AccessVUMC Utilization Requirements

Please note:

To utilize the AccessVUMC Identity Management tool, enrollment in Multi-Factor Authentication is required. This extra layer of security ensures that your personal identifiable information (PII) is protected.

If you are not already enrolled, visit the Enterprise Cybersecurity website at:
https://www.vumc.org/enterprisecybersecurity/multi-factor-authentication-mfa

Manage your VUMC ID Menu

- How to Change your Password

- How to Set your Display Name

- View your Profile – Click on the **View Your Profile** button on the AccessVUMC dashboard to see your profile information.

- Forgot your password? View instructions on what to do if you **Forgot Your Password**.

Visit the AccessVUMC Identity Management Project home page for the latest project information.

AccessVUMC Identity Management Tool
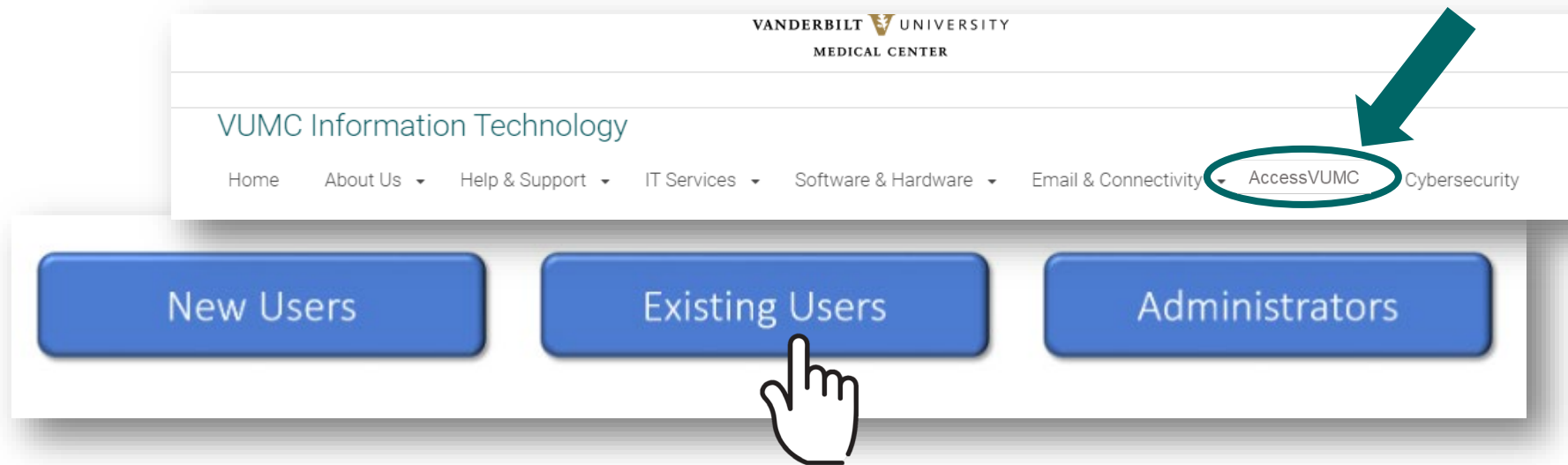## How to Change a Password

AccessVUMC Identity Management

Return to Menu

VANDERBILT UNIVERSITY
MEDICAL CENTER

Users with a valid VUMC ID **AND** enrolled in Multi-Factor Authentication (MFA) can use AccessVUMC to change/reset a password.

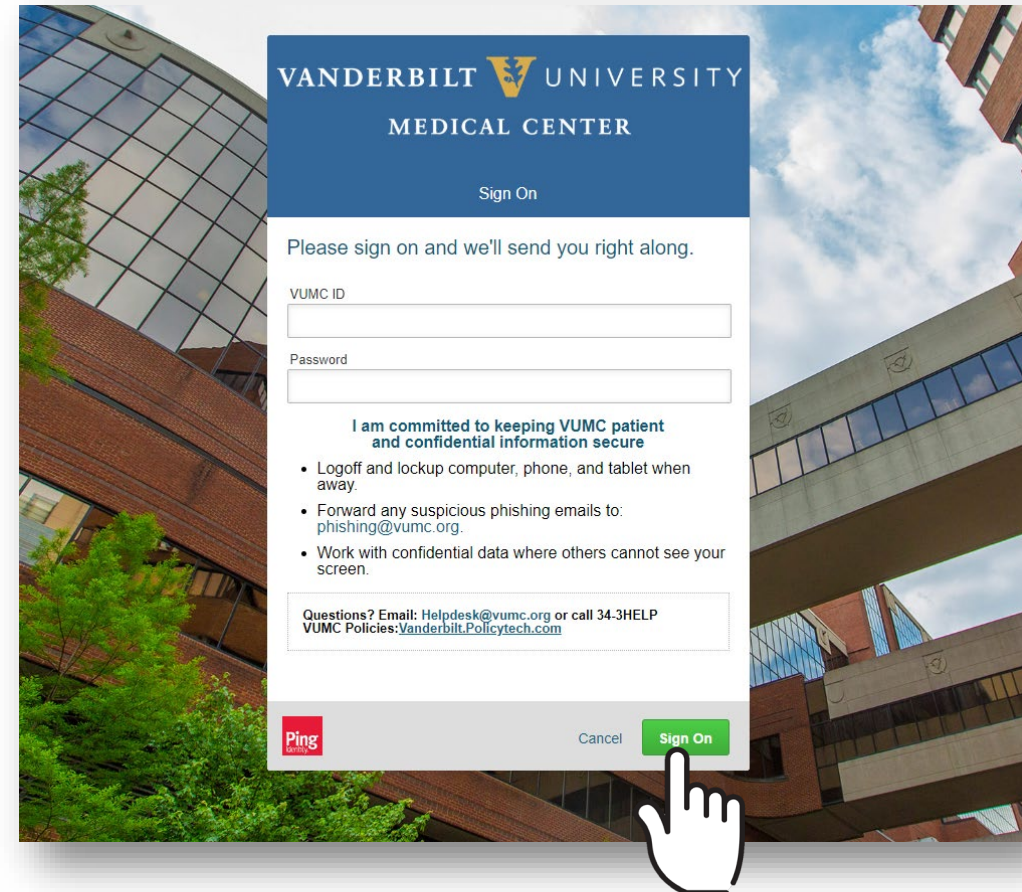- Click **Existing Users** from the AccessVUMC home page https://www.vumc.org/it/accessvumc.

- From the AccessVUMC home page, you will be prompted to authenticate using your VUMC ID and password.
- Click **Sign On**.

- You will then be prompted to enter a Multi-Factor Authentication passcode.

NOTE: Your MFA sign on experience will vary based upon your MFA enrollment status (e.g. token, SMS texting, etc.).

- Click **Sign On** once you have entered your passcode.

MFA Sign on for SMS Text users

MFA Sign on for Token users

AccessVUMC Identity Management

Click **Change VUMC ID Password** from the AccessVUMC dashboard.

VANDERBILT UNIVERSITY
MEDICAL CENTER
Information Technology
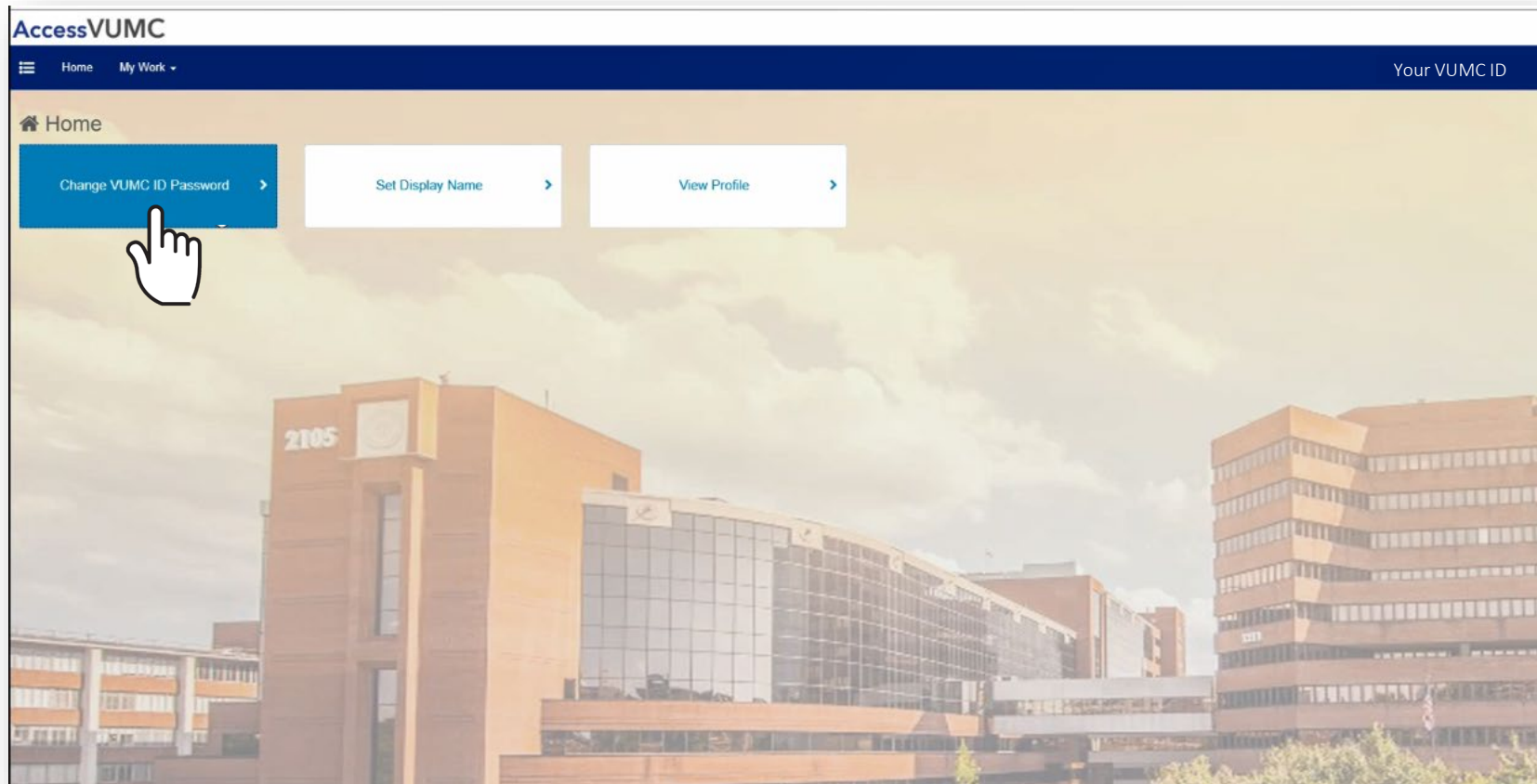
Click **Accept** once you have read the VUMC Acceptable Use Policy regarding your computer privileges and responsibilities.

E. Publication or Distribution of Unauthorized Recordings, Photos, Images, Text or Video

With the availability of low cost cameras, smart phones, and consumer electronics, it is possible for someone to acquire voice, video images, still images, multimedia, or text in non-public situations without the knowledge or consent of all parties. VUMC network computing assets must not be used by anyone in the organization to publish or distribute this type of material without the expressed consent of all involved parties.

F. Right to Copy and Inspect for Legal, Regulatory, and VUMC Purposes

VUMC is committed to protecting the privacy of faculty, students, staff, patients, and other users of its IT resources, and their electronic communications. However, because VUMC operates subject to compliance with various federal and state laws and regulations and must be able to enforce its own policies, VUMC must occasionally inspect, preserve and produce records to fulfill legal obligations and to carry out internal investigations. VUMC reserves the right to obtain, copy, and convey to outside persons any records or electronic transactions completed using VUMC information systems in the event it is required by law or institutional policy to do so. VUMC may also in its reasonable discretion, when circumstances require, obtain and review any records relevant to an internal investigation concerning compliance with VUMC rules or policies applicable to faculty, staff, or to all others granted use of VUMC's information technology resources. Users therefore should not expect that records created, stored or communicated with VUMC information technology or in the conduct of VUMC's business will necessarily be private. VUMC reserves its right to any work product generated in the conduct of its business.

G. Locally Specific Policies

Individual units within VUMC may create additional policies for information resources under their control. These policies may include additional detail, guidelines and further restrictions but must be consistent with principles stated in this policy document. Individual units adopting more specific policies are responsible for establishing, publicizing and enforcing such policies, as well as any rules governing the authorized and appropriate use of equipment for which those units are responsible.
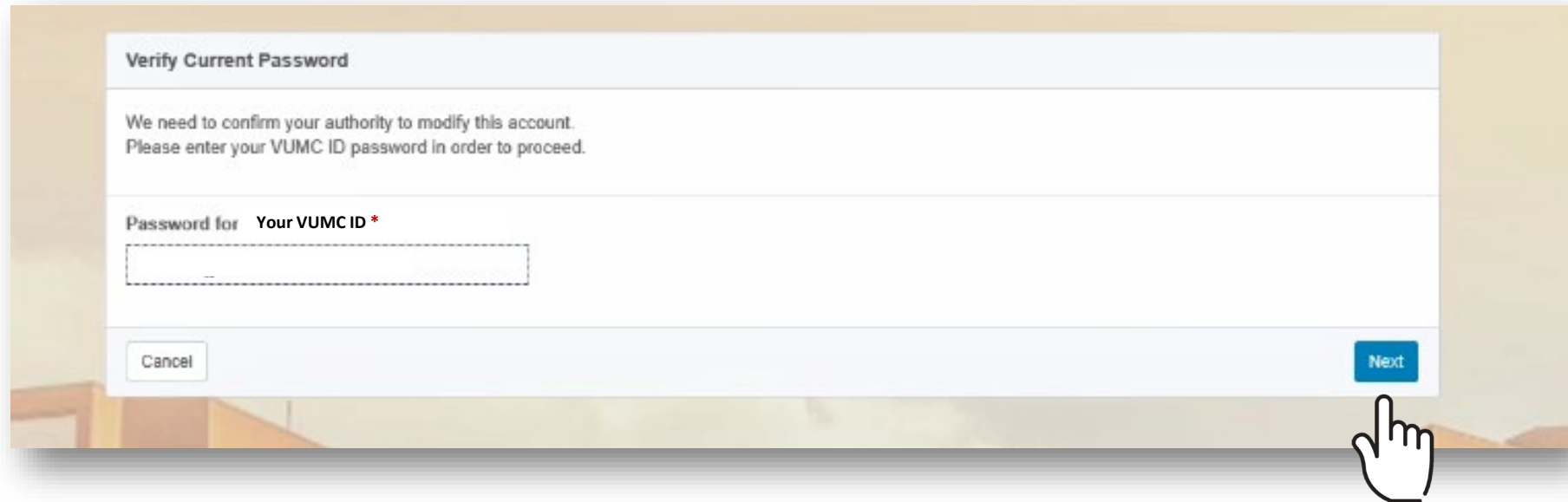
IV. Disclosures

A. All members of the VUMC Workforce Members are given notice of this policy by virtue of its publication and are subject to it on the same basis. Ignorance of this policy does not relieve any user of his or her responsibilities under the policy. All Workforce Members are expected to familiarize themselves with the contents of this policy and act in conformance with these principles regarding any use of VUMC's IT resources.

B. Due to the rapid nature of change in both information technologies and their applications, VUMC may amend this policy whenever deemed necessary or appropriate. Users are encouraged to periodically review this policy in order to understand their rights and responsibilities under it.

I Decline | Accept

VANDERBILT UNIVERSITY
MEDICAL CENTER
Information Technology

8

- Verify your current password.

- Click **Next**.

- Enter and confirm your **NEW** password.

- Click **Submit**.

VUMC Password Requirements

1. You cannot reuse your last 10 passwords.

2. Passwords **MUST CONTAIN:**
   - At least eight (8) characters
   - Characters from at least three (3) character sets:
   Lowercase Letters: abcdefghijklmnopqrstuvwxyz
   Uppercase Letters: ABCDEFGHIJKLMNOPQRSTUVWXYZ
   Numbers: 0123456789
   Special Characters: ~!@#$%^&*()_+-=;./[]<>,?{}

3. Passwords **CANNOT CONTAIN**:
   - More than 16 characters
   - Three (3) consecutive characters from the VUMC ID
   - Primary email
   - Last name
   - Display name
   - VUMC ID in reverse

4. Your password will be checked against commonly used terms.

- You will receive a confirmation screen that your password was successfully re-authenticated.

- You will also receive an email that your password was changed.

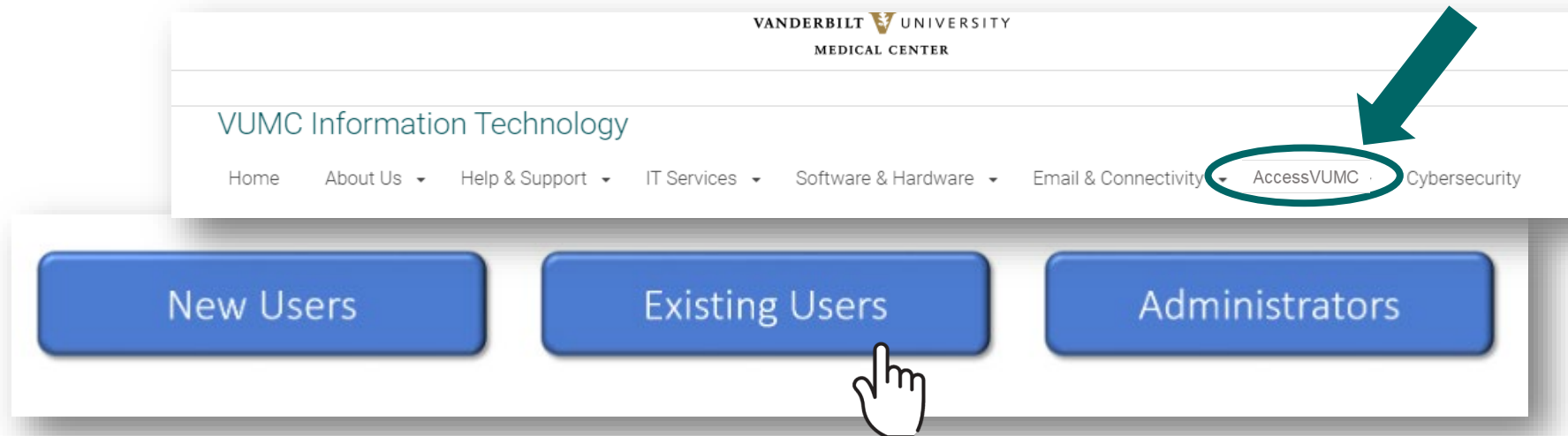- Click **OK**.
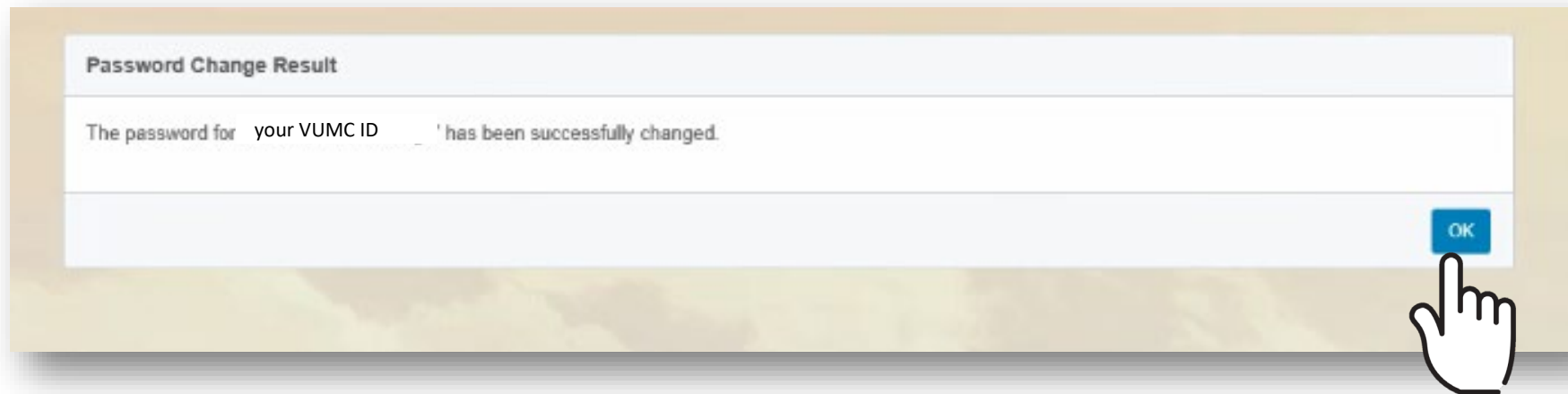
AccessVUMC Identity Management Tool
How to Set a Display Name

AccessVUMC Identity Management

Return to Menu

VUMC employees enrolled in Multi-Factor Authentication AND with a valid VUMC ID can use AccessVUMC to Set a Display Name.

- Click **Existing Users** from the AccessVUMC website https://www.vumc.org/it/accessvumc.

To enroll in Multi-Factor Authentication now, visit
www.vumc.org/enterprisecybersecurity/mfa

AccessVUMC Identity Management

From the AccessVUMC homepage, you will need to authenticate using your VUMC ID and password and **Sign On**.

Information Technology

- You will then be prompted to enter a Multi-Factor Authentication passcode.

NOTE: Your MFA sign on experience will vary based upon your MFA enrollment status (e.g. token, SMS texting, etc.).

- Click **Sign On**.

MFA Sign on for SMS Text users

MFA Sign on for Token users

VANDERBILT UNIVERSITY
MEDICAL CENTER
Information Technology

AccessVUMC Identity Management

15

Click **Set Display Name** from your AccessVUMC Dashboard.
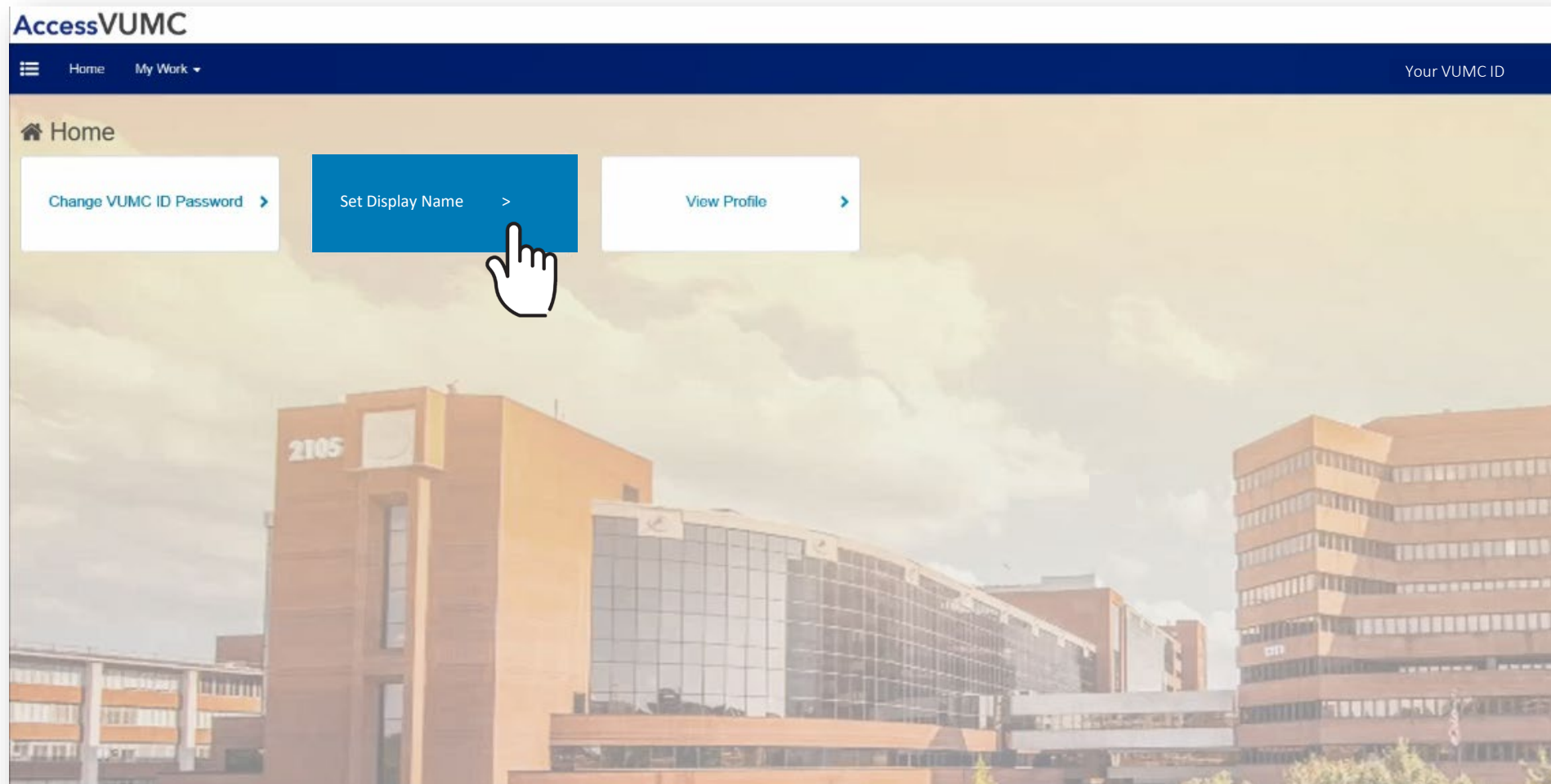
- The Account's **Current Display Name, Last Name, First Name and Middle Name** will automatically appear.
- Enter the **New Display Name**.
- Click **Next**.

Set Display Name

Display Name is the name shown in the VUMC Corporate Outlook and Skype address list. You may customize First Name and Middle Name to your preference. Last Name cannot be modified. When you are ready to review your changes, click 'Submit'.

Account

Current Display Name

Doe, Jon

Last Name	First Name *	Middle Name
Doe	Timothy	Johnathon

New Display Name

Timothy Doe

Cancel   Next

How to Set a Display Name

- Confirm the new display name on your account.
- Click **Submit**.

AccessVUMC Identity Management

Information Technology

VANDERBILT UNIVERSITY
MEDICAL CENTER