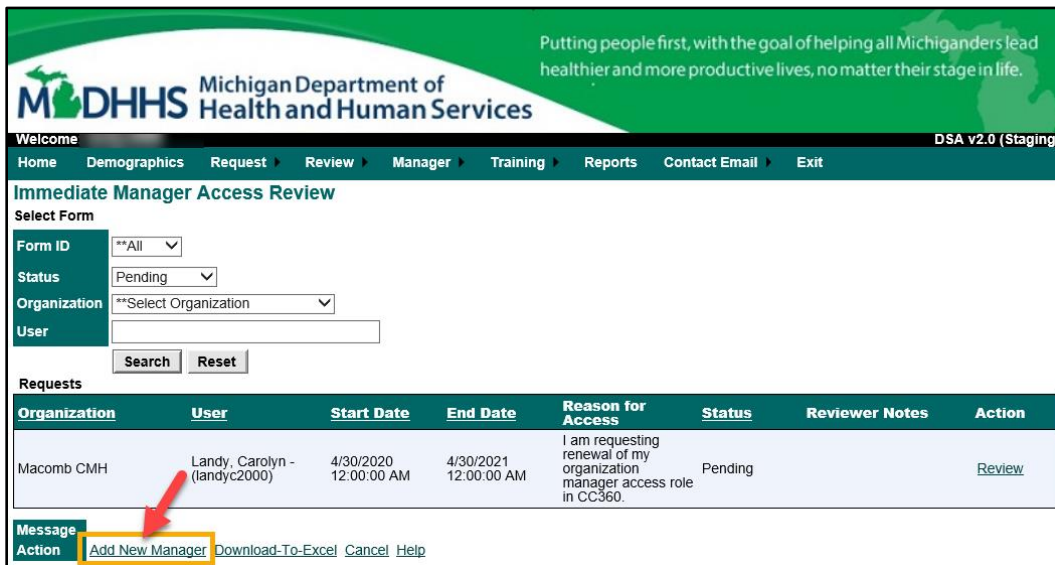
Figure 7.1.3: Review Immediate Manager Access Request

Note: Immediate Managers can also be assigned using the Add New Manager link (*Figure 7.1.4*).

Figure 7.1.4: Immediate Manager Access Review

Upon clicking Add New Manager, the Add Immediate Manager window appears (*Figure 7.1.5*):

✓ Select the access request *Form* for which the user is the Immediate Manager, then select the user's *Organization*.

✓ Begin entering the user's *User ID*, a list of potential suggestions automatically displays. Select the user from the list.

✓ Update the *Start Date* and *End Date* if necessary, otherwise it defaults to a one year timeframe.

✓ Enter detailed *Notes* regarding the Immediate Manager role assignment. *Notes are required*.

✓ Click Add.

Figure 7.1.5: Add Immediate Manager

7.2 Review Organization Manager DSA Role Request

Each organization has an individual assigned the Organization Manager role within the DSA. The Organization Manager approves, grants, and maintains the Immediate Manager role within the DSA for their organization. The Organization Manager role is approved, granted, and maintained by the MDHHS Sponsor.

Complete the following steps to review an Organization Manager DSA role request:

1. Complete the steps in 1.4 Accessing the DSA.
2. Select **Organization Manager Access** from the **Manager** sub-menu (*Figure 7.2.1*). The Organization Manager Access Review page displays.
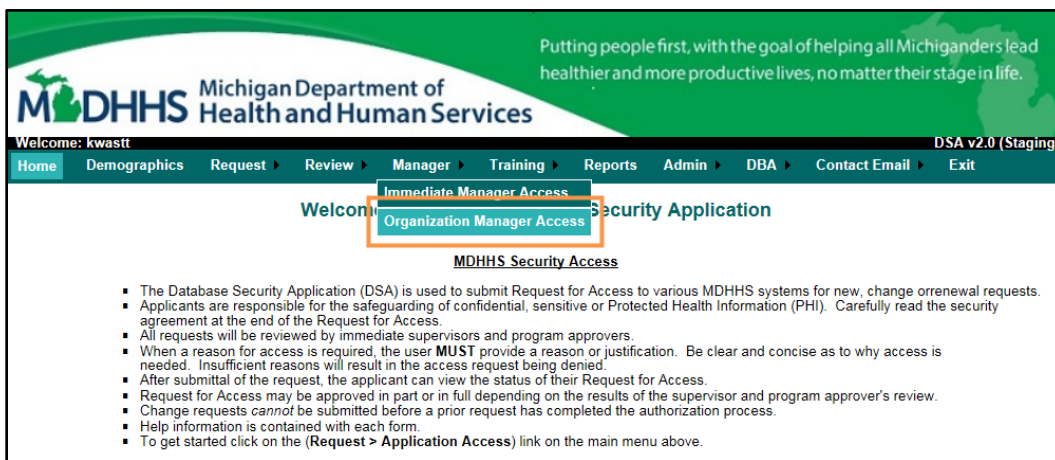

Figure 7.2.1: Home

3. Click Review beside the request to be reviewed (*Figure 7.2.2*). The Review Organization Manager Access Request window displays.
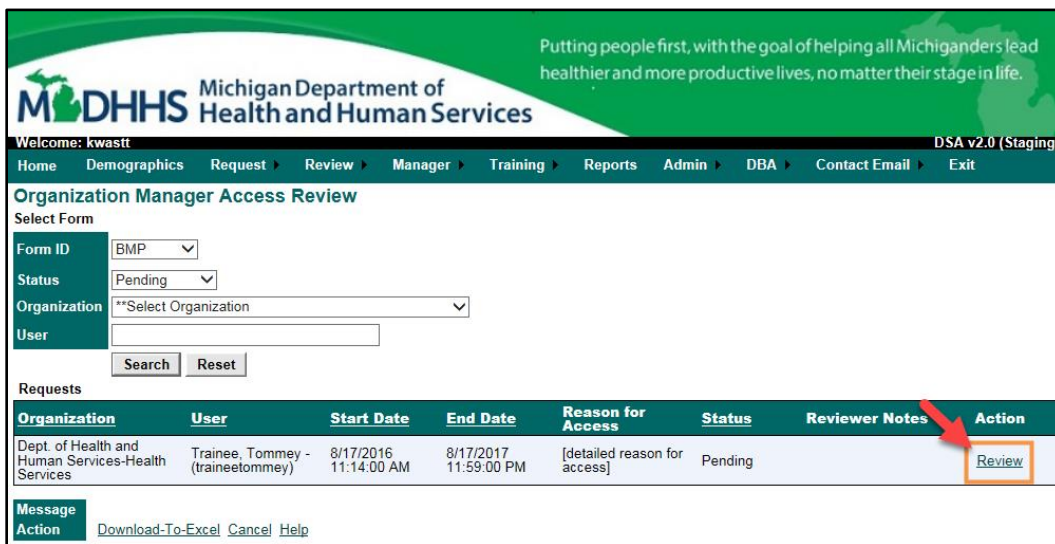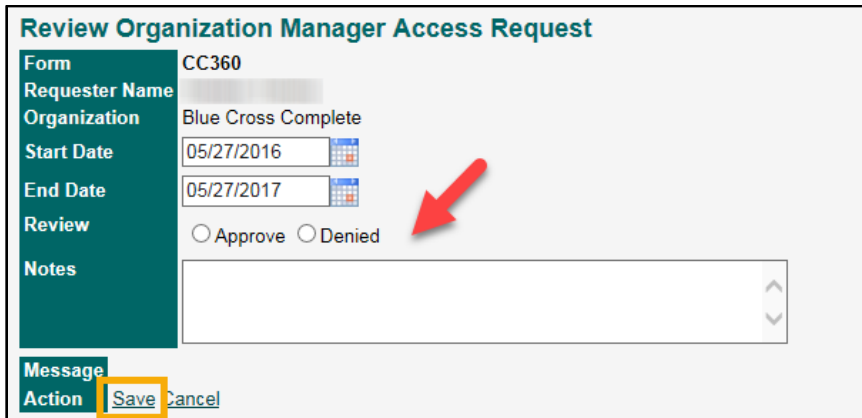

Figure 7.2.2: Organization Manager Access Review

> *Note*: The Organization Manager role defaults to a one-year timeframe. Update the **Start Date** and/or **End Date** if appropriate.

4. To approve the Organization Manager role assignment, select the **Approve** radio button (*Figure 7.2.3*).

5. To deny the Organization Manager role assignment, select the **Denied** radio button.

6. Enter detailed **Notes** regarding the Organization Manager role assignment or denial. *Notes are required*.

7. Click Save.

Figure 7.2.3: Review Organization Manager Access Request

7.3 Assign Backup Approvers

Backup approvers complete reviews when the usual approver is unavailable. All approvers should have one or more backup approver assigned for each approval level for which they are responsible (e.g., Immediate Manager, Program Manager, Director). Backup approvers are designated for a defined timeframe and they must be approved.

Complete the following steps to assign your backup approvers in the DSA:

1. Complete the steps in 1.4 Accessing the DSA.
2. Select **My Backup Users** from the **Request** sub-menu (*Figure 7.3.1*). The My Backup Users page displays.

Figure 7.3.1: Home – Request – My Backup Users

3. If necessary select the access request **Form**, or **Form** and **Role** combination, (*Figure 7.3.2, top*) and click **Search** to narrow items displaying on the **Overview** tab.
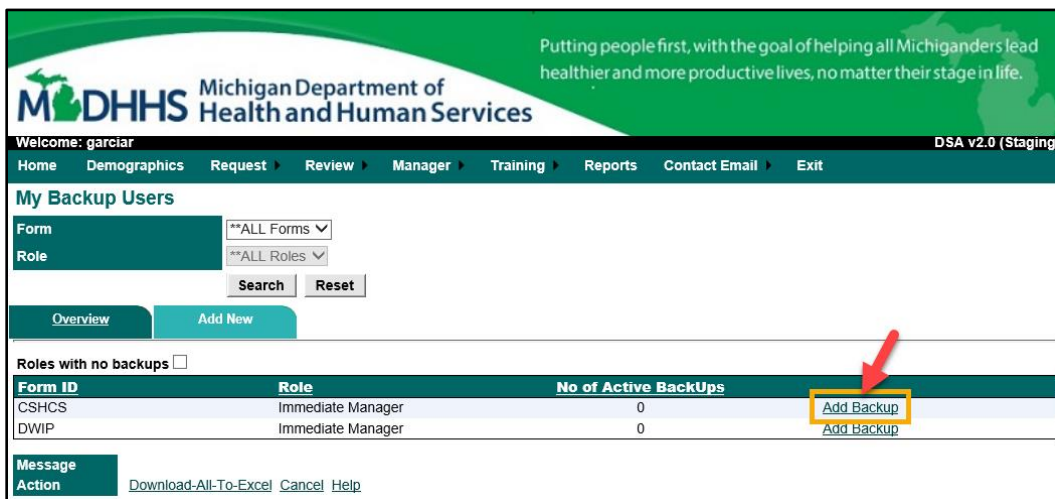

Figure 7.3.2: My Backup Users – Overview

4. To assign a new backup approver:

   a. Click Add Backup (*Figure 7.3.2, above*). The **Add New** tab displays.

   b. Select the checkbox beside the role(s) for which you are adding a backup approver (*Figure 7.3.3*).

   > *Note*: The **Begin Date** and **End Date** default to a one-year timeframe for your backup approver. Update the dates if necessary. Future dates (within one year) are accepted.

   c. Begin entering the backup approver's name in the **Backup User** field. As you enter, a list of potential suggestions automatically displays.

   d. Select your backup approver from the auto-suggestions list. The backup approver's name and user ID populate the **Backup User** field.
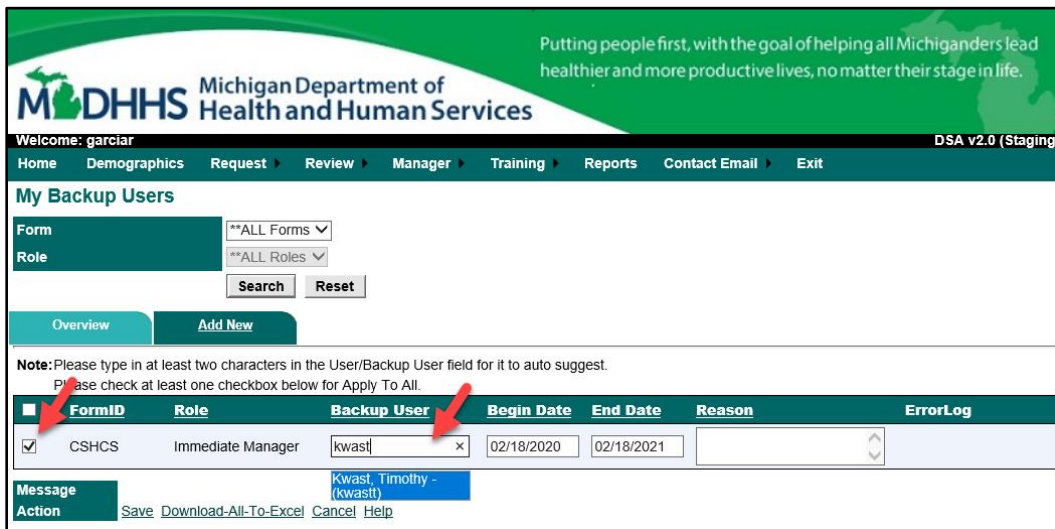

Figure 7.3.3: My Backup Users – Add New

   e. Enter a detailed **Reason** (*Figure 7.3.4*) explaining the backup approver assignment.

   f. Click Save.

   g. Repeat steps 4a-4f to assign additional backup approvers.
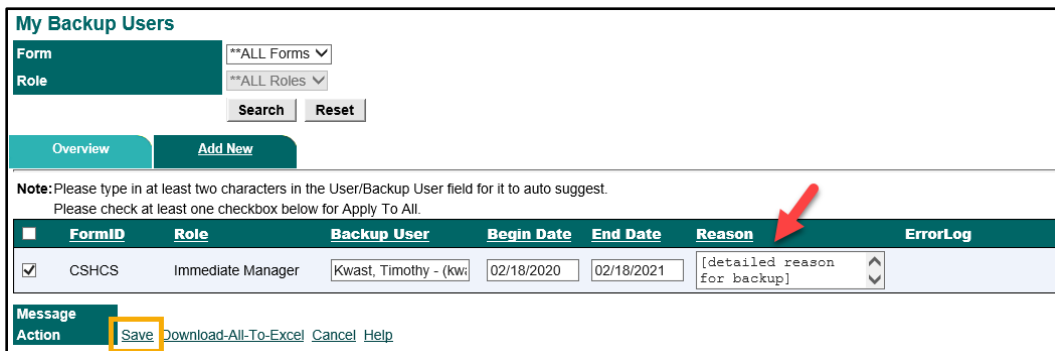

Figure 7.3.4: My Backup Users – Add New

Note: All backup approver assignments remain in a 'Pending' status (*Figure 7.3.5, Pending tab*) until approved by the access request form's Form Administrator. Please reference 7.4 Review Backup Approver Assignments for additional information.
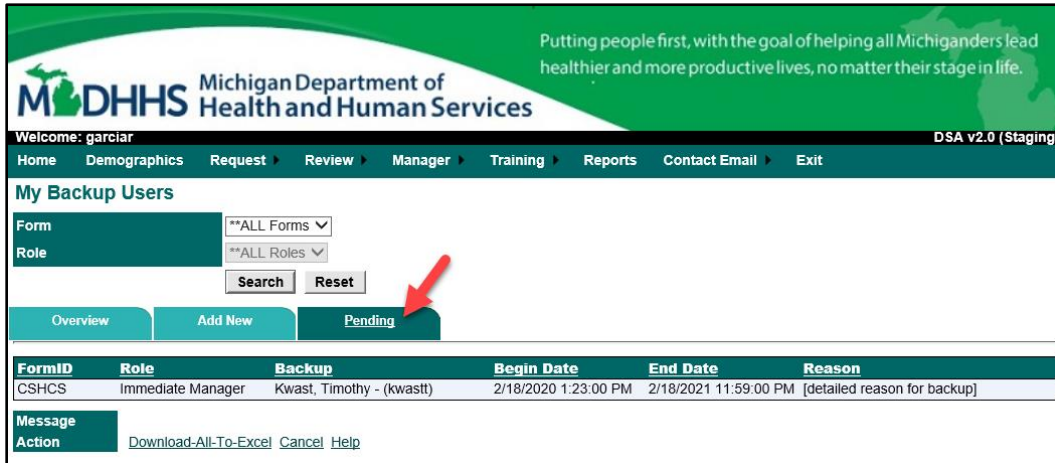

Figure 7.3.5: My Backup Users – Pending

5. To assign backup approvers for multiple approver roles at once:

   a. Access the **Add New** tab (*Figure 7.3.6*).

   b. Select the checkbox beside the roles for which you are designating a backup approver. To 'select all', select the check box in the green header row.

   Note: The **Begin Date** and **End Date** default to a one-year timeframe for your backup approver. Update the dates if necessary. Future dates (within one year) are accepted.
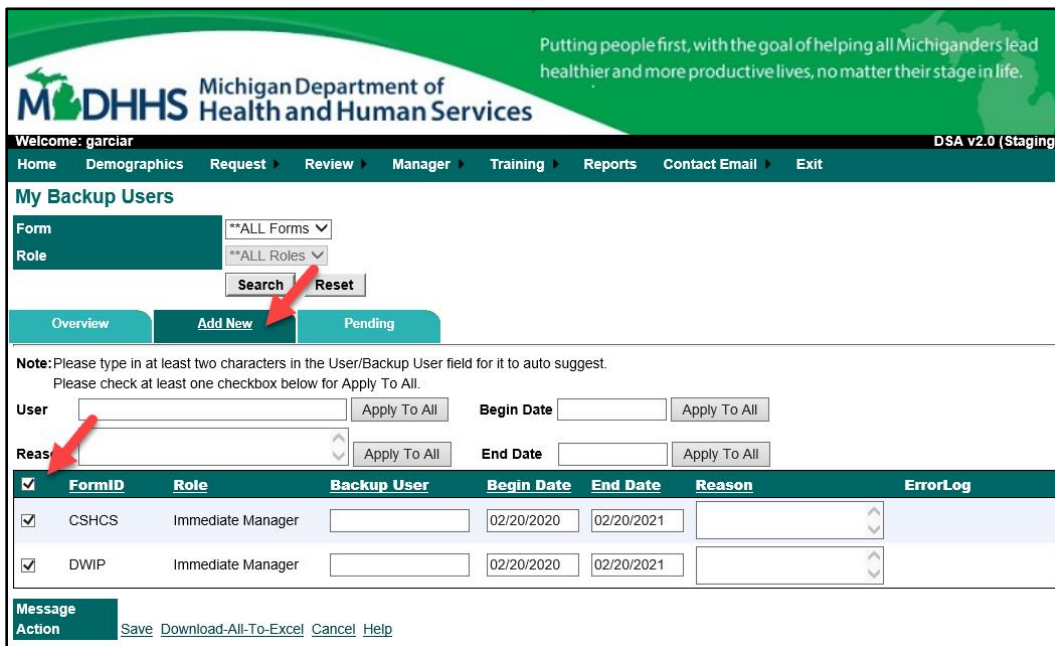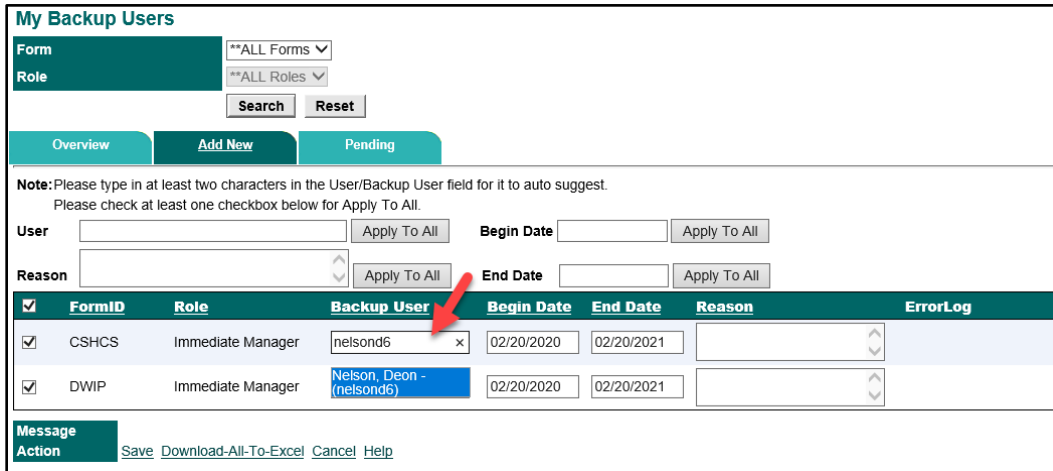

Figure 7.3.6: My Backup Users – Add New

c. Begin entering the backup approver's name in the ***Backup User*** field (*Figure 7.3.7*). As you enter, a list of potential suggestions automatically displays.

d. Select your backup approver from the auto-suggestions list.

Figure 7.3.7: My Backup Users – Add New

e. Enter a detailed ***Reason*** (*Figure 7.3.8*) explaining the backup approver assignment.

f. Complete steps 5a-5e for all rows you selected.

g. Click Save.

Figure 7.3.8: My Backup Users – Add New

6. To assign the same backup approver details for multiple approver roles at once:

   a. Select the checkbox beside the roles for which you are designating a backup approver (*Figure 7.3.9*). To 'select all', select the check box in the green header row.

   b. Begin entering the backup approver's name in the *User* field at the top of the **Add New** tab. As you enter, a list of potential suggestions automatically displays.

   c. Select your backup approver from the auto-suggestions list and click **Apply To All**. The backup approver's name and user ID populate the *Backup User* field for each row selected below.

   d. Enter a detailed reason explaining the backup approver assignment in the *Reason* field at the top and click **Apply To All**. The reason populates the *Reason* field for each row selected below.

   e. If the default one-year timeframe is incorrect for your backup approver assignment, enter the appropriate date(s) in the *Begin Date* and/or *End Date* fields at the top and click **Apply To All**. The corresponding date populates the *Begin Date* and/or *End Date* for each row selected below.

   f. Click Save.

Figure 7.3.9: My Backup Users – Add New

> **IMPORTANT**: Remember, all backup approver assignments remain in a 'Pending' status until approved by the access request form's Form Administrator. Please reference 7.4 Review Backup Approver Assignments for additional information.

7.4 Review Backup Approver Assignments

Users who review and approve MDHHS application access requests are called approvers in the DSA. Backup approvers complete reviews when the usual approver is unavailable.

All approvers should have at least one backup approver assigned for each approval level for which they are responsible. Backup approvers are designated for a defined timeframe and they must be approved by the access request form's Form Administrator.

Complete the following steps to review a DSA backup approver assignment:

1. Complete the steps in 1.4 Accessing the DSA.
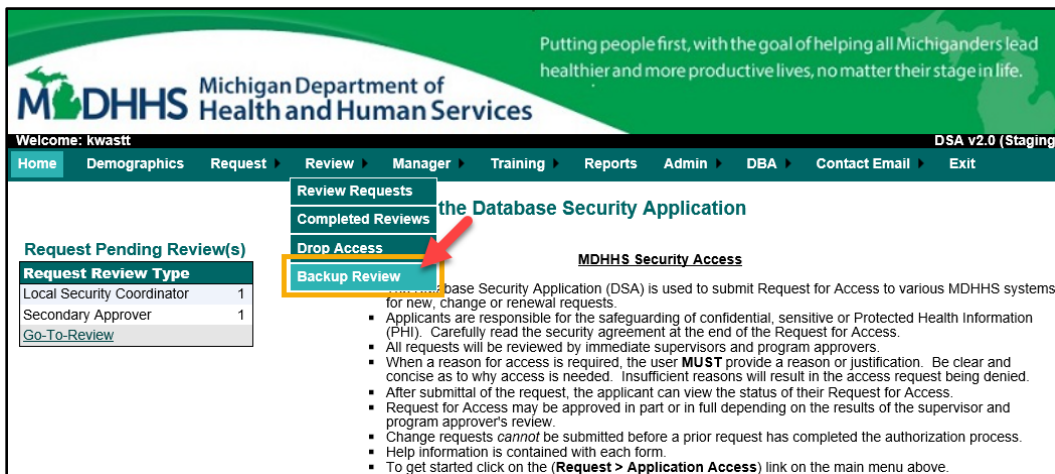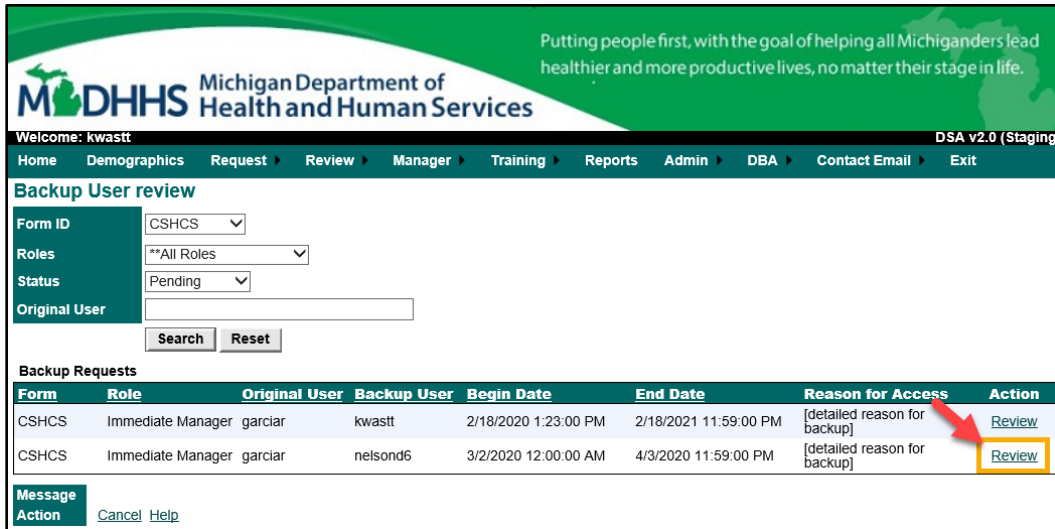2. Select **Backup Review** from the **Review** sub-menu (*Figure 7.4.1*). The Backup User Review page displays.

Figure 7.4.1: Home – Review – Backup Review

3. Click Review beside the backup approver to be reviewed (*Figure 7.4.2*). The Backup User Review window displays.

Figure 7.4.2: Backup User Review

4. To approve the backup approver assignment, select the ***Approved*** radio button (*Figure 7.4.3*).

5. To deny the access request, select the ***Denied*** radio button.

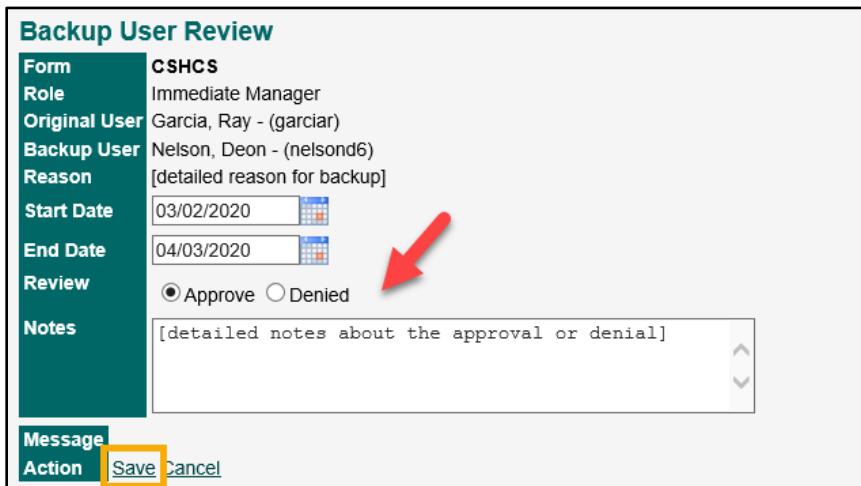6. Enter detailed ***Notes*** about the backup approver approval or denial. *Notes are required*.

7. Click Save.

Figure 7.4.3: Backup User Review pop-up