



## All-Payer Model Amendment and Care Redesign Programs

*CMS Overview of Data Provided to Care Redesign Program Participant Hospitals*

*9:00-10:00 EST*

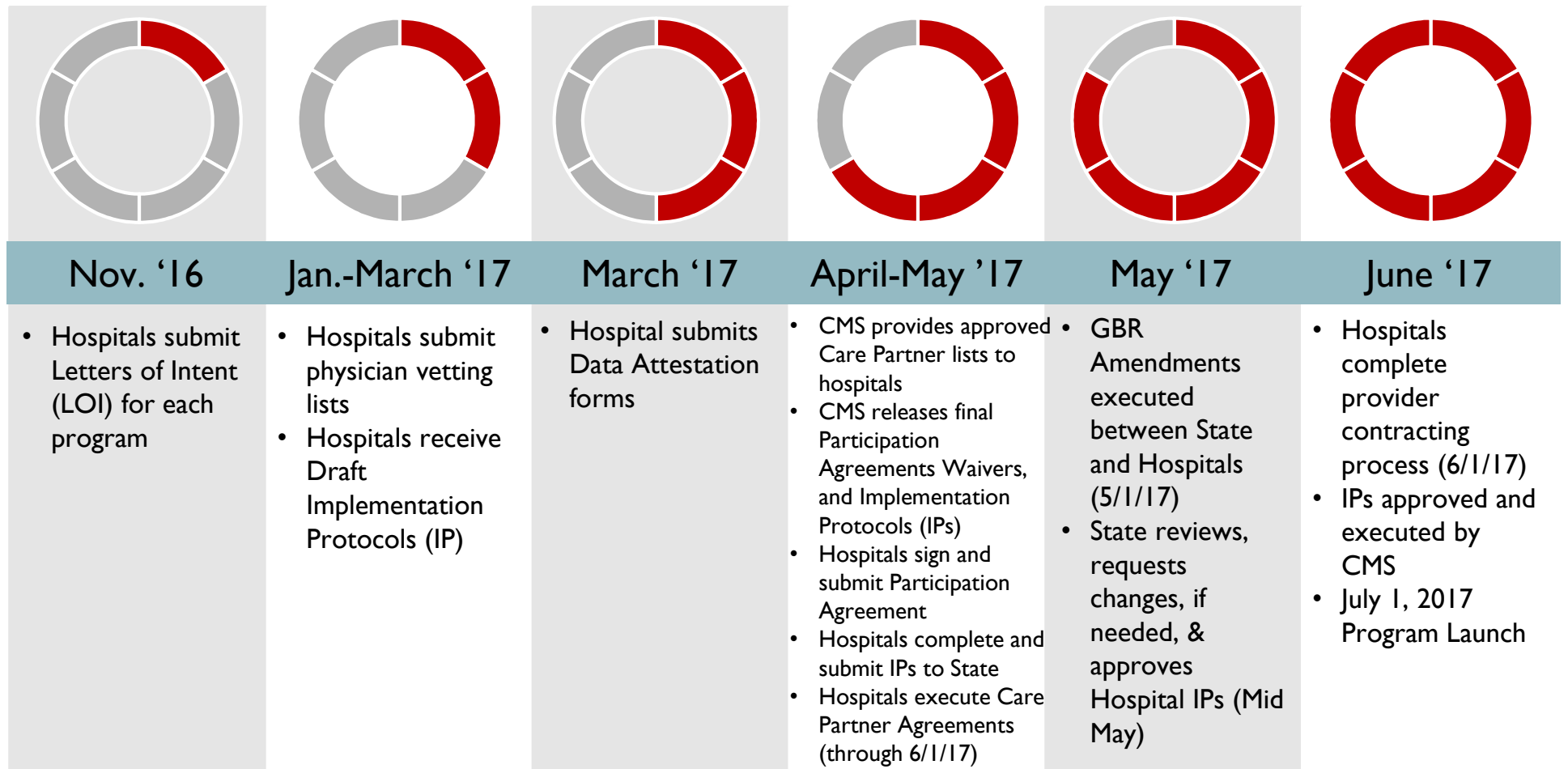
*Thursday, March 30, 2017*

# Introductions

---

- HSCRC
- CMMI
- Lewin Group

# Updated Timeline for HCIP & CCIP Implementation



# Agenda

---

- Medicare Data Extracts
- Use of the MDAPM Exchange Portal on the CCW
- Questions

# This session will cover

---

- What is in your Medicare data extracts
- How to access your Medicare data
  - CCW account registration
  - First time log in
  - Logging in
  - Downloading data and logging out

# MEDICARE DATA EXTRACTS

---

Overview

Content and Use

Differences from ACO Files

# Medicare Data Extracts: Overview

---

- Extracts are hospital-specific
- Ten (10) files provided to each hospital each month
  - Content and formats closely resemble data provided to NextGen ACOs
  - The data files are considered Protected Health Information (PHI)
- Contain multiyear data for the period ending with the last Friday of the Reporting Month
  - E.g., July extracts contain data up through the last Friday of June
- Medicare Claims, enrollment and clinical data for patients admitted to your hospital in the multiyear observation period
  - Patients who were not residents of Maryland at the time of admission are excluded

# Medicare Data Extracts: Overview (con't)

---

Part A Header File	Part B DME File
Part A Revenue Center Detail	Part D File
Part A Procedure Codes File	Beneficiary Demographics File
Part A Diagnosis Codes File	Beneficiary XREF File
Part B Physicians File	Summary Statistics Record

- All data files available in both SAS and Comma Separated Values (CSV) formats
- Additional supplemental files include the technical specifications with a data dictionary



# Part A Header File

---

- Contents
  - Summary claims from
    - Home Health Agencies (HHAs)
    - Skilled Nursing Facilities (SNFs)
    - acute care hospitals (inpatient and outpatient claims)
    - hospice facilities
- Uses
  - Provides beneficiary-level spending on facility services (overall, by diagnostic related group (DRG), or by principal diagnosis)
  - Permits calculation of proportion of services for the hospital's Medicare beneficiaries that are provided by the hospital versus non-hospital providers.

# Part A Revenue Center Detail File

---

- Contents
  - Line-item level detail for each claim from the Part A Claims Header File
  - Healthcare common procedure coding system (HCPCS) for each service received, as well as the date the service was received
- The file does **not** contain payment amounts for individual services
  - Use Part A claim header record to identify payment amounts in line-item records
- Uses
  - To identify costs by types of service

# Part A Procedure Codes Files

---

- Contents
  - Detailed information regarding the claims from the Part A Claims Header File, such as the type of procedure performed and the date it was performed
- Uses
  - This file can be used in conjunction with the Part A Claims Header File to aggregate services by procedure

# Part A Diagnosis Codes Files

---

- Contents
  - Diagnosis codes for the principal diagnosis, as well as all secondary diagnoses from the Part A Claims Header File
  - Secondary diagnoses can be distinguished from one another using the unique claim identifier
  - The part A diagnosis files have diagnosis code 1 through (up to) 25. Diagnosis code 1 is either always or almost always (99.9%) the same as principal diagnosis code.
- Uses
  - Used in conjunction with the Part A Claims Header File to identify secondary diagnoses that are associated with a given principal diagnosis

# Part B Physicians File

---

- Contents
  - Services delivered by physicians, practitioners, and suppliers
  - Both claim level and line level information
  - At the claim level, the file contains date of service, and type of claim (Durable Medical Equipment, Prosthetics, Orthotics, and Supplies (DMEPOS) or non-DMEPOS)
  - At the line level, the file contains provider specialty, date of service, HCPCS code, payment amount, diagnosis code, primary payer, provider Taxpayer Identification Number (TIN), and rendering NPI number
  
- Uses
  - To identify the proportion of total Part B services supplied by specific providers

# Part B DME File

---

- Contents
  - Claim-level and line-level information
  - Claim-level information includes:
    - date of service
    - type of claim submitted (DMEPOS versus non-DMEPOS)
  - Line-level information includes:
    - date of service
    - HCPCS code
    - payment amount
    - ordering NPI number
    - paid to NPI number
- Uses
  - To identify the types of DME being supplied to Medicare beneficiaries

# Part D File

---

- Contents
  - Prescription drug information at the beneficiary level
  - Some of the data elements in this file include
    - National Drug Code (NDC)
    - quantity dispensed
    - days supply
    - prescribing provider ID
    - service provider ID (e.g., pharmacist)
    - patient payment amount
- Uses
  - To determine the medications prescribed to Medicare beneficiaries and the costs of the medication, including cost sharing

# Beneficiary Demographics

---

- Contents

- Demographic characteristics of patients admitted to your hospital, including
  - current HICN
  - Beneficiary ID
  - ZIP code
  - date of birth (DOB)
  - sex
  - race
  - Medicare Status Code
  - dual eligibility status
- This file also contains hospice information

- Uses

- Identify the key patient characteristics and help identify populations or communities that are over/under utilizers



# Beneficiary XREF File

---

- Contents
  - The beneficiary's current HICN and any previous HICNs
    - For example, if a beneficiary becomes a widow or widower or remarries, the beneficiary's HICN is likely to change
  - Beneficiary ID (BENE\_ID), which remains constant over time, is also provided
- Uses
  - Provides ability to link claims from a unique beneficiary over time

# Summary Statistics and Supplemental Files

---

- The Summary Statistics File contain record counts for each file sent to the hospital
- Technical Specifications Document
  - Provides information describing how each data file was constructed and its contents
  - Data Dictionary
    - Provides brief description of the variables in the data

# Differences from ACO Files

---

- Certain Variables are excluded from MD Hospital extracts
  - Claim Adjustment Type code
  - Claim Provider Type code
  - HICN effective and end dates
- Additional variables added to MD Hospital Extracts
  - Medicare BENE\_ID

# QUESTIONS?

---

# USE OF THE MDAPM EXCHANGE PORTAL ON THE CCW

---

MDAPM Exchange Portal on the CCW

CCW System Requirements

New User Access Request Process Flow

Access Request Process Steps

Preparing for First Time Log In

Downloading the Symantec VIP App

Linking your Symantec Credential

Future Visits: Logging into the MDAPM Exchange Portal on the CCW VRDC

Downloading Your Medicare Data

# MDAPM Exchange Portal on the CCW

---

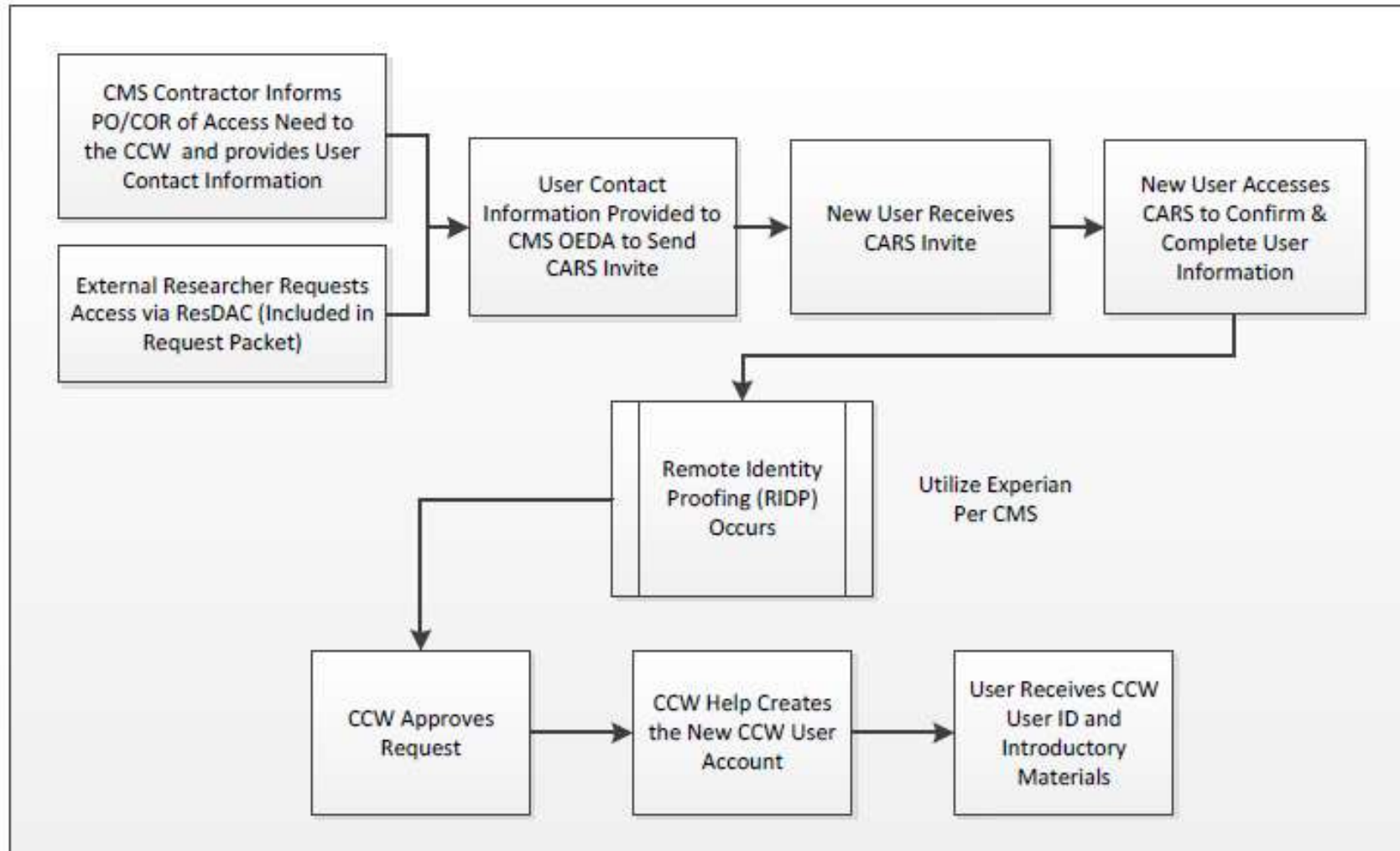
- Data will be stored on the Chronic Condition Data Warehouse (CCW) Virtual Research Data Center (VRDC)
  - A Web-based secure file transfer system (CCW SFTS)
    - Securely houses data
    - Encrypts data upon download
    - Mechanism for securely exchanging data including PHI or PII
- Other CMMI models utilize the CCW SFTS to transfer data
- Each participating hospital will have its own designated folder
  - Users cannot access another hospital's data

# CCW System Requirements

---

- Supported Web browsers are the current version and one previous version of Microsoft Internet Explorer
  - To take advantage of the full functionality of the CCW STFS features, Microsoft Internet Explorer is recommended
- Currently supports Windows 7 or newer operating systems
  - Does not support MAC
- Disable caching
- Requires Multi-Factor Authentication (MFA)
- Must have enough free disk space to hold the file to be downloaded

# New User Access Request Process Flow





# Access Request Process Steps: Step 1

---

- MDAPM Exchange Portal Users
  - Each hospital may have up to 3 users
    - Users were identified on your hospital's Letter of Intent or the Technical Capability Survey
      - In instances where more than 3 users were submitted, Lewin will use the contacts submitted on the LOI unless otherwise instructed by the hospital
    - Contact [MarylandModel@cms.hhs.gov](mailto:MarylandModel@cms.hhs.gov) to replace a user for your hospital
  - Portal users should be personnel that will be using the Medicare data extracts
- Requirements for account registration
  - A unique business e-mail address
  - A completed Participation Agreement
  - An approved Data Attestation Agreement (for continued data use)

## Access Request Process Steps: Step 2

---

- The Lewin Group will compile your hospital's user contact information
  - First Name
  - Last Name
  - Unique Business Email
  - User's Hospital
  - DAA number
- Your hospital's user contact information will then be forwarded to CMS Office of Enterprise Data and Analytics (OEDA) to initiate creation of user access credentials

## Access Request Process Steps: Step 3

---

- Users will receive an email from CCW Help with a link and instructions
- Click on the link and complete the access request information

Hello John,

Joe Smith, sent you an invite to access the Chronic Condition Data Warehouse (CCW).

Please follow the link below which will only be available for fourteen days. Please access this request before it expires on 11/19/14 12:00 AM.

[https://www.ccwdata.org/acces\\_request\\_flow/public/new\\_request?reqId=<request ID>](https://www.ccwdata.org/acces_request_flow/public/new_request?reqId=<request ID>)

If you are unable to create your request before it expires, please contact Joe Smith to request a follow-up invitation.

Please keep this email until your application is complete. The link above will allow you to access your request during the request process.

Sincerely,  
The CCW Team

# Access Request Process Steps: Step 4

- The **New User Request – User Information** page will display

**New User Request - User Information**

Step 1 User Information | Step 2 Contact Info | Step 3 IT Contact | **Step 4 Review** | Step 5 Finished

The information below is required to grant access to secure areas of the CCW environment. Only authorized users will be granted access.  
Required fields are marked with red asterisk (\*). Blue fields are read-only and have been filled out by the form initiator.

**CCW User Agreement**

CCW User Agreement:  
The CCW solution is provided with funding from the Centers for Medicare & Medicaid Services for use by Quality Improvement Organizations, CMS-approved research projects (including pilots), healthcare reform projects, interagency agreement projects, and/or CMS staff. This User Agreement is designed to tell you about the practices regarding collection, use, and disclosure of information that you may have access to with CCW. Please be sure to read this entire User Agreement. In order to ensure the integrity, security, and confidentiality of information maintained by CCW, and to permit appropriate disclosure and use of such data as permitted by law, the User enters into this Agreement with CCW to comply with the following specific paragraphs. The User represents and warrants further that he/she shall not disclose, release, reveal, show, sell, rent, lease, loan, or

Yes, I have read and agree to these terms: \*

**User Information**

First Name: \* John  
Last Name: \* Doe  
Business Email: \* John.Doe@ccw.com  
User's Company or Organization: \* Respona

**CCW Profile**

CMS Department: \* CCW  
Program Name: \* ID  
Project Name: \* Study and Report

Save Changes Save and Continue

- Confirm or correct entries then select **Save and Continue**

# Access Request Process Steps: Step 5

- The **New User Request – Contact Information** page will display

**New User Request - Contact Information**

Step 1  User Information → Step 2  Contact Info → Step 3  IT Contact → Step 4  Review → Step 5  Finished

Required fields are marked with red asterisk (\*).

**Contact Information**

Business Address: \*

City: \*

State: \*

Zip Code: \*

Telephone: \*

Telephone Ext:

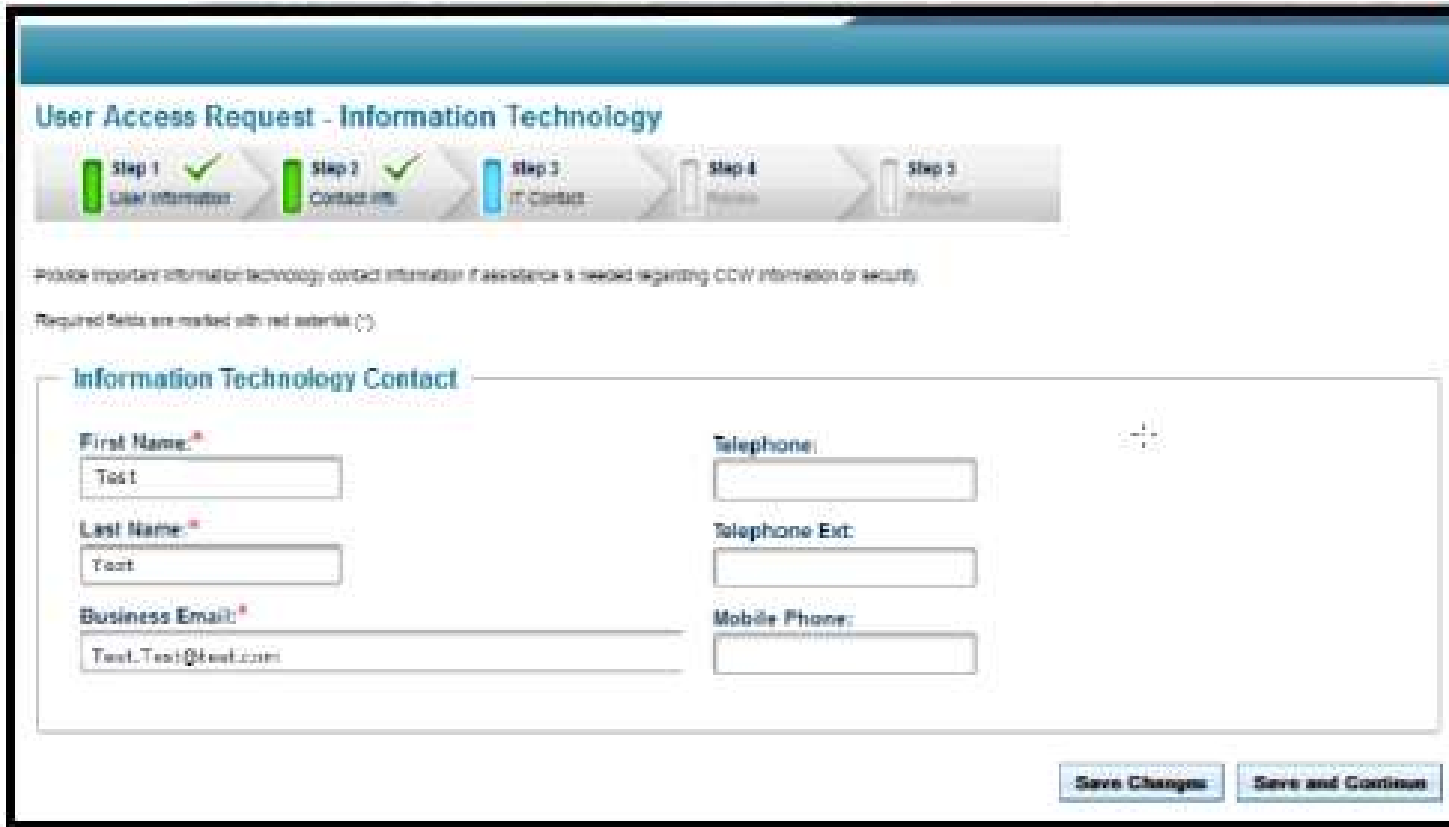
Mobile Phone:

Fax:

- Confirm or correct entries then select **Save and Continue**

# Access Request Process Steps: Step 6

- The **User Access Request – Information Technology** page will display



The screenshot displays the 'User Access Request - Information Technology' page. At the top, a progress bar shows five steps: Step 1 (User Information), Step 2 (Contact Info), Step 3 (IT Contact), Step 4 (Phone), and Step 5 (Mobile). Step 3 is currently active. Below the progress bar, a note states: 'Please provide information technology contact information if assistance is needed regarding CCW information or security.' A warning message indicates 'Required fields are marked with red asterisk (\*)'. The main form area is titled 'Information Technology Contact' and contains the following fields:

First Name: *	Telephone:
<input type="text" value="Test"/>	<input type="text"/>
Last Name: *	Telephone Ext:
<input type="text" value="Test"/>	<input type="text"/>
Business Email: *	Mobile Phone:
<input type="text" value="Test.Test@test.com"/>	<input type="text"/>

At the bottom right of the form, there are two buttons: 'Save Changes' and 'Save and Continue'.

- Confirm or correct entries then select **Save and Continue**

# Access Request Process Steps: Step 7

- The **New User Request – Review** page will display

The screenshot displays the 'New User Request - Review' page. At the top, a green message box states 'The Access Request changes has been successfully saved.' Below this is a progress bar with five steps: Step 1 (User Information), Step 2 (Contact Info), Step 3 (IT Contact), Step 4 (Review), and Step 5 (Pending). Steps 1-3 are marked with green checkmarks, and Step 4 is highlighted in blue. A note indicates 'Required fields are marked with red asterisk (\*)'.

**User Information**

First Name: *	Business Email: *
<input type="text" value="John"/>	<input type="text" value="John.Doe@test.com"/>
Last Name: *	User's Company or Organization: *
<input type="text" value="Doe"/>	<input type="text" value="Associate"/>

**CCW Profile**

CMS Department: *
<input type="text" value="CRM"/>
Program Name: *
<input type="text" value="LO"/>
Project Name: *
<input type="text" value="Study and Support"/>

**Information Technology Contact**

First Name: *	Telephone:
<input type="text" value="Test"/>	<input type="text"/>
Last Name: *	Telephone Ext:
<input type="text" value="Test"/>	<input type="text"/>
Business Email: *	Mobile Phone:
<input type="text" value="Test.Test@test.com"/>	<input type="text"/>

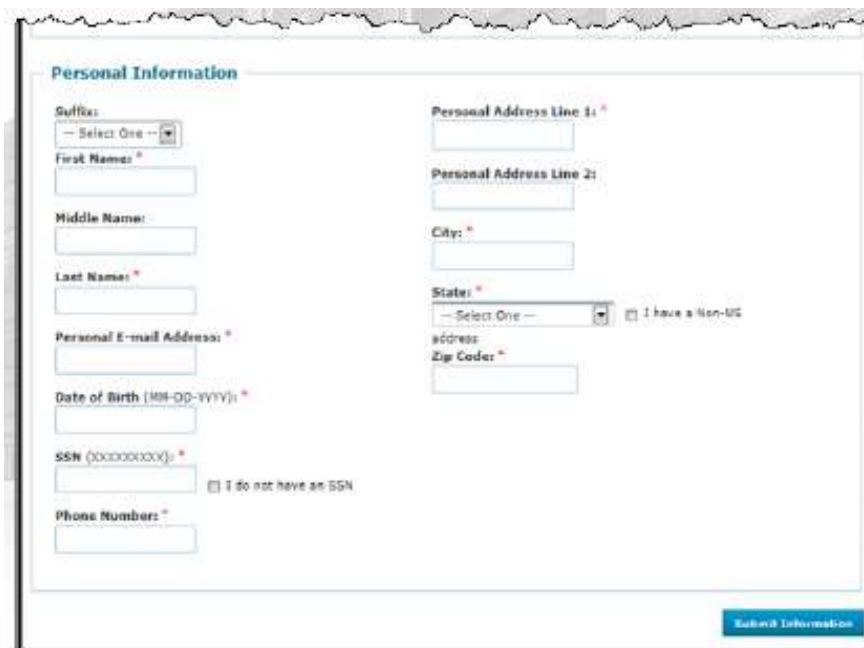
Buttons:

- Confirm or correct entries then select **Save and Continue**

# Access Request Process Steps: Step 8

---

- Identity Confirmation ('Proofing')
- Enter requested information and then select **Submit**
  - The personal information you provide is securely encrypted and sent to Experian
    - It may look like “phishing” but it is not – your inputs are destroyed as soon as non-PI data are retrieved

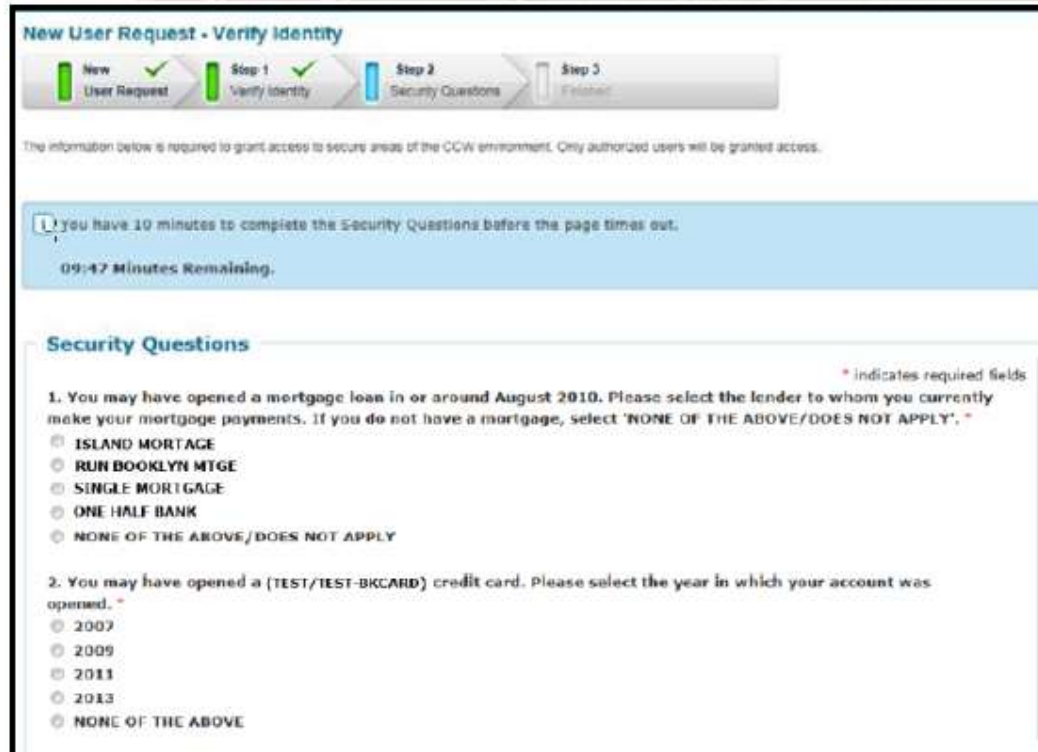


The image shows a screenshot of a web form titled "Personal Information". The form is divided into two columns of input fields. The left column contains: "Suffix:" with a dropdown menu showing "-- Select One --"; "First Name:"; "Middle Name:"; "Last Name:"; "Personal E-mail Address:"; "Date of Birth (MM-DD-YYYY):"; "SSN (XXXXXXXX):" with a checkbox "I do not have an SSN"; and "Phone Number:". The right column contains: "Personal Address Line 1:"; "Personal Address Line 2:"; "City:"; "State:" with a dropdown menu showing "-- Select One --" and a checkbox "I have a Non-US address"; and "Zip Code:". A blue "Submit Information" button is located at the bottom right of the form.



# Access Request Process Steps: Step 9

- You will have ten minutes to answer five (5) security questions (which are specific to you)
  - Based on non-PI data from credit history – such as make and model of recent auto lease
  - These questions are not meant to be easy to answer
    - But only you should know the answer



The screenshot shows a web interface for a 'New User Request - Verify Identity' process. At the top, a progress bar indicates four steps: 'New User Request' (green), 'Step 1 Verify Identity' (green), 'Step 2 Security Questions' (blue), and 'Step 3 Finished' (grey). Below the progress bar, a warning message states: 'The information below is required to grant access to secure areas of the CCW environment. Only authorized users will be granted access.' A blue banner below the warning message reads: 'You have 10 minutes to complete the Security Questions before the page times out.' Below the banner, a timer shows '09:47 Minutes Remaining.' The main section is titled 'Security Questions' and contains two questions. Question 1 asks about a mortgage loan opened in or around August 2010, with radio button options: ISLAND MORTGAGE, RUN BOOKLYN MTGE, SINGLE MORTGAGE, ONE HALF BANK, and NONE OF THE ABOVE/DOES NOT APPLY. Question 2 asks about a credit card opened, with radio button options: 2007, 2009, 2011, 2013, and NONE OF THE ABOVE. A red asterisk indicates required fields.

**New User Request - Verify Identity**

Progress: New User Request (Completed), Step 1 Verify Identity (Completed), Step 2 Security Questions (Active), Step 3 Finished

The information below is required to grant access to secure areas of the CCW environment. Only authorized users will be granted access.

⚠️ You have 10 minutes to complete the Security Questions before the page times out.

09:47 Minutes Remaining.

### Security Questions

\* indicates required fields

1. You may have opened a mortgage loan in or around August 2010. Please select the lender to whom you currently make your mortgage payments. If you do not have a mortgage, select 'NONE OF THE ABOVE/DOES NOT APPLY'. \*

- ISLAND MORTGAGE
- RUN BOOKLYN MTGE
- SINGLE MORTGAGE
- ONE HALF BANK
- NONE OF THE ABOVE/DOES NOT APPLY

2. You may have opened a (TEST/TEST-BKCARD) credit card. Please select the year in which your account was opened. \*

- 2007
- 2009
- 2011
- 2013
- NONE OF THE ABOVE

# Access Request Process Steps: Step 10a

---

- Once identity is confirmed, the request immediately continues for CCW approvals

## New User Request - Confirmation

Thank You!

Your CCW Access Request has been submitted for review and approval. You will receive email messages at the provided address with updates on your request as it is processed. Please refer to these email messages for next steps.

Prior to approval of access to CCW, you will receive an automated email from CCW Help. Please check your spam/junk mail folder for email notifications from [ccwhelp@gdlt.com](mailto:ccwhelp@gdlt.com). Internal security systems within some organizations may direct this email to your spam/junk email folder. Please review the information for accuracy.

# Access Request Process Steps: Step 10a (con't)

---

- You will receive an email confirming the successful submission of your registration request

Hello John,

You have successfully submitted your registration request to the Chronic Condition Data Warehouse (CCW). Your request will be reviewed by the initiator who invited you to access CCW. If revisions are required you will receive additional communications. The initiator will also setup your program access.

Sincerely,  
The CCW Team

## Access Request Process Steps: Step 10b

---

- If you are not identified through Experian you will receive information from CCW Help to proceed with manual identity proofing



# Access Request Process Steps: Step 11

---

- Once approved, CCW Help will create your CCW User ID and send you instructions for logging in to the CCW VRDC

**From:** [CCWHelp@gdit.com](mailto:CCWHelp@gdit.com) [mailto:CCWHelp@gdit.com]

**Sent:** Wednesday, February 05, 2014 1:25 PM

**To:** Doe, Jane Q

**Subject:** New CCW Account Information

A new account has been created for you in the CCW production environment with the following details. You will be required to change your password at the next login. Please review the [CCW Access - User First Login and Next Steps](#) document for instructional guidance. You may also go directly to the [Login Page](#) to complete the registration process.

# Preparing for First Time Log In

---

- Prerequisites for first time log in
  - Your CCW account registration must be complete
  - CARS, via CCW Help, has provided you, via email, with your CCW User ID and password
- Within 5 business days of completing the CARS process you will receive an invitation to an online **Security Awareness Training (SAT)**
- The invitation will be sent via email from CCW Help and will include a link to the SAT
- Upon successful completion of the SAT, you will need to submit your SAT Certification via email to [CCWHelp@GDIT.com](mailto:CCWHelp@GDIT.com)

# Preparing for First Time Log In (con't)

---

- Within 5 business days of submitting your SAT Certification, you will receive a “First Login” email from CCW Help
- This email will provide:
  - Your **CCW User ID** and a temporary password (which you will later change)
  - A Link to the **CCW First Login and User Next Steps guide**, which contains instructions for completing three important steps:
    - Downloading a Symantec VIP token for **Multifactor Authentication (MFA)**;
    - Registering your Symantec VIP token
    - Logging in to the CCW SFTS for the first time

# Multi-Factor Authentication

---

- Multi-Factor authentication is required, which includes user ID, password and “soft” random number security code (“credential”)
  - User ID and Password provided by CCW Help
  - “Soft” credential provided via VIP App for desktop or mobile device
- Download Symantec VIP App before starting the log in process



# Downloading the Symantec VIP App

- To download the Symantec VIP token navigate to:  
<https://idprotect.vip.symantec.com/desktop/download.v>



The screenshot shows the Symantec Validation & ID Protection Center website. The header includes the Symantec logo and the text "VALIDATION & ID PROTECTION CENTER". Below the header is a navigation bar with "Home", "Learn More", and "Where to Use" links. The main content area is titled "Protect Your Online Accounts with VIP Access Desktop".

There are two sections for downloading the app:

- VIP Access Desktop 2.2.1:** This section includes a screenshot of the app interface showing a Credential ID (VSST57144377) and a Security Code (723062). Below the screenshot is a yellow button labeled "Download for Windows" with a red arrow pointing to it. To the right of the button is a red arrow pointing to the left. Below the button is a note: "Important: You must have administrative permission to install VIP Access Desktop." and "System Requirements: Windows® XP Professional SP3 (32-bit only) or Windows® 7 SP1, Windows® 8 and 8.1 (native desktop mode only)".
- VIP Access Desktop 1.0.3:** This section includes a screenshot of the app interface showing a Credential ID (VSST57144377) and a Security Code (523876). Below the screenshot is a yellow button labeled "Download for Mac". To the right of the button is a note: "Important: You must have administrative permission to install VIP Access Desktop for Mac." and "System Requirements: Mac OS X 10.6 or higher".

- Select **Download for Windows**

## Downloading the Symantec VIP App (con't)

---

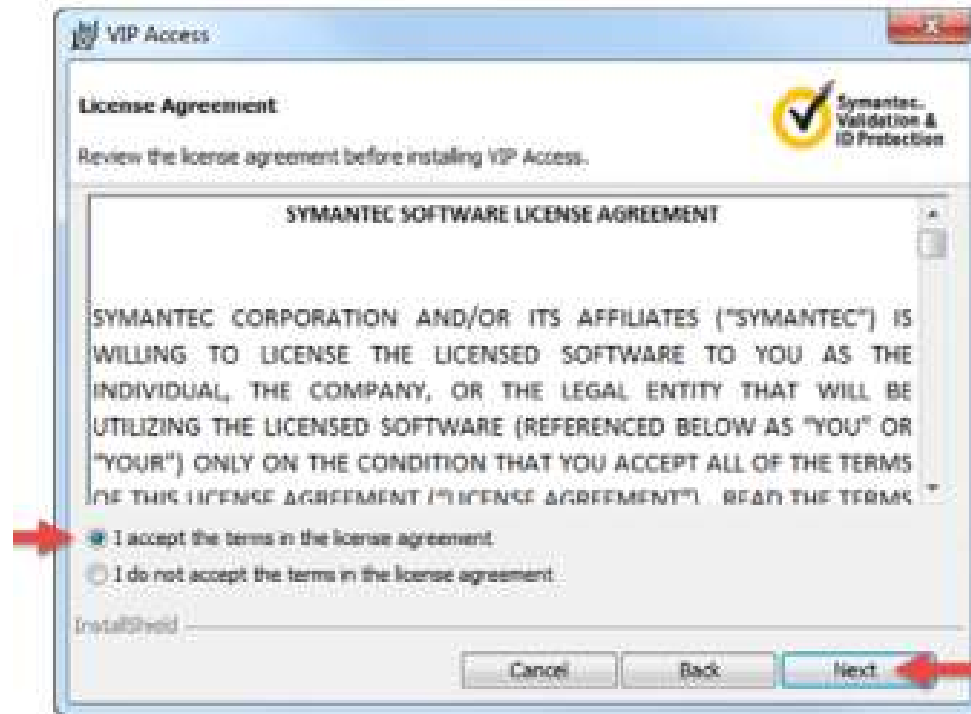
- The Download and Install VIP Access Desktop will begin



- Select **Run** from the pop-up window to continue with the installation

# Downloading the Symantec VIP App (con't)

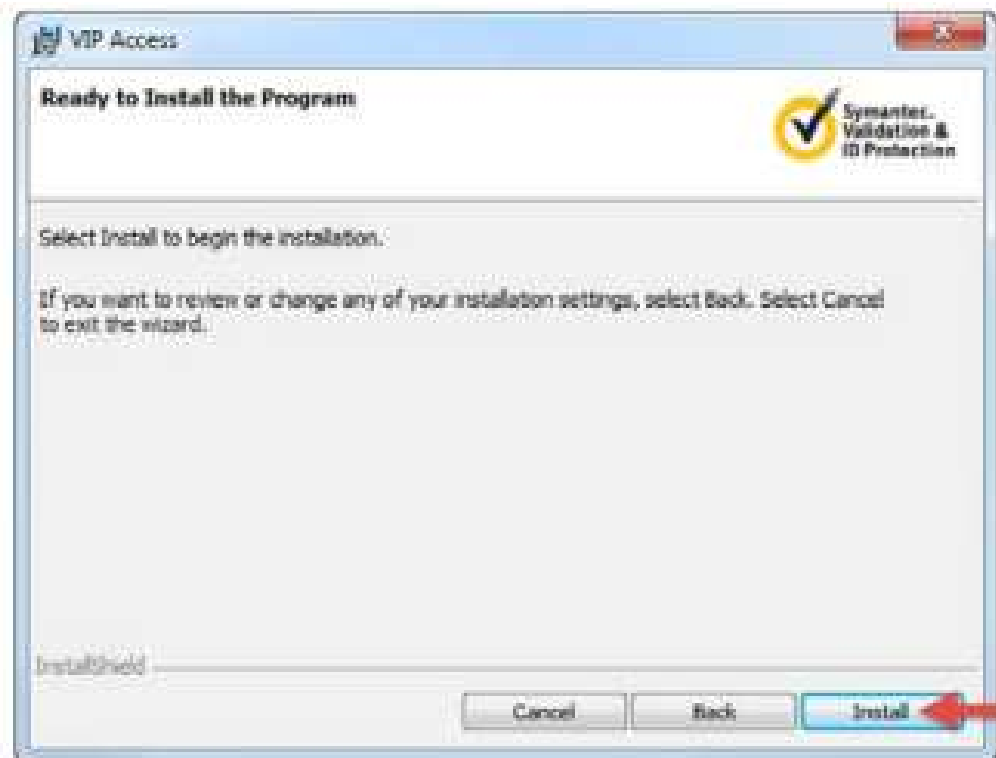
- The VIP Access Setup Wizard will open
- Select **Next**



- Review the License Agreement and select the “I accept the terms in the license agreement” radio button.
- Select **Next**

# Downloading the Symantec VIP App (con't)

- The Select Install Location window will open
- Select **Next**



- Then select **Install**

# Downloading the Symantec VIP App (con't)

---

- Allow the installation to complete



- Then select **Finish** to complete the installation

# Linking your Symantec Credential

- A VIP Access icon shortcut will appear on the user's desktop. Select the icon to open VIP Access
  - Your Credential ID is the number on top, it never changes
  - Enter your Credential ID and security code. Be sure to enter the security code within its 30 second window



# Linking your Symantec Credential (con't)

---

- To register a token navigate to: <https://www.ccwdata.org/vipssp>
- Enter CCW credentials in the User Name and Password fields
- Select **Sign In**

## Welcome to the Symantec® VIP Self Service Portal

To access the Self Service Portal, enter your user name and password, and click **Sign In**.

**Sign In**

User Name

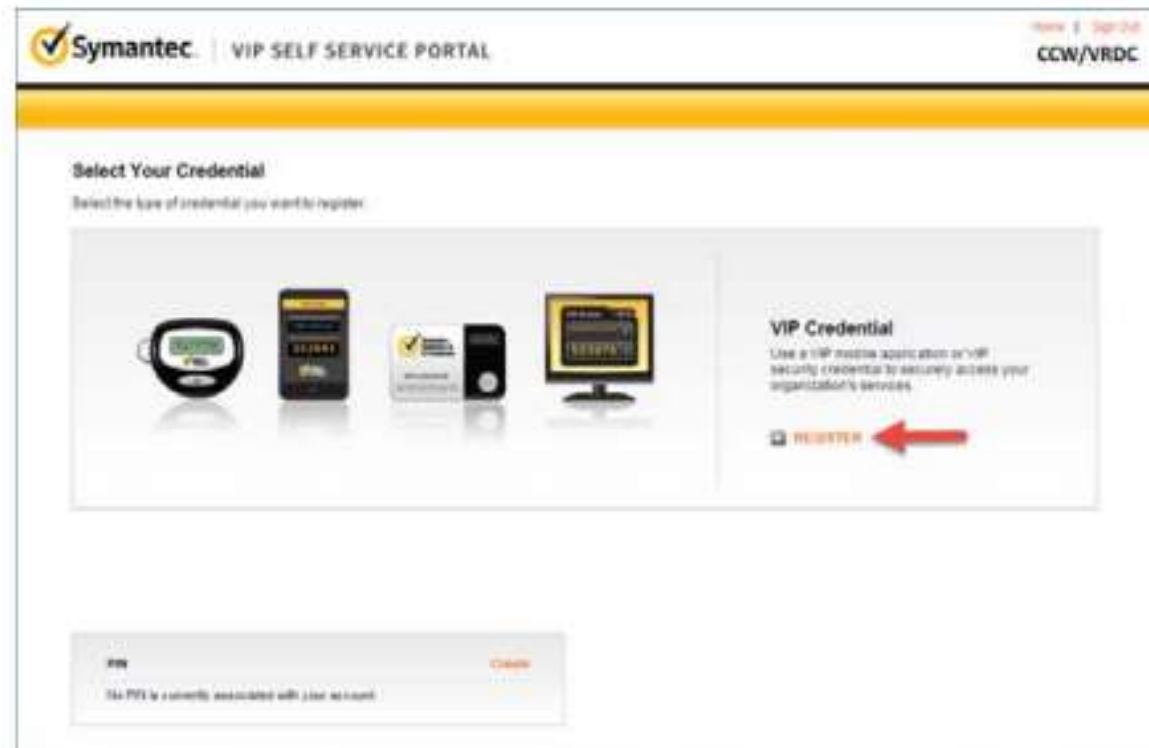
Password

Enabled by:  
 Symantec.  
Validation &  
ID Protection

**Sign In**

# Linking your Symantec Credential (con't)

- Select Register





# Linking your Symantec Credential (con't)

- Create a **Credential Name**
- Enter the **Credential ID** and **Security Code** from the previously downloaded token
  - Note that Security Code changes every 30 seconds

**Symantec** | VIP SELF SERVICE PORTAL Home | Sign Out  
CCW/VRDC

**Register Your Credential**

\* Required information

\*Credential Type: VIP Credential

\*Credential Name:  →

Enter a simple name that is easy to remember.

\*Credential ID:  →

What is a Credential ID?

**Credential ID examples:** Close  
Your credential contains a unique alphanumeric ID.

VIP Security Token (Back)	VIP Security Card (Front)	VIP Access

\*Security Code:  →

What is a Security Code?

**Security Code examples:** Close  
Your credential provides a dynamic 5-digit code that changes every 30 seconds.


VIP Security Token (Front)	VIP Security Card (Front)	VIP Access

→

- Select **Submit**

# Linking your Symantec Credential (con't)

- A green window will appear when registration is successful
- Create a PIN and Confirm the PIN
  - This PIN will be used every time you log into a Multi-Factor Authentication screen



The screenshot shows the Symantec VIP Self Service Portal. At the top left is the Symantec logo and the text "VIP SELF SERVICE PORTAL". At the top right are links for "Home" and "Sign Out" and the text "CCW/VRDC". A green message box states: "You have successfully registered JLU245. Enter a security code from this credential the next time you Sign in." Below this is the "Create Your PIN" section, which includes the instruction: "To help secure your account, you can create a PIN to use with a VIP security code when accessing your organization's services." The form contains two input fields: "PIN:" and "Confirm PIN:", each with a red arrow pointing to the right. Below the fields are two buttons: "Cancel" and "Create", with a red arrow pointing to the "Create" button.

- Select **Create**

# Linking your Symantec Credential (con't)

- A green window will appear when a PIN is successfully created

The screenshot shows the Symantec VIP Self Service Portal interface. At the top, the Symantec logo and 'VIP SELF SERVICE PORTAL' are visible on the left, and user information '(TST411) Home | Sign Out' and 'CCW/VRDC' are on the right. A green notification box at the top left contains a checkmark and the text 'You have successfully created your PIN.' Below this is the 'Manage Your Credentials' section, which includes a sub-header and a brief description: 'This VIP Self Service Portal enables you to register, test, or reset credentials. You can also remove credentials from your account.' The main content area is divided into two sections: 'Your Registered Credentials' and 'Your Registered Devices'. The 'Your Registered Credentials' section features a table with one entry and a 'Register' button. The table has columns for Credential Name, Credential ID, Type, State, and Actions. The entry shows 'JLU245' as the name, 'VSS751244726' as the ID, 'VIP Credential' as the type, and 'Enabled' as the state. The 'Your Registered Devices' section includes a warning icon and text: 'Only 20 remembered devices can be registered to your account at any one time. Contact your administrator to remove a currently-remembered device.' Below this is a table with columns for Device Name, Credential ID, Type, State, and Actions, which is currently empty with the message 'No devices are currently registered with this account.' At the bottom, there is a 'PIN' section with a 'Change' button and the text 'You can change your current PIN.'

# Future Visits: Logging into the MDAPM Portal on the CCW VRDC

---

- Log in to the portal with your:
  - User ID
  - password
  - Symantec VIP Access security code (changes every 30 seconds)
- Users must change their CCW password every 60 days to remain active

# Downloading Your Medicare Data

---

- Users will receive an email notice when new data is available
  - Data will be updated every 30 days
  - The email notification will include a link to the CCW SFTS at <https://sfts.ccwdata.org/> as well as a link to the **CCW SFTS User Guide**
- Once in your hospital's download folder
  - Select the file for download
  - Save data to local drive
- Delete older files on User systems
- Log out after downloading your Medicare data

# One Week Test Period

---

- Thursday, 3/30 – Monday, 4/10
- Hospitals can access Axway accounts and download test files
- One Zip file containing
  - one SAS file, and
  - one CSV file
- No actual data contained in test files

# Upcoming Webinars

---

- **Webinar 8: 9:00am EST, Monday, April 10th, 2017**
  - Purpose of this webinar will be to address questions and technical difficulties encountered during the one week test access period.

## QUESTIONS?

---

For all information regarding the Care Redesign Programs please visit: <http://www.hscrc.maryland.gov/care-redesign.cfm>

Please send any questions to: [hscrc.care-redesign@maryland.gov](mailto:hscrc.care-redesign@maryland.gov)

For questions related to CARS or AXWAY access, contact the CMS Helpdesk or [MarylandModel@cms.hhs.gov](mailto:MarylandModel@cms.hhs.gov)