LEWIN GROUP®

November 30, 2016

All-Payer Model Amendment and Care Redesign Programs

Comprehensive Medicare Data Process and Use

9:00-10:00 EST

Wednesday, November 30, 2016

Agenda

- Introductions
- Medicare Data Extracts
- Use of the MDAPM Exchange Portal
- Questions

INTRODUCTIONS

This session will cover

- What is in your Medicare data extracts
- How to access your Medicare data
  - 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
- Eleven (11) 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 day of the Reporting Month
  - E.g., July extracts contain data up through June 30
- 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 D File
Part A Revenue Center Detail	Beneficiary Demographics File
Part A Procedure Codes File	Beneficiary XREF File
Part A Diagnosis Codes File	Summary Statistics Header Record
Part B Physicians File	Summary Statistics Detail Records
Part B DME File	

- All data files available in both SAS and Comma Separated Values (CSV) formats

- Additional supplemental files include the technical specifications and 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
- 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, HICN, 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, along with their associated start/end dates
    - 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 stable 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 and Details Files 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

- Coding of geographic variables
  - MD Hospital Extracts use Social Security Administration taxonomy
  - ACO Extracts use Federal Information Processing Standard (FIPS) codes

- Variables excluded from MD Hospital extracts
  - Claim Adjustment Type code
  - Claim Provider Type code

- 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

Preparing for First Time Log In

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

Preparing for First Time Log In

- Prerequisites for first time log in
  - Your CCW account registration must be complete
  - **CCW Access Request System (CARS)**, via CCW Help, has provided you, via email, with your CCW User ID and password

- Within 5 business days of completing the account registration 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

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

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

Upcoming Webinars

- Webinar 6: 9:00am EST, Friday, January 13, 2017
  - Care Partner Agreements
- Webinar 7: 9:00am EST, Friday, February 3, 2017
  - Care Redesign Program Monitoring

The FAQ on the CCIP and HCIP are now posted on the HSCRC website:

http://www.hscrc.state.md.us/care-redesign.cfm

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

APPENDIX

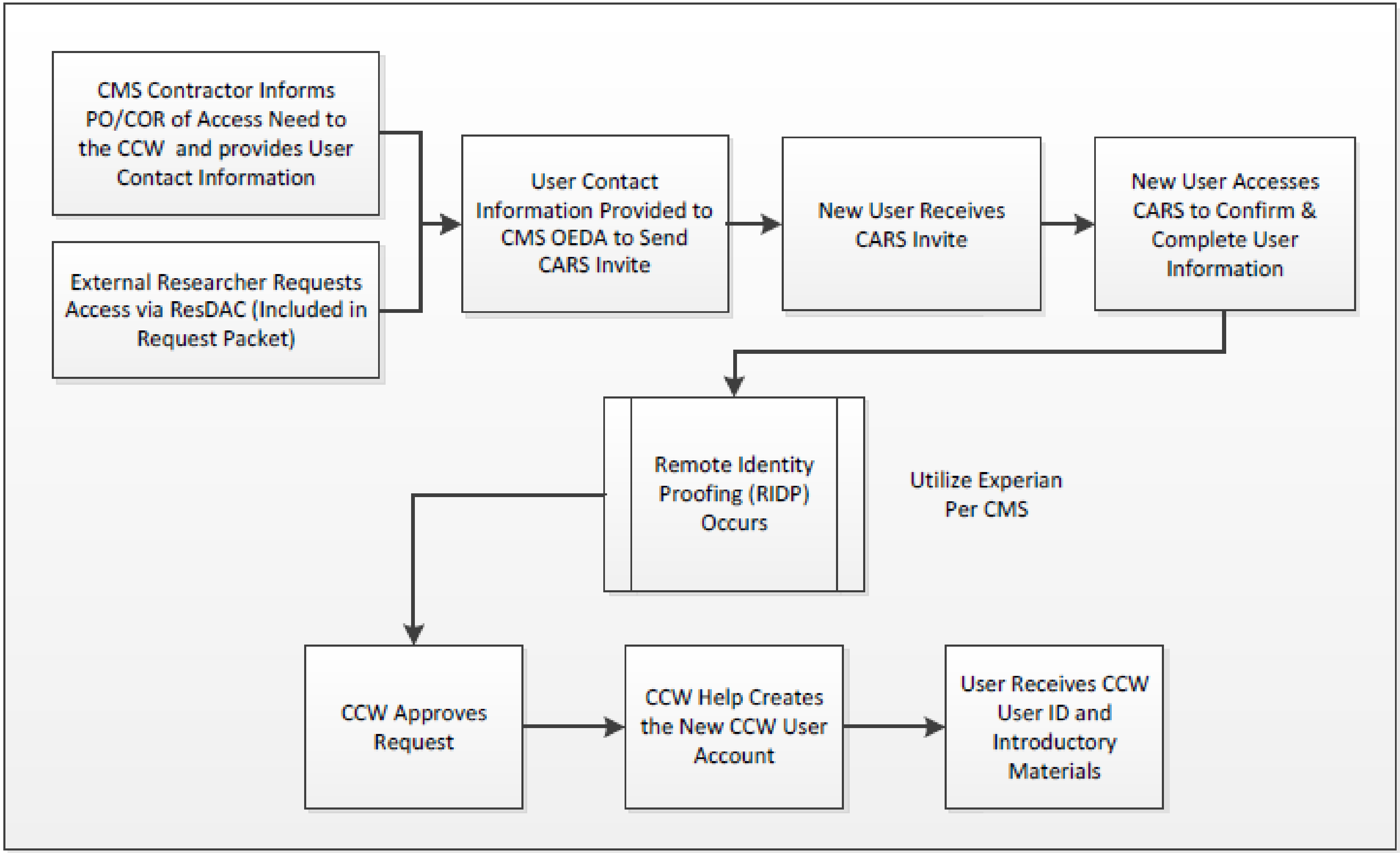
New User Access Request Process Flow

Access Request Process Steps

Downloading the Symantec VIP App

Linking your Symantec Credential

New User Access Request Process Flow



CMS Contractor Informs PO/COR of Access Need to the CCW and provides User Contact Information

External Researcher Requests Access via ResDAC (Included in Request Packet)

User Contact Information Provided to CMS OEDA to Send CARS Invite

New User Receives CARS Invite

New User Accesses CARS to Confirm & Complete User Information

Remote Identity Proofing (RIDP) Occurs

Utilize Experian Per CMS

CCW Approves Request

CCW Help Creates the New CCW User Account

User Receives CCW User ID and Introductory Materials

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
    - Contact The Lewin Group 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

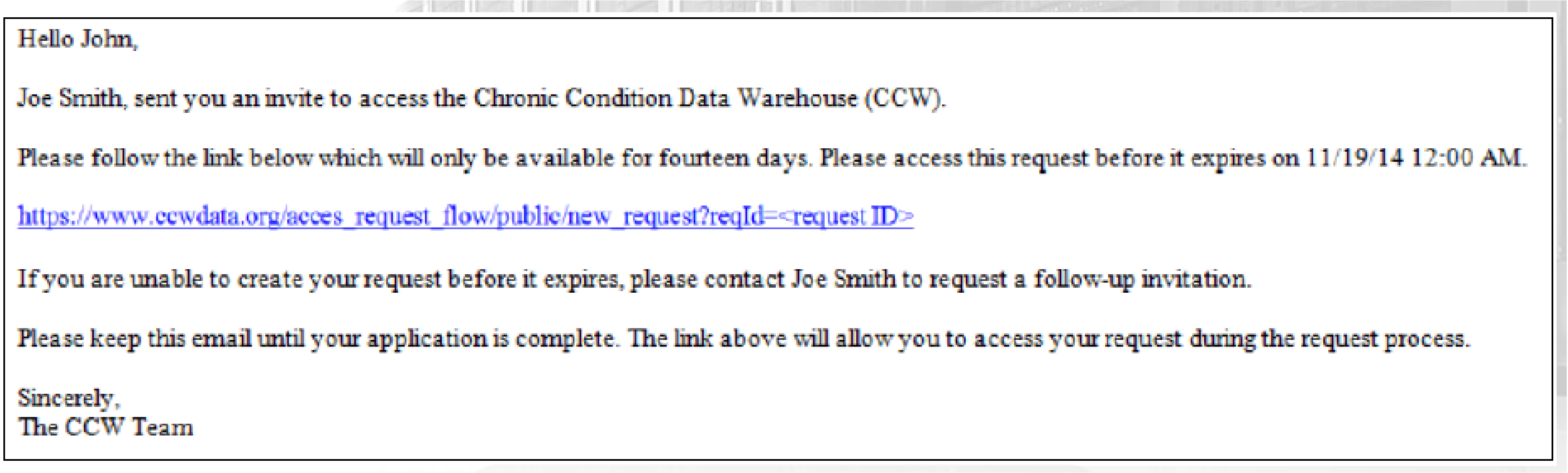
Access Request Process Steps: Step 2

- The Lewin Group will compile your hospital's user contact information
  - First Name
  - Last Name
  - Unique Business Email
  - User's Hospital

- 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>

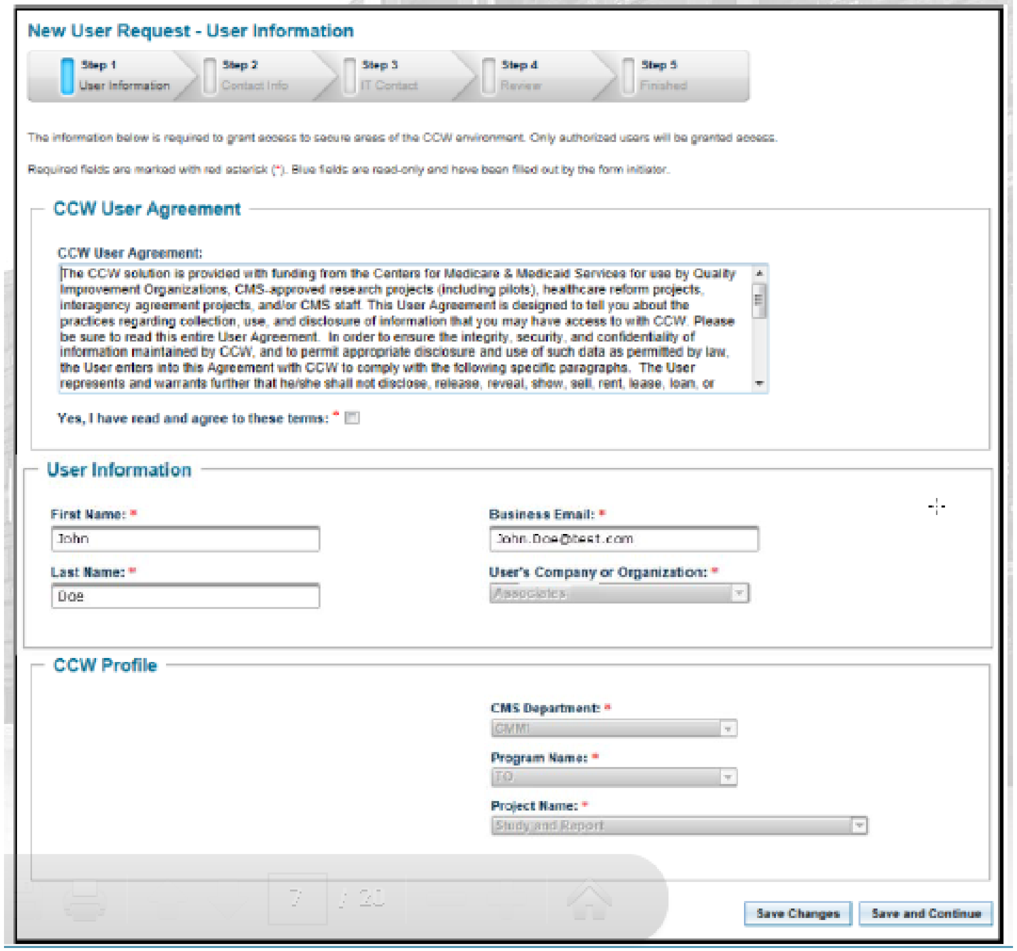
If you are unable to create your request before it expires, please contact Joe Smith to request a follow-up invitation.

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

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@test.com

User's Company or Organization: * Associates

CCW Profile

CMS Department: * CMMI

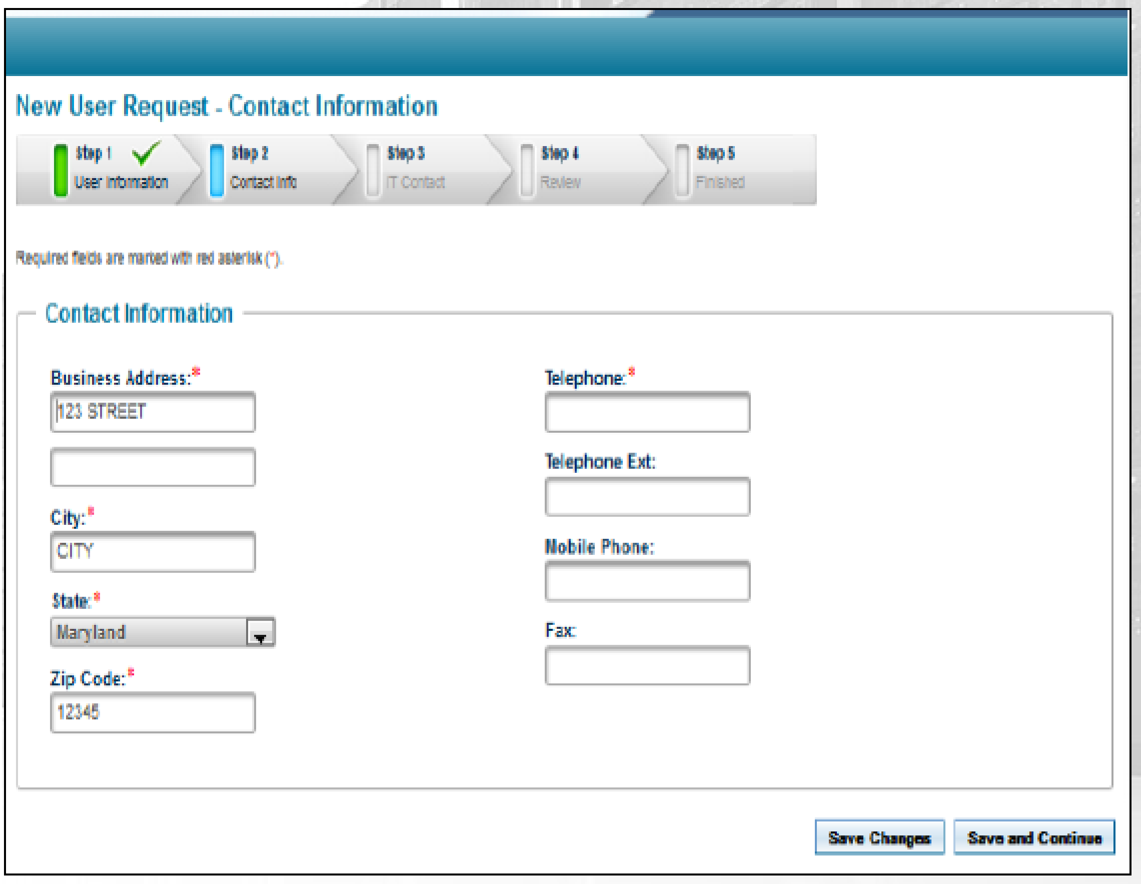
Program Name: * TO

Project Name: * Study and Report

- 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

Required fields are marked with red asterisk (*).

Contact Information

Business Address:* 123 STREET

City:* CITY

State:* Maryland

Zip Code:* 12345

Telephone:*

Telephone Ext:

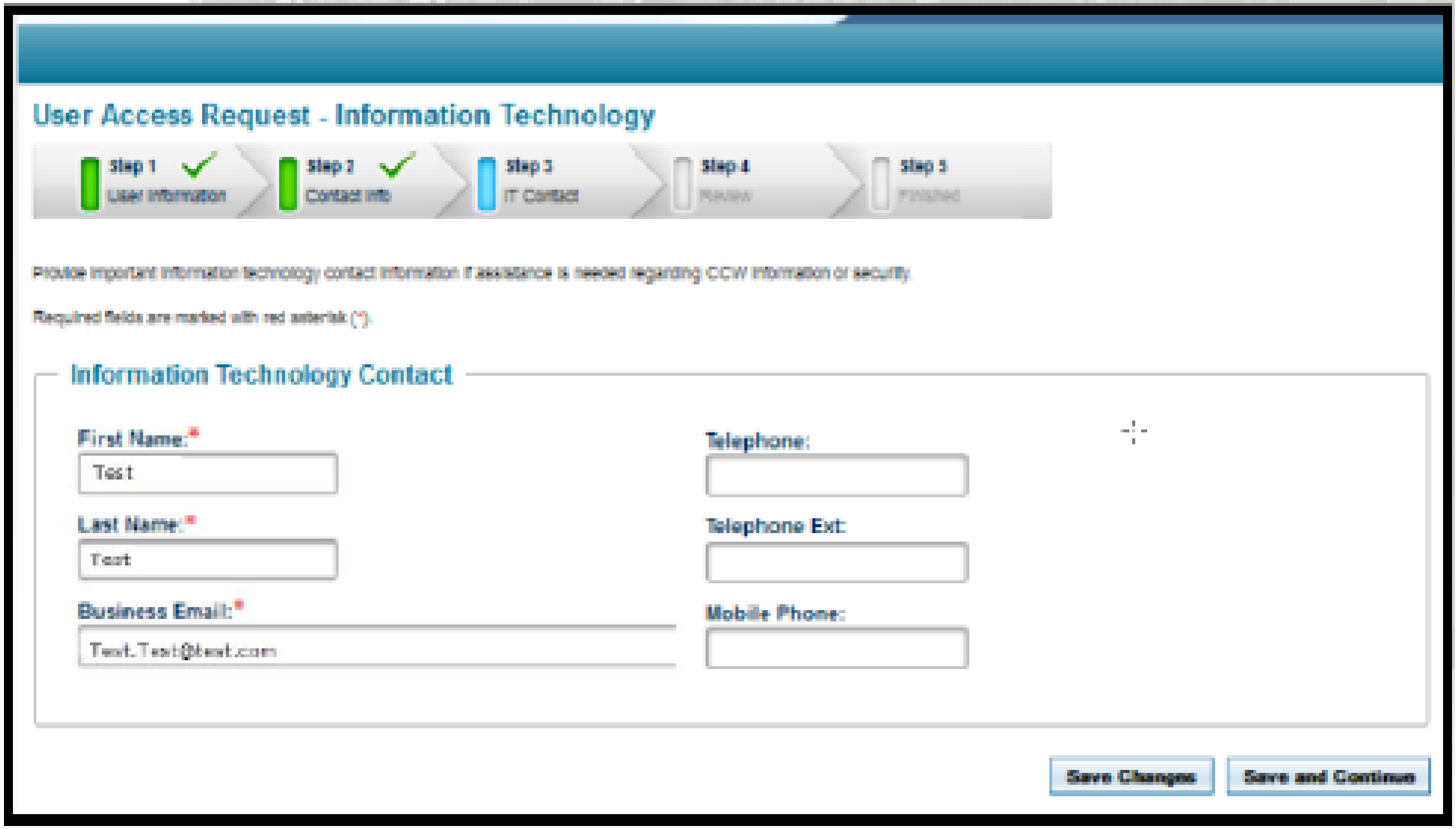
Mobile Phone:

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



User Access Request - Information Technology

Provide important information technology contact information if assistance is needed regarding CCW information or security.

Required fields are marked with red asterisk (*).

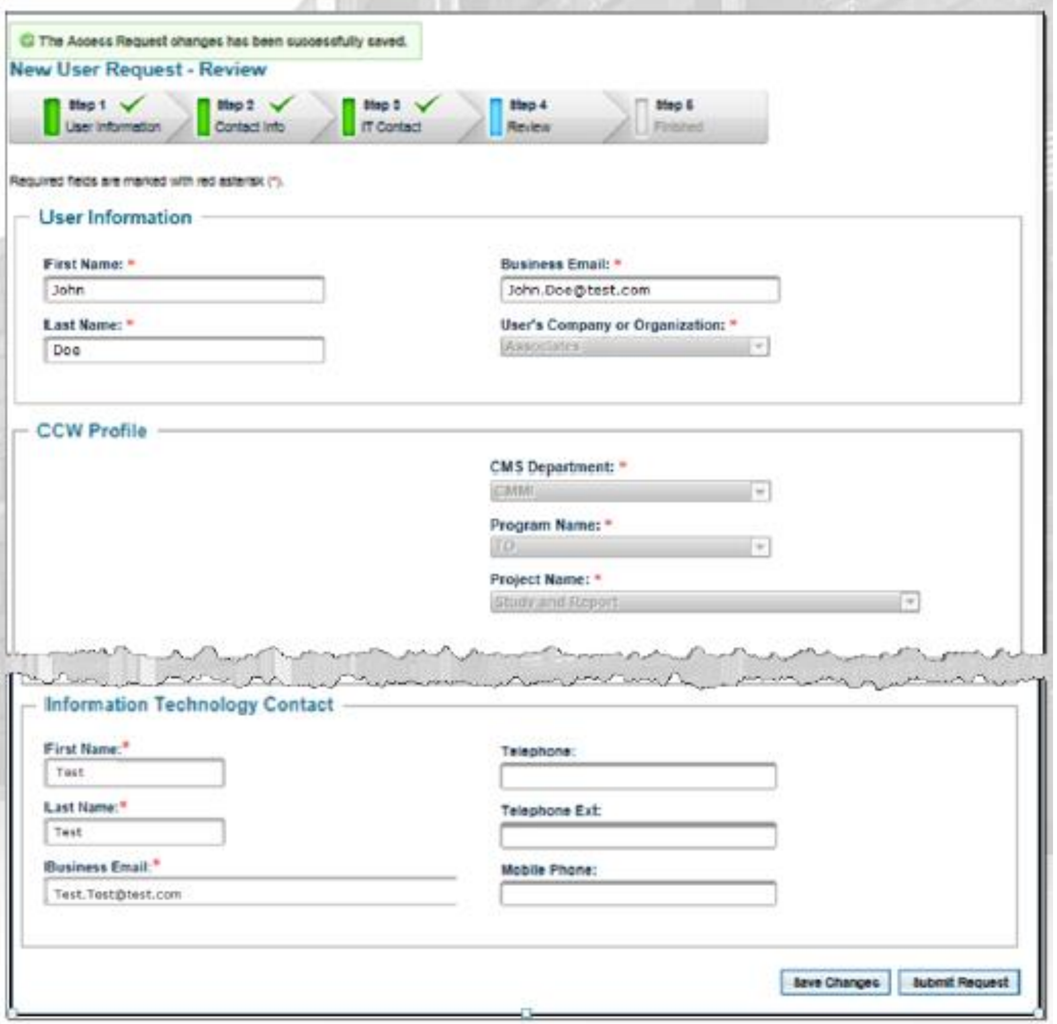
Information Technology Contact

First Name:* Test	Telephone:
Last Name:* Test	Telephone Ext:
Business Email:* Test.Test@test.com	Mobile Phone:

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

Access Request Process Steps: Step 7

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



The Access Request changes has been successfully saved.

New User Request - Review

Required fields are marked with red asterisk (*).

User Information

First Name: * John

Last Name: * Doe

Business Email: * John.Doe@test.com

User's Company or Organization: * Associates

CCW Profile

CMS Department: * CMMI

Program Name: * TO

Project Name: * Study and Report

Information Technology Contact

First Name:* Test

Last Name:* Test

Business Email:* Test.Test@test.com

Telephone:

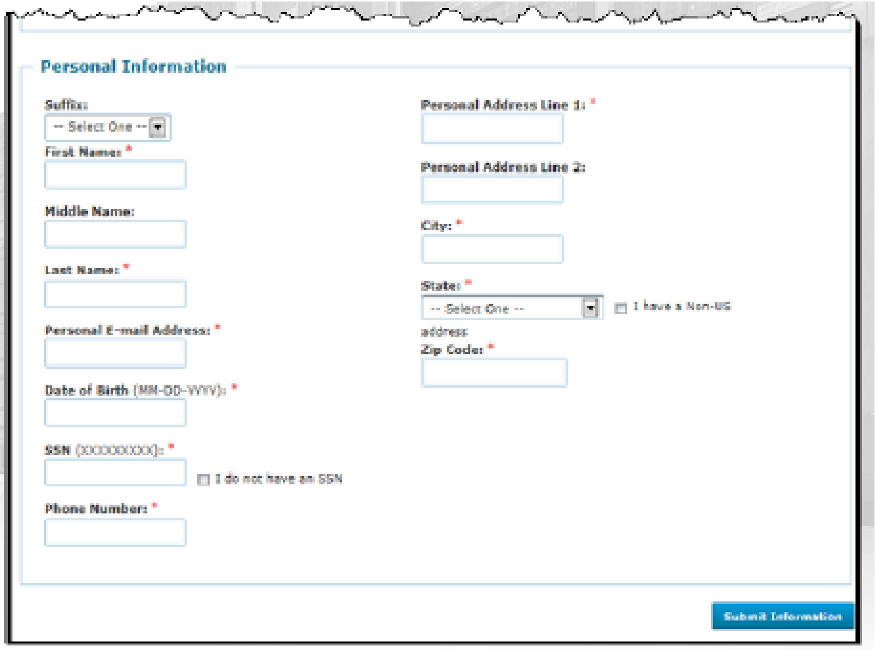
Telephone Ext:

Mobile Phone:

- 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



Personal Information

Suffix:
-- Select One --

First Name: *

Middle Name:

Last Name: *

Personal E-mail Address: *

Date of Birth (MM-DD-YYYY): *

SSN (XXXXXXXXX): *

□ I do not have an SSN

Phone Number: *

Personal Address Line 1: *

Personal Address Line 2:

City: *

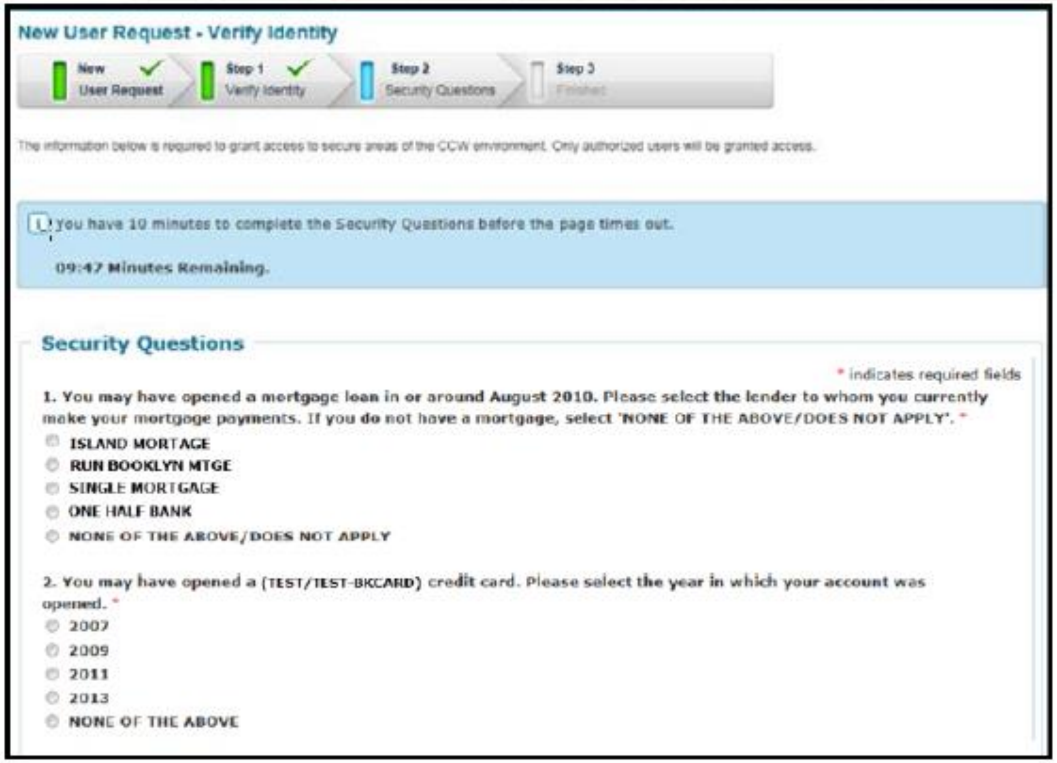
State: *
-- Select One --

□ I have a Non-US address

Zip Code: *

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



New User Request - Verify Identity

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'. *

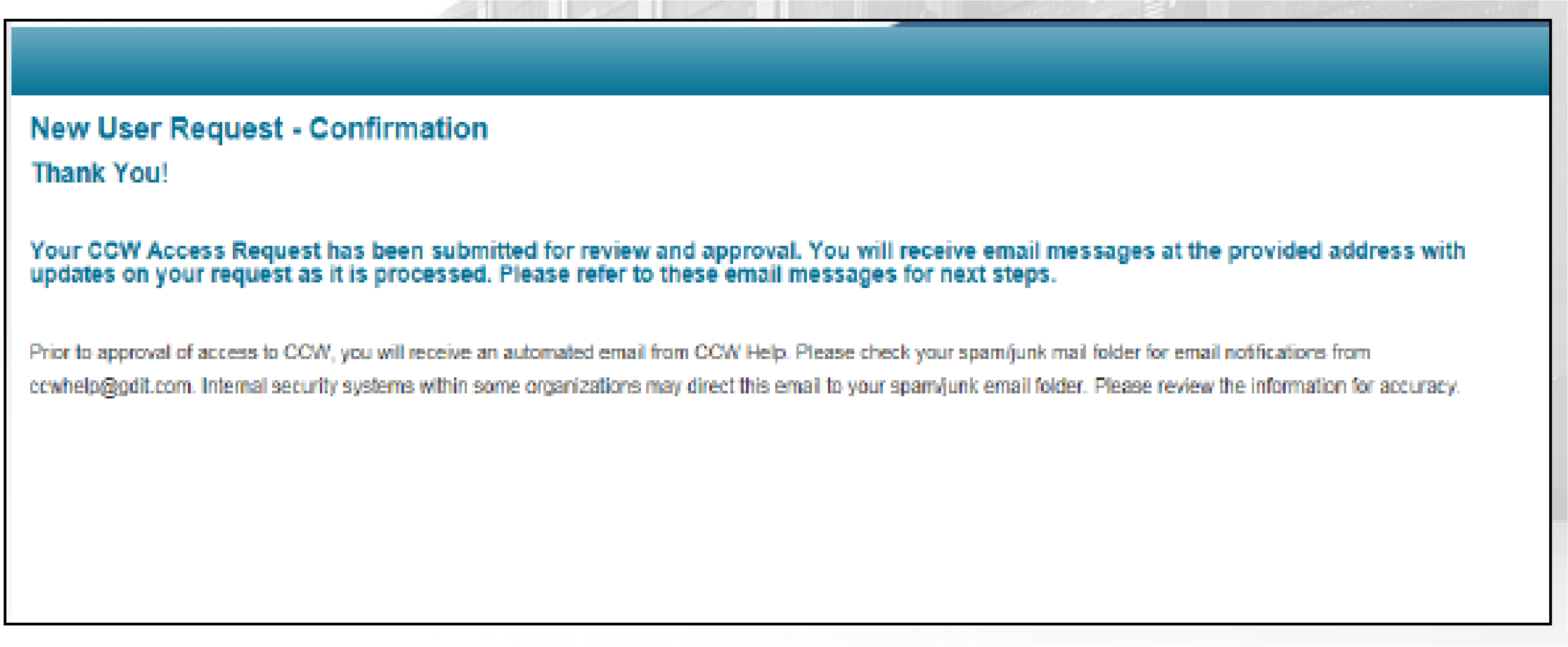
○ ISLAND MORTAGE
○ RUN BOOKLYN MTGE
○ SINGLE MORTGAGE
○ ONE HALF BANK
○ NONE OF THE ABOVE/DOES NOT APPLY

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

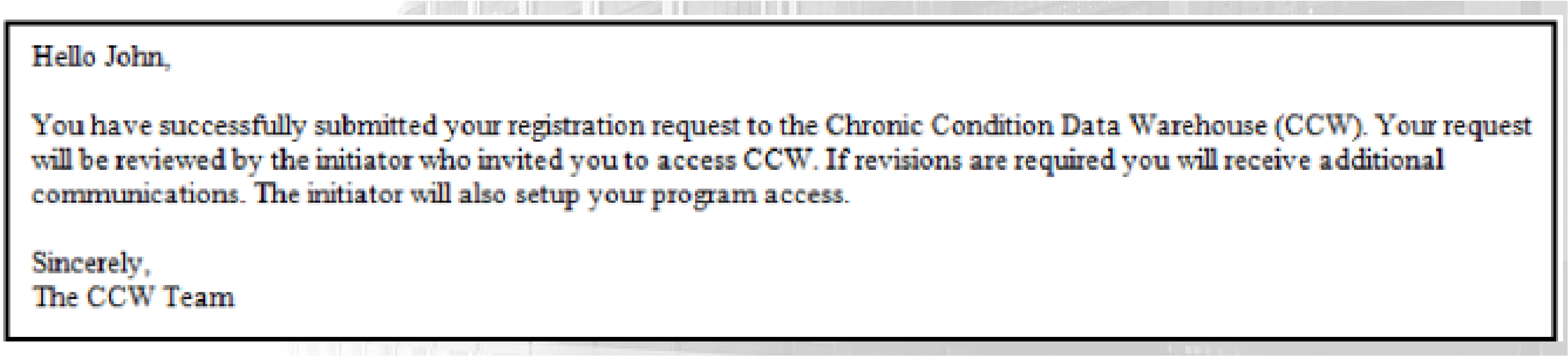
Thank You!

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@gdit.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.

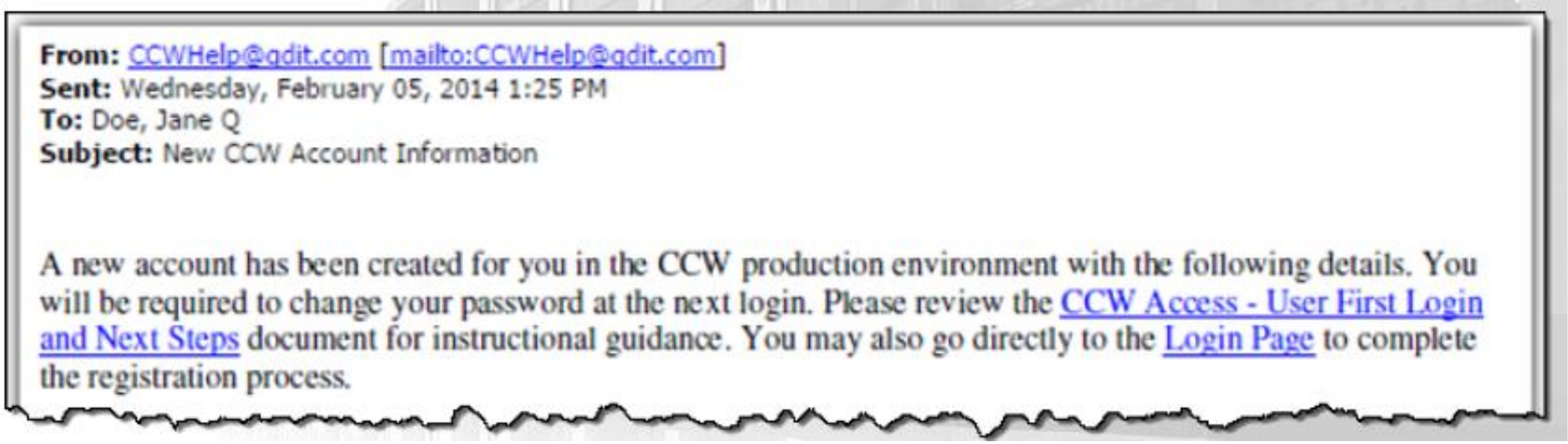
Sincerely,
The CCW Team

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

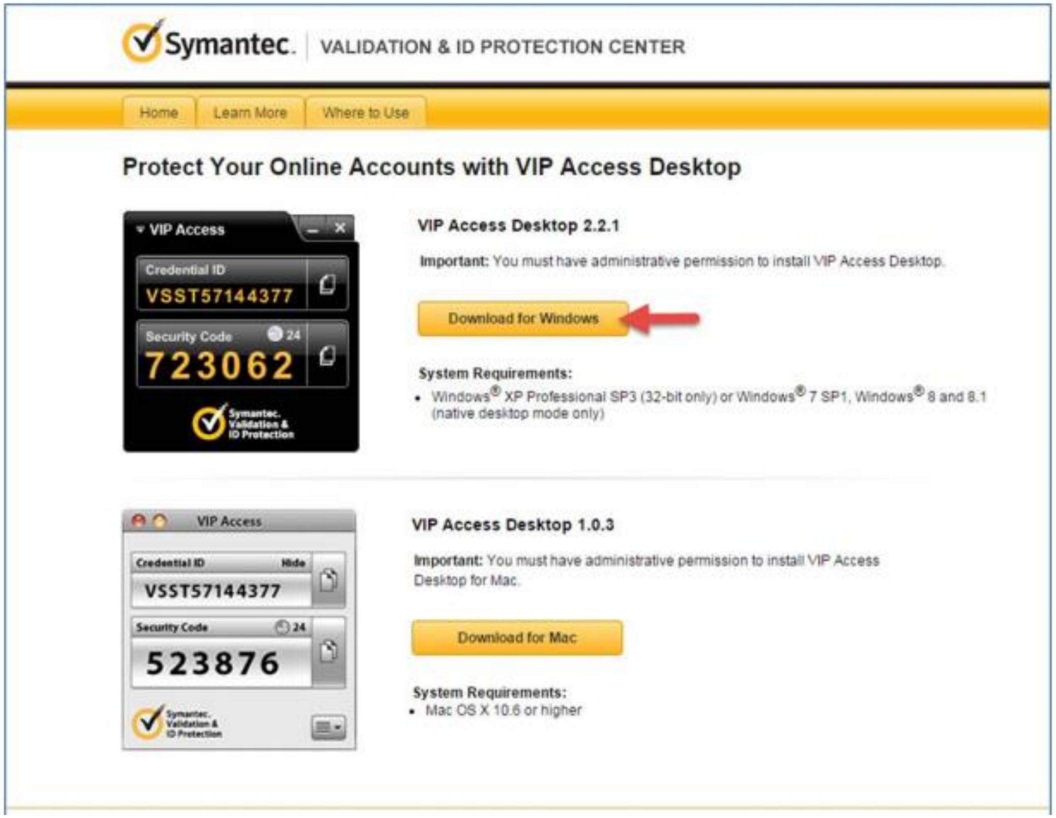


From: CCWHelp@gdit.com [mailto:CCWHelp@gdit.com]
Sent: Wednesday, February 05, 2014 1:25 PM
To: Doe, Jane Q
Subject: New CCW Account Information

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.

Downloading the Symantec VIP App

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



Protect Your Online Accounts with VIP Access Desktop

Credential ID: VSST57144377

Security Code: 723062

VIP Access Desktop 2.2.1

Important: You must have administrative permission to install VIP Access Desktop.

System Requirements:

- Windows® XP Professional SP3 (32-bit only) or Windows® 7 SP1, Windows® 8 and 8.1 (native desktop mode only)

Credential ID: VSST57144377

Security Code: 523876

VIP Access Desktop 1.0.3

Important: You must have administrative permission to install VIP Access Desktop for Mac.

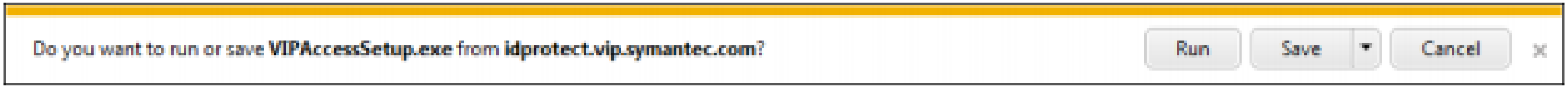
System Requirements:

- 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

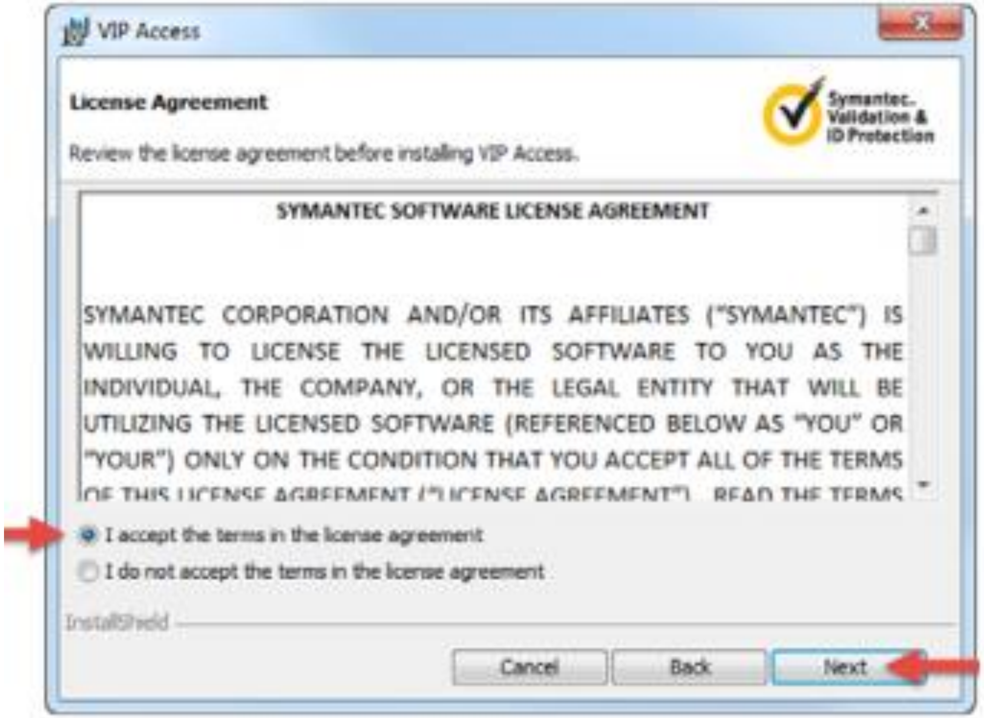


Do you want to run or save **VIPAccessSetup.exe** from **idprotect.vip.symantec.com**?

- 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**



License Agreement

Review the license agreement before installing VIP Access.

SYMANTEC SOFTWARE LICENSE AGREEMENT

SYMANTEC CORPORATION AND/OR ITS AFFILIATES ("SYMANTEC") IS WILLING TO LICENSE THE LICENSED SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE LICENSED SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT ("LICENSE AGREEMENT"). READ THE TERMS

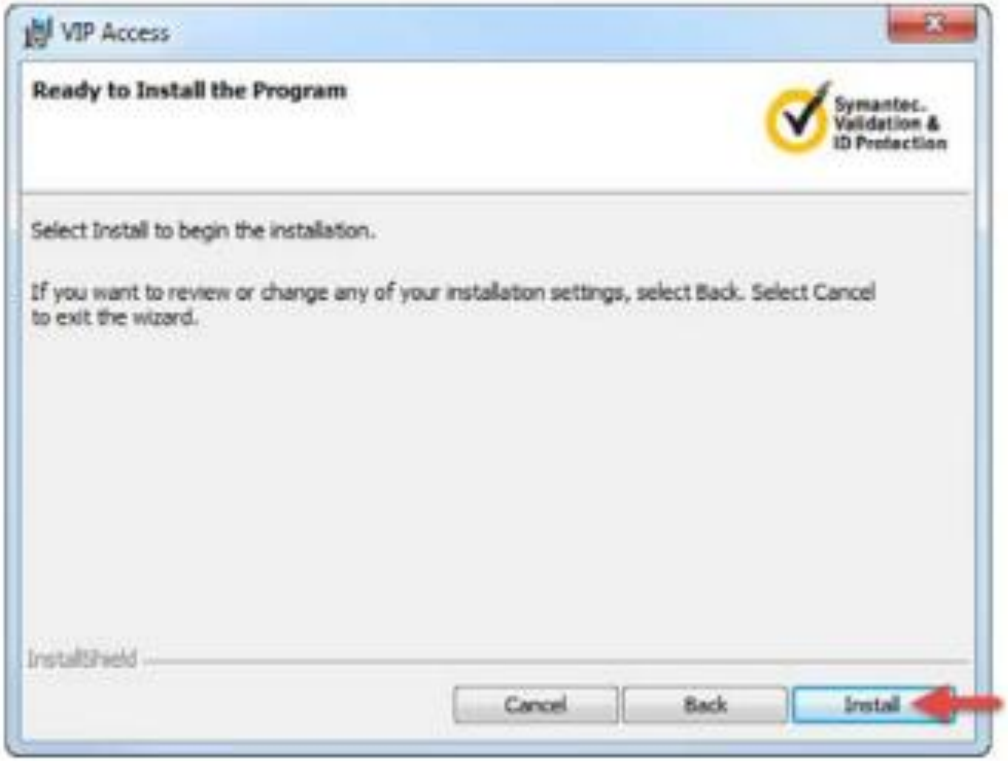
● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

- 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**



Ready to Install the Program

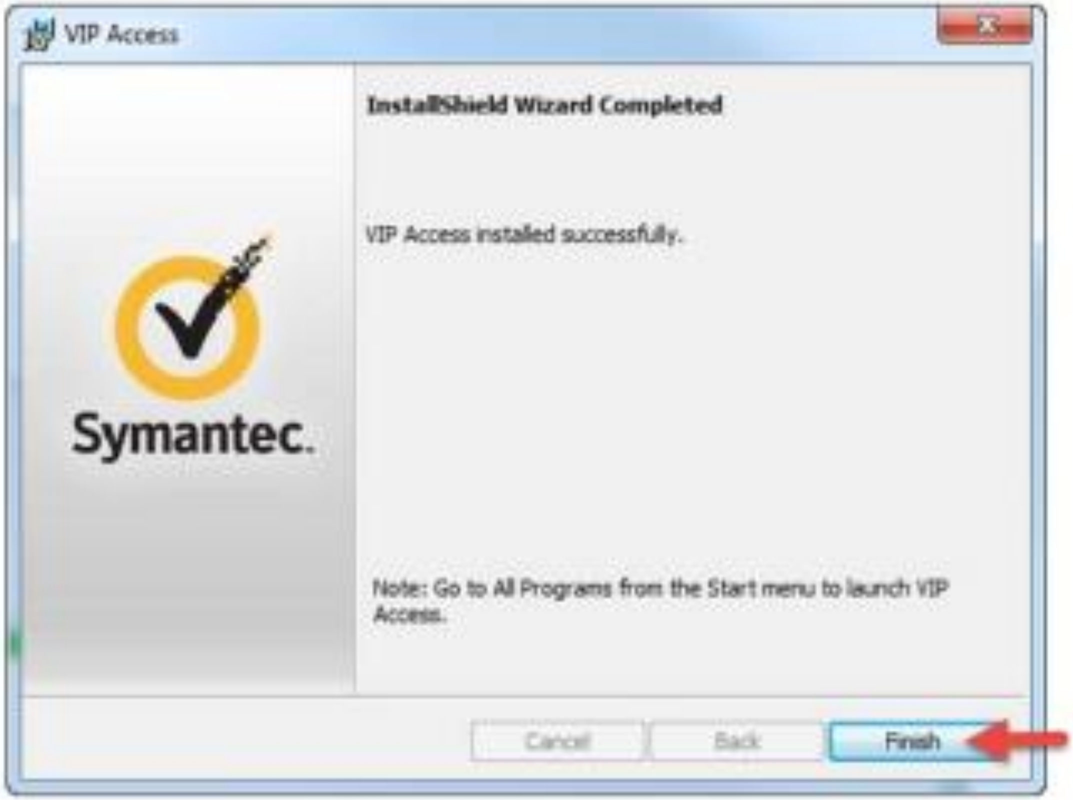
Select Install to begin the installation.

If you want to review or change any of your installation settings, select Back. Select Cancel to exit the wizard.

- Then select **Install**

Downloading the Symantec VIP App (con’t)

- Allow the installation to complete



VIP Access

InstallShield Wizard Completed

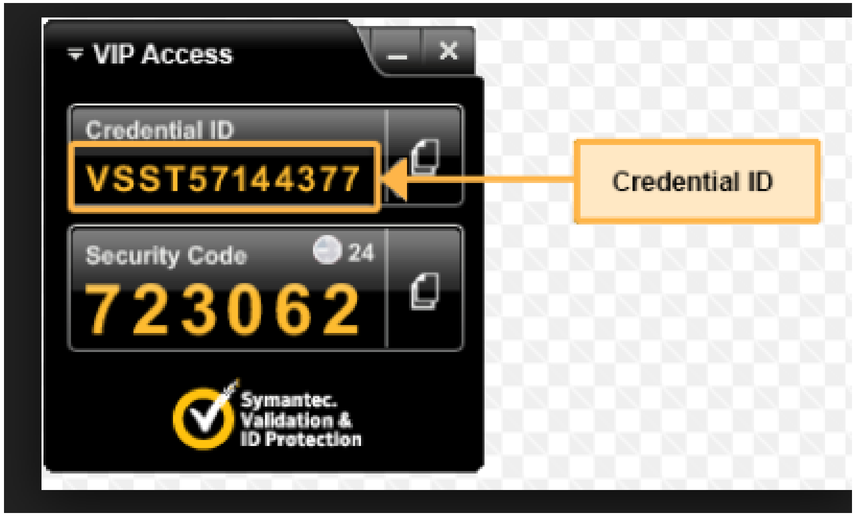
VIP Access installed successfully.

Note: Go to All Programs from the Start menu to launch VIP Access.

- 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

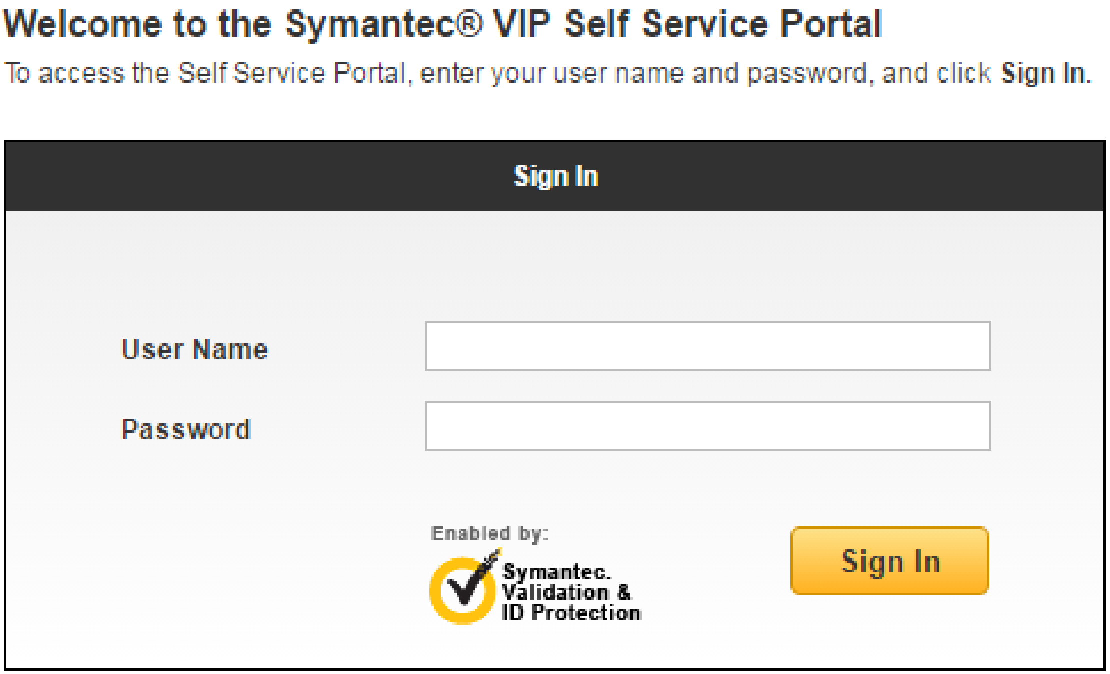


Credential ID: VSST57144377

Security Code: 723062

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**

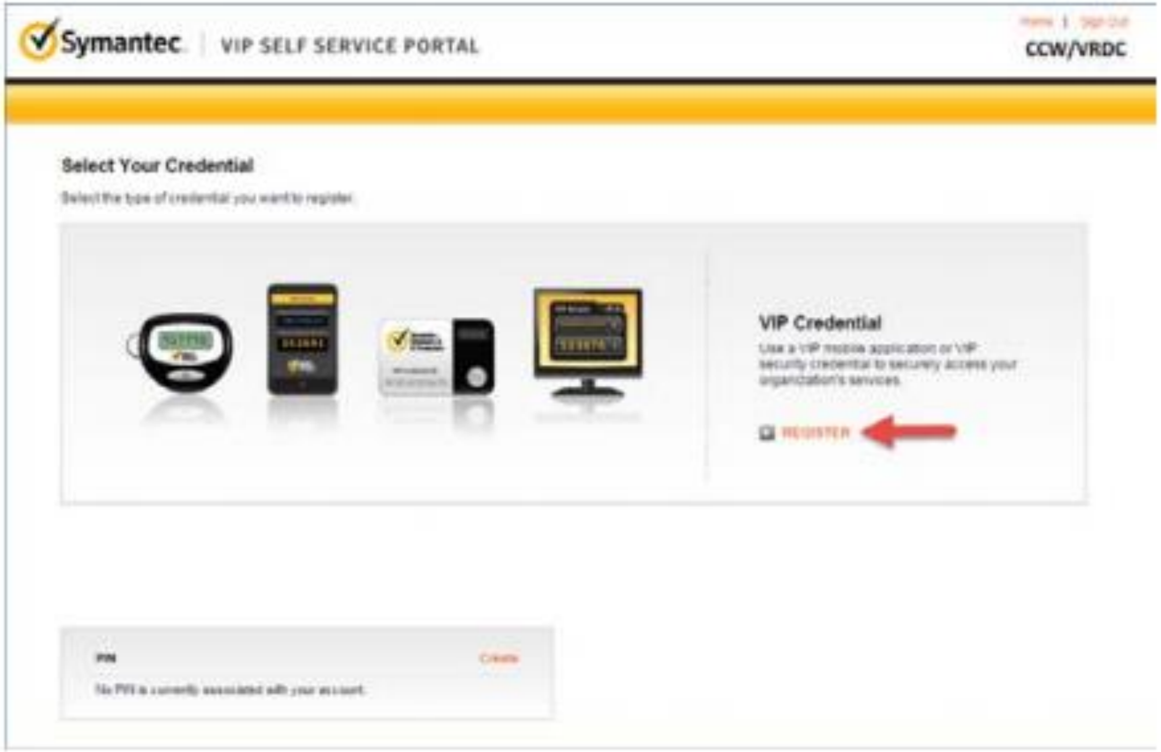


Welcome to the Symantec® VIP Self Service Portal

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

Linking your Symantec Credential (con’t)

- Select **Register**



Select Your Credential

Select the type of credential you want to register

VIP Credential

Use a VIP mobile application or VIP security credential to securely access your organization's services.

REGISTER

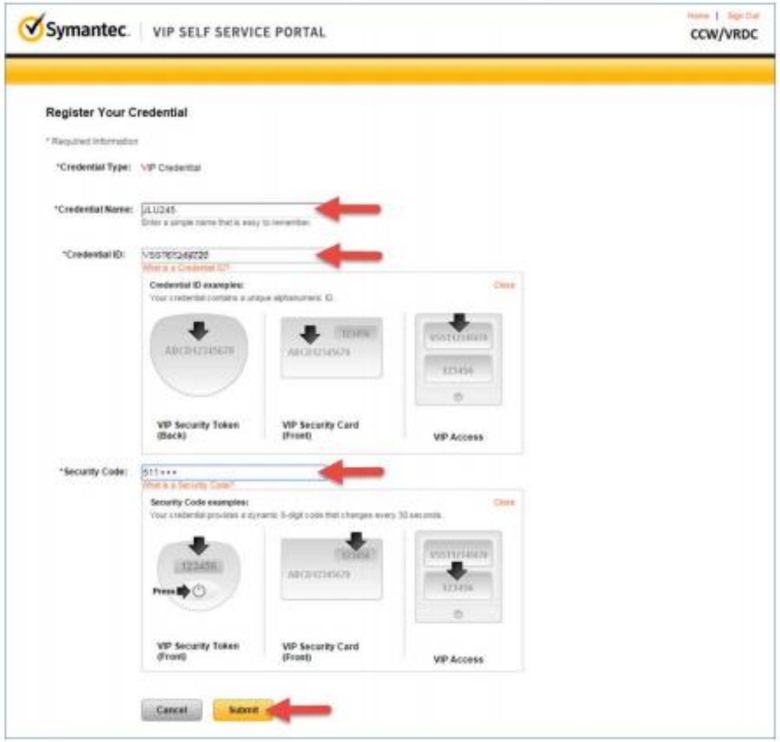
PIN

Create

No PIN is currently associated with your account.

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: JLU245

Enter a simple name that is easy to remember.

*Credential ID: VSST67248720

What is a Credential ID?

Credential ID examples:

Your credential contains a unique alphanumeric ID.

*Security Code: 511•••

What is a Security Code?

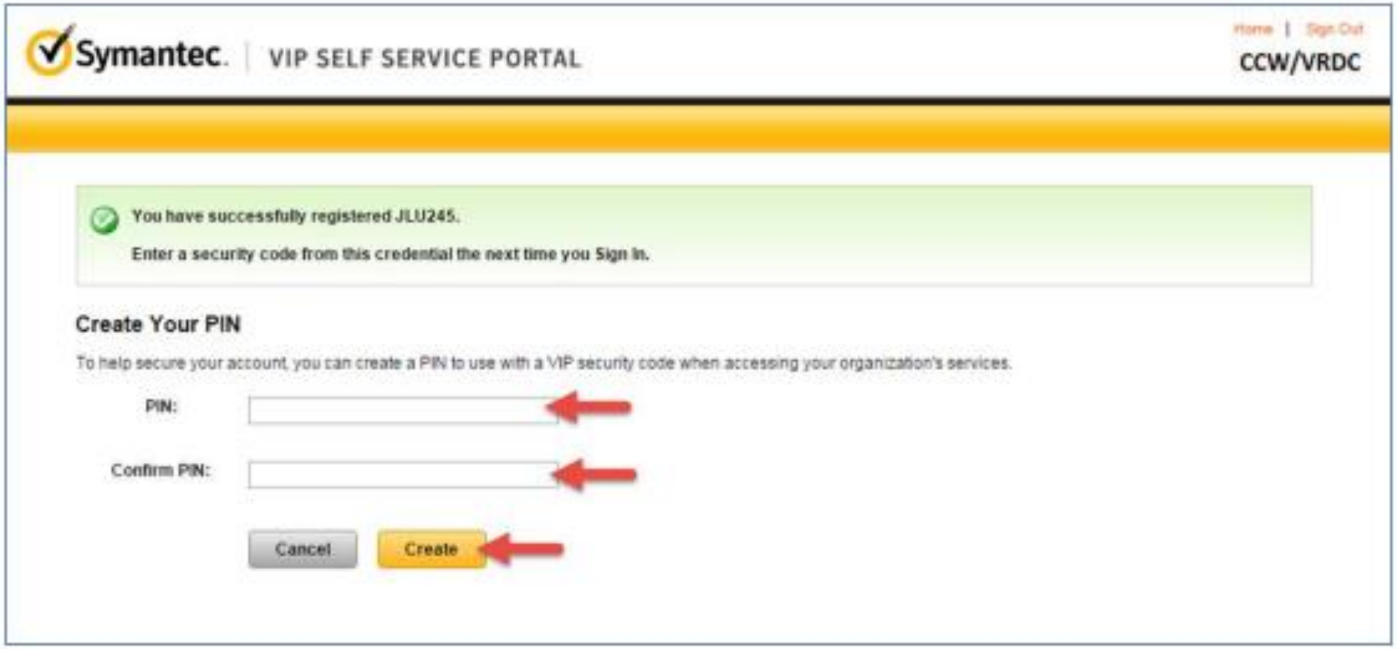
Security Code examples:

Your credential provides a dynamic 6-digit code that changes every 30 seconds.

- 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



You have successfully registered JLU245.

Enter a security code from this credential the next time you Sign In.

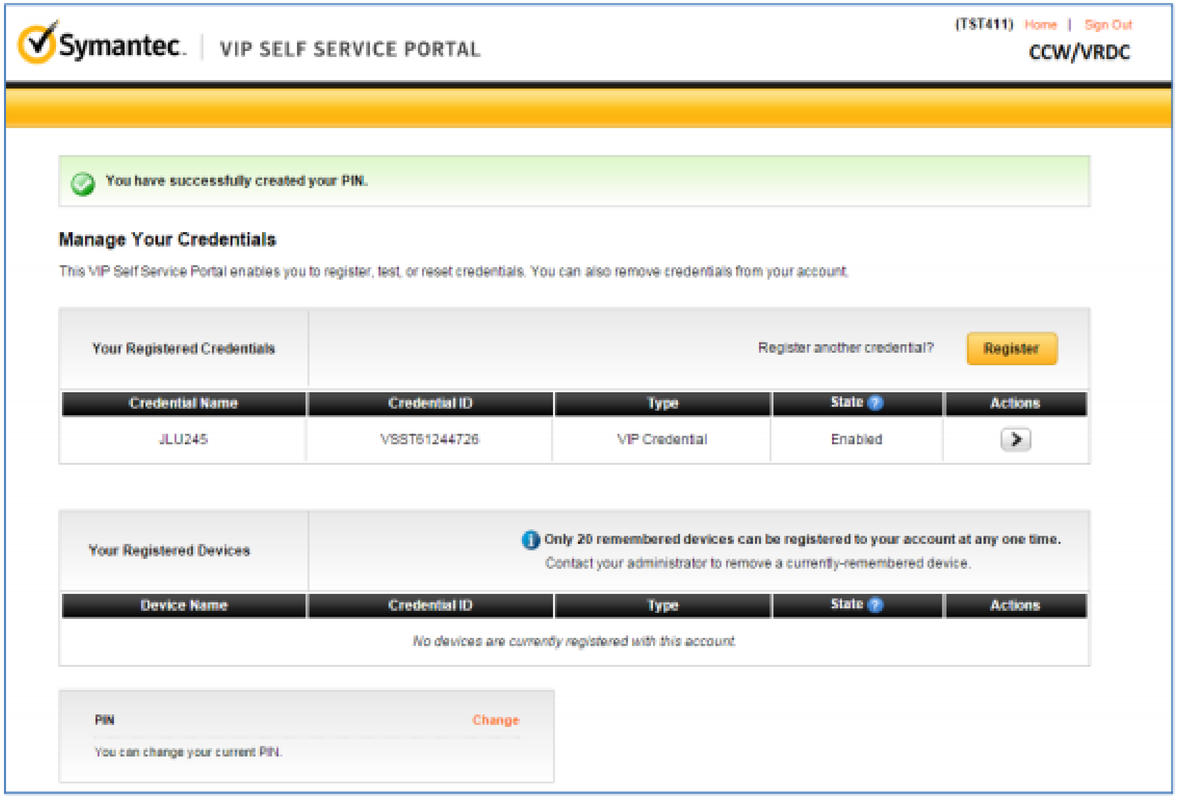
Create Your PIN

To help secure your account, you can create a PIN to use with a VIP security code when accessing your organization's services.

- Select **Create**

Linking your Symantec Credential (con't)

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



You have successfully created your PIN.

Manage Your Credentials

This VIP Self Service Portal enables you to register, test, or reset credentials. You can also remove credentials from your account.

Your Registered Credentials

Register another credential? Register

Credential Name	Credential ID	Type	State	Actions
JLU245	VSST61244726	VIP Credential	Enabled	>

Your Registered Devices

Only 20 remembered devices can be registered to your account at any one time.
Contact your administrator to remove a currently-remembered device.

Device Name	Credential ID	Type	State	Actions
No devices are currently registered with this account.				

PIN Change

You can change your current PIN.