File Submission

Preparation and Transfer of PNSS Files to CDC

Preparation and transfer of PNSS transaction or data files to CDC is a data processing staff function. Contributors may elect to have other staff persons manage either or both of these tasks, but assistance from data processing experts will likely be needed. Specifications for PNSS transaction files are outlined in the *PNSS User's Guide* chapter on record specifications.

One record per pregnancy is submitted to the PNSS, not one record per visit. A complete PNSS record (completion code =1, A or B) includes prenatal and postpartum data for a woman as well as data on her infant. A prenatal only record (completion code= 2-6), includes prenatal only data for a woman. A postpartum only record (completion code = 7-8) includes postpartum only data for a woman as well as data on her infant. The chapter on PNSS record specifications defines the fields to populate on complete, prenatal only, and postpartum only records and offers guidance on how to link data from multiple state records when assembling PNSS records.

In addition to preparing and transferring *transaction* files to CDC, contributors are also responsible for preparing and transferring up-to-date PNSS and PedNSS *code* files, defining codes for geographic entities, e.g. individual clinics and counties in their state. Instructions for maintaining and submitting the code file are outlined in the *PNSS User's Guide* chapter on the PNSS and PedNSS Code File.

Schedule

Submit PNSS transaction files to CDC based on the actual or expected infant's date of birth. Files may be submitted quarterly, or may also be submitted annually if records are linked to Birth Certificate files.

Quarterly Submission

Actual or Expected Infant's Month of Birth	Record to CDC by:
January-March	September 1
April-June	December 1
July-September	March 1 of the following year
October-December	June 1 of the following year

Annual Submission (Vital Record Birth Certificate Linkage)

Actual or Expected Infant's Month of Birth	Record to CDC by:
January-December	September 1

File Transfer Options

The preferred mode for transferring transaction files to CDC is via the Internet, using the CDC Secure Data Network (SDN), described in greater detail on pages 5-17. Files may also be submitted on CD-ROM, cartridge, disk, or tape. Advantages of using the SDN include special precautions taken to enhance security of the files, such as user authorization via digital certification, and file encryption. PNSS files also reach CDC quicker and the SDN is free (no need to purchase cartridges, disks, or tapes). In special circumstances, CDC may approve submission of files via the Internet using FTP (file transfer protocol), and establish the related account.

Files submitted to the CDC National Center for Chronic Disease Prevention and Health Promotion (NCCDPHP) on CD-ROM, cartridge, disk or tape should be mailed to:

PNSS/PNSS Data Manager
Maternal and Child Nutrition Branch
NCCDPHP
4770 Buford Highway NE, MS K-25
Atlanta, GA 30341-4133

Encryption of Personal Identifiers

To ensure the confidentiality of clients in the PNSS database, personal identifiers that are based on full social security numbers (SSNs) or names of individuals that can be linked back to individual clients, must be encrypted. If you cite full SSNs or names of individuals in the first 30 positions of 1) field 9/Alphanumeric Identifier-Woman (record positions 36-65), and/or 2) field 59/Alphanumeric Identifier-Infant (record positions 240–269) on your PNSS transaction file, these record positions must be encrypted before transaction files are submitted to CDC.

ID Encryption Software

On request, CDC will send you a copy of the software required to encrypt your personal identifiers. Use of this software enhances the security of your PNSS data, since only you as the sender of the PNSS files has the encryption key (no one else, including CDC has access to the key). Because the related encryption process doubles the length of PNSS field 9/Alphanumeric ID-Woman and field 59/Infant Alphanumeric ID, it is important that SSNs and names of clients not exceed 30 original characters on the PNSS record. Both fields are 60 positions in length in the encrypted output file to accommodate this alteration.

The ID encryption software requires a Java Runtime Environment 4.79 or higher. It consists of three files; a Java program named 'EncryptFileParts.jar', a sample batch file named 'Encrypt.bat' and an encryption key file named ‘passkey.txt’. When you receive these files, we recommend that you create a folder on your C:\ drive named C:\encryption and use that folder for all of your encryption and data transfer operations.

Creating an Encryption Key

The encryption key file, ‘passkey.txt’, contains one line of 108 characters. In order to make your encryption key different from the default sent to you from CDC, you need to make a one-time change to the file before you use it for your first encryption. Open the file in your editor of choice (Notepad, for example), and change at least one of the characters in the file. The only restrictions are that you can only use the characters 0-9 and A-F and that the file must still contain 108 characters when you are finished. Once

you make this change, you must never change the file again and you must protect it as discussed in the section on Java Encryption Key Backup on page 4. If you change or lose your encryption key file, you will lose the ability to link future records with those that have already been encrypted.

Encrypting IDs on a PNSS File

When you are ready to begin to encrypt and transfer your PNSS data files to CDC, copy your data files into your transfer folder (C:\encryption or whatever other folder you decided to use).

Next, access your encryption folder. How you do so will depend on how your windows operating system is set up. Follow the instructions below that apply to your operating system. These instructions assume that you named your transfer encryption folder c:\encryption.

If you have DOS, go to a DOS Prompt and type C:\encryption.
If you have an older version of Microsoft, Go to Start, then Run, and type 'cmd' and click 'ok.'
If you have a newer version of Microsoft and NT, go to Start, Programs and click on Command Prompt .
If you have Windows 2000 or XP, go to Start, Programs, Accessories and click on Command Prompt.

Once you are at the c:\ prompt, type: C:\encryption.

Next run the encryption batch file by typing in the following command at the prompt (having one or more spaces between each command option):

```
Encrypt   UnencryptedInputFilename    EncryptedOutputFilename  S1 L1 S1 L1
```

Where UnencryptedInputFilename is the name of your unencrypted PNSS data file, EncryptedOutputFilename is the name you want to call your data file once the IDs are encrypted:

S1 – Sn is the starting record position of the Alphanumeric ID in each record you want to encrypt, and
L1 – Ln is the corresponding length of that ID field.

For example, to encrypt a PNSS file named Sta.PNSSdata.txt ("Sta" refers to state name) which has one woman's identifier (field 9) per record that begins at record position 36 and is 30 positions long prior to encryption and one infant's identifier (field 59) per record that begins at record position 240 and is 30 positions long prior to encryption and that returns a file named Sta.PNSSdataEncrypted.txt, use the following command:

```
Encrypt   Sta.PNSSdata.txt   Sta.PNSSdataEncrypted.txt  36 30 240 30
```

This encryption process will double the length of the PNSS field 9/Alphanumeric ID-Woman from 30 to 60 characters as well as PNSS field 59/Infant Alphanumeric ID on the encrypted output transaction file.

Once your data file has been encrypted, be sure when you are prompted for the name of a file to electronically transfer or copy to CD-Rom, cartridge, etc., to enter the encrypted file name (e.g., Sta.PNSSdataEncrypted) rather than the name of your original unencrypted file.

Encryption of IDs on Current and Historical PNSS Files

To maximize client confidentiality, contributors that must encrypt personal identifiers on their PNSS records need to perform the encryption process on all their PNSS records maintained at CDC. CDC will create a historical PNSS file with master file records in a flat text file format, and send it to the contributor, to support this effort.

Within one to three months after receiving the historical file from CDC, the contributor should return the amended file to CDC containing the newly encrypted identifiers. If the annual PNSS report is scheduled for production in less than one to three months after the contributor begins encrypting files, it may be most efficient for the contributor to assemble replacement transaction files with encrypted IDs for the most recent three years, and then encrypt remaining files at a later date. Three year combined analyses are included in annual PNSS reports.

All historical files at CDC with identifiers that are based on names and/or social security numbers will be destroyed for security purposes once the replacement file(s) containing the new encrypted identifiers has been received at CDC.

Java Encryption Key Back-Up

To identify duplicate records, and in the event that state or CDC staff wish to link records of individual women across different reporting periods, it is important to consistently encrypt identifiers in the same fashion. It is imperative that you use the same encryption 'key' (stored in the file 'passkey.txt' in your c:\encryption folder) *that originally accompanied the Java software* to encrypt identifiers on all historical, current, and future PNSS records. Each contributor creates a unique key that cannot be replicated.

When you agree to utilize the Java encryption software provided by the CDC's Maternal and Child Nutrition Branch, you are also agreeing to make a permanent back-up copy of the encryption key. To back-up your java encryption key, copy the configuration file 'passkey.txt from the computer where the encryption process is done to a back-up CD-ROM (or disk) and store in an 'on-site' and 'off-site' location in the event your computer fails or is replaced at a later time.

Advantages of the CDC Java Encryption Software

Use of the Java encryption software in the manner described above ensures that:

1) **the encryption process is consistent (i.e. Mary Smith always encrypts to the same encrypted ID.**
2) **the security of the contributor's encryption key is maintained (no one, including CDC has access to the encryption key);**
3) **the encryption software is maintained indefinitely and can be accessed from the configuration file on your computer.**

Internet File Submission
Using the CDC Secure Data Network

The Secure Data Network (SDN) is a facility provided by the CDC that allows remote users to transfer data to and from the CDC in a secure manner across the Internet. A remote user can be a state, U.S. territory or tribal government.

SDN System Requirements

To permit access to the SDN, you must have the following:

- **an IBM PC or compatible with a CPU of 486 or higher.**
- **Windows 95 or Windows NT 4.x or greater.**
- **Internet connectivity.**
- **Internet Explorer 5.x or Netscape Communicator 6.x or higher, with a connection to the Internet.**
- **Browser "cipher strength" of 128 byte or higher.**
- **administrative rights for the local machine on which the SDN digital certificate is to be installed (only for initial certificate installation).**

SDN Enrollment

Obtain Approval to Enroll

To begin the enrollment process, you must first gain approval for SDN enrollment by contacting the CDC PNSS and PedNSS staff at nccddnpapednss@cdc.gov, attention SDN Nutrition Administrator. If approved, you will receive the CDC general registration password to use on the CDC SDN enrollment web site.

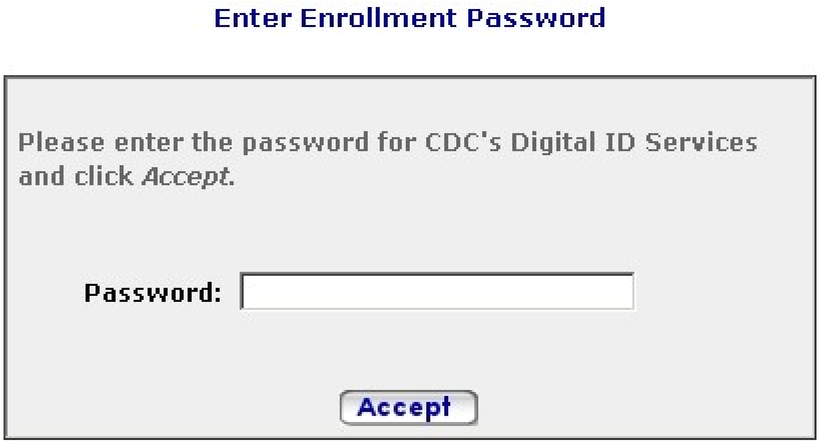
The CDC Nutrition SDN Administrator will routinely approve SDN enrollment for one person in a state, tribal government, or territory responsible for assembling and transmitting PNSS and/or PedNSS (Pediatric Nutrition Surveillance System) files to CDC. If the PNSS and PedNSS files are managed by different persons, CDC will approve enrollment for the person responsible for assembling and transmitting PNSS files to CDC, as well as the person responsible for assembling and transmitting PedNSS files to CDC. If these person(s) feel strongly that they need an additional person as 'back-up' to the person(s) responsible for assembling and transmitting PNSS and/or PedNSS files, the CDC Nutrition SDN Administrator may also grant approval to the 'back-up' person.

Access Enrollment Site

The SDN enrollment website can be reached by accessing the following uniform resource locator (URL):

https://ca.cdc.gov

Upon accessing the site, an initial enrollment password page will appear. To continue, you must enter the general registration password provided by the CDC SDN Nutrition Administrator. After entering the registration password, click on the *Accept* button to continue.



Enter Enrollment Password

Please enter the password for CDC's Digital ID Services and click *Accept*.

Password:

Review Requirements and Accept Subscriber Agreement

You will be presented with a general information page providing an overview of digital certificates and system requirements that should be reviewed thoroughly before continuing. Additionally, the VeriSign Subscriber Agreement referenced from this page must be reviewed prior to application for a digital certificate.

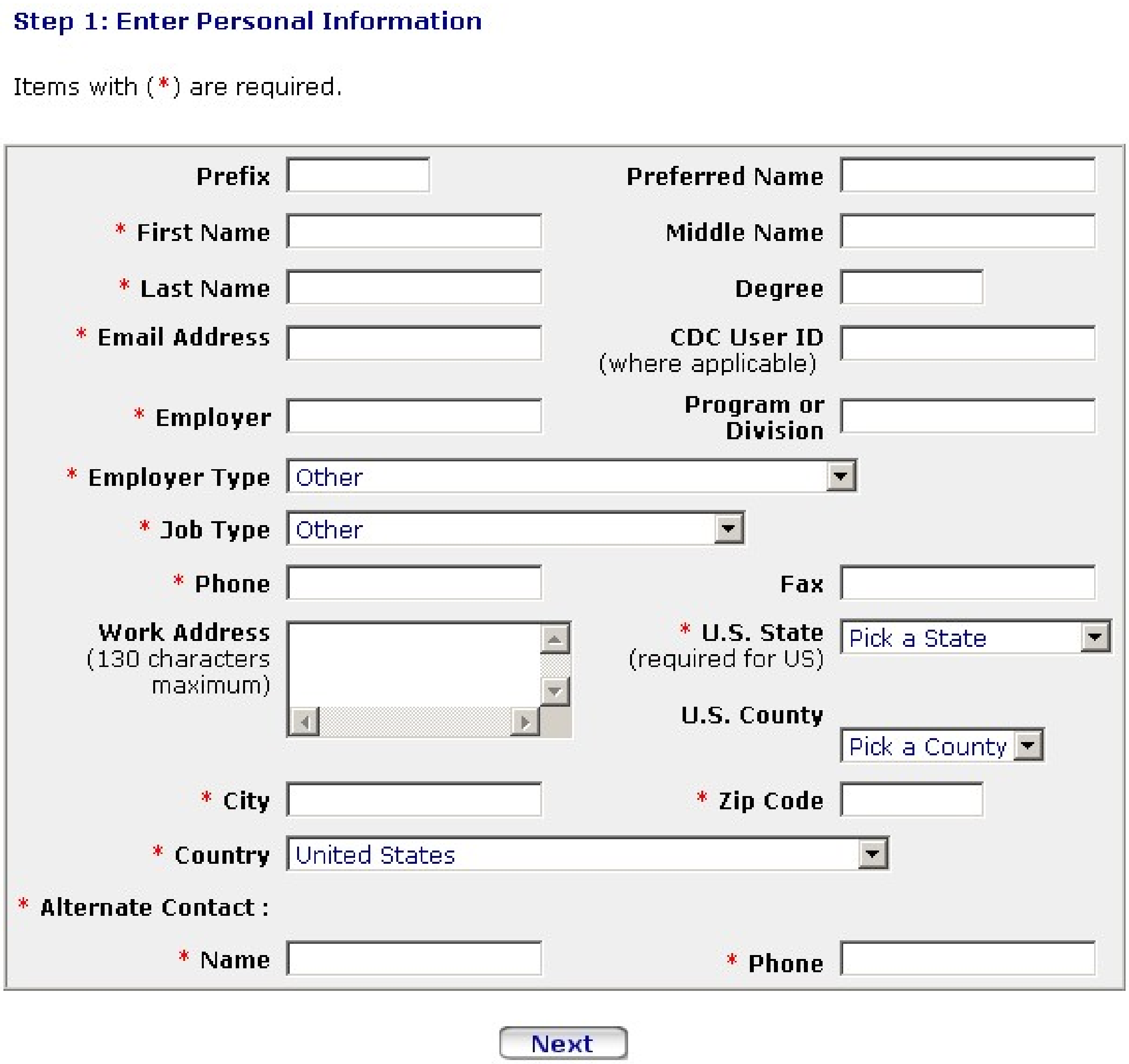
Obtaining and installing an SDN digital certificate, which authorizes a user to access the SDN, needs to be done <u>only</u> <u>once</u> for each workstation that will be used for uploading data using the SDN. The computer used for the original application must be the same computer used to download and install the approved SDN digital certificate.

The issuance and use of a digital certificate from VeriSign is governed by the VeriSign Certification Practice Statement (CPS) and Digital ID Subscriber Agreement. For more information regarding the CPS or Agreement, please visit the VeriSign website at www.verisign.com/repository.

After reviewing the enrollment information, indicate your acceptance of the terms of the agreement and proceed to the first enrollment step by clicking the *Enroll* button.

Enter Personal Information

Below the information area is a form that must be completed to continue the enrollment process. The form is used to create your digital certificate and should be completed with as much information as possible (all required fields are denoted by an asterisk). This information will be used by the CDC SDN Nutrition Administrator and the CDC SDN Working Group to verify your identity.



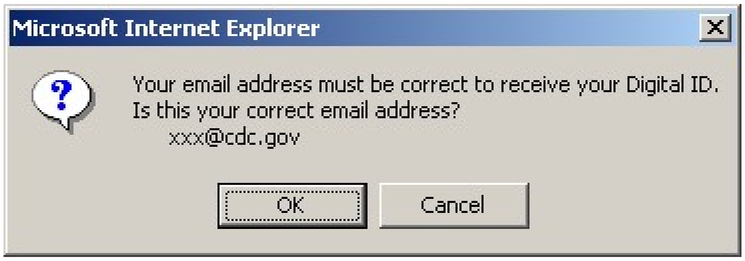
Step 1: Enter Personal Information

Items with (*) are required.

Prefix		Preferred Name	
* First Name		Middle Name	
* Last Name		Degree	
* Email Address		CDC User ID (where applicable)	
* Employer		Program or Division	
* Employer Type	Other		
* Job Type	Other		
* Phone		Fax	
Work Address (130 characters maximum)		* U.S. State (required for US)	Pick a State
		U.S. County	Pick a County
* City		* Zip Code	
* Country	United States		
* Alternate Contact :			
* Name		* Phone	

After completing the personal information form, click the *Next* button to continue.

A confirmation dialog will appear to verify the e-mail address provided on the personal information form.



Microsoft Internet Explorer

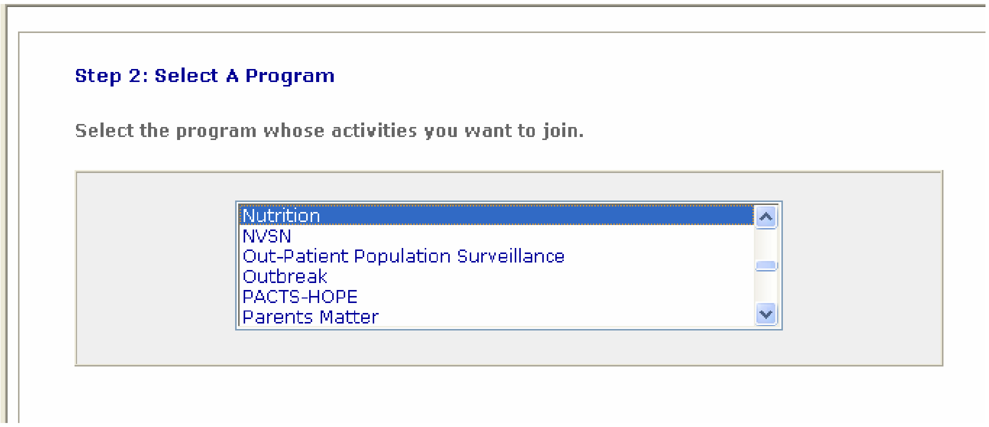
Your email address must be correct to receive your Digital ID.
Is this your correct email address?
xxx@cdc.gov

It is important that the e-mail address you provide is accurate and used in conjunction with the performance of your duties (i.e., not a personal account). The information required to complete the installation of your digital certificate will be sent to the address provided.

After confirming your e-mail address is correct, click the *OK* button to continue. If your e-mail address is incorrect, click the *Cancel* button to return to the personal information form.

Select Program

The program selection list box allows you to choose the program for which you are requesting access. To select the program, simply highlight it from the list box and click Next.



Step 2: Select A Program

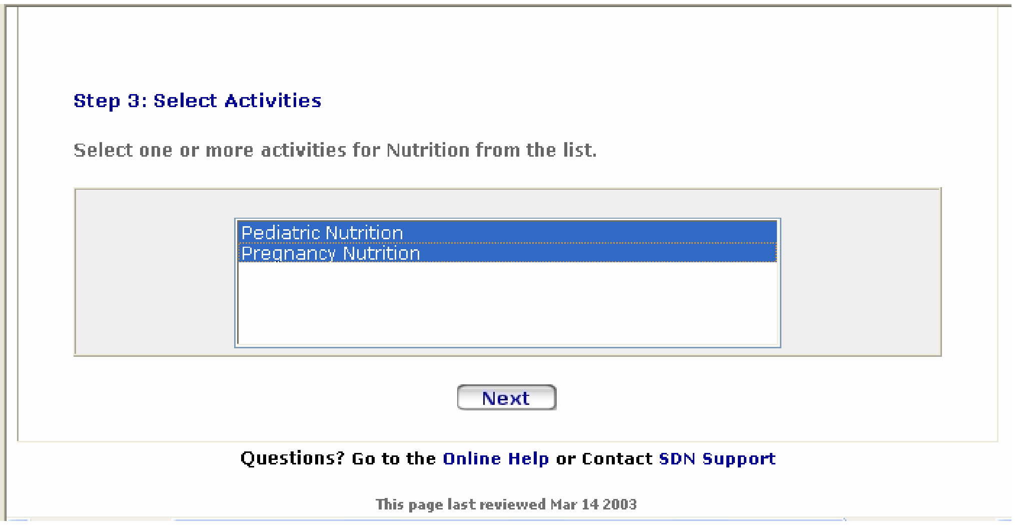
Select the program whose activities you want to join.

During initial enrollment, you may only select one program, e.g., Nutrition, from the available list. In the unlikely event that you require access to more than one program, first select the program (e.g., Nutrition) identified by the program administrator who extended the enrollment invitation. After your digital certificate has been issued and you access SDN, there will be an opportunity to request additional programs and activities (i.e., it is not necessary to apply for more than one digital certificate).

Select Activities

To identify the program-specific activities, (e.g. Pregnancy Nutrition and/or Pediatric Nutrition), to which you desire access, select one or both entries from the list. In the example below, the available activities for the Nutrition program are presented.

After you have made your activity selection(s), click the *Next* button to continue.



Step 3: Select Activities

Select one or more activities for Nutrition from the list.

Questions? Go to the Online Help or Contact SDN Support

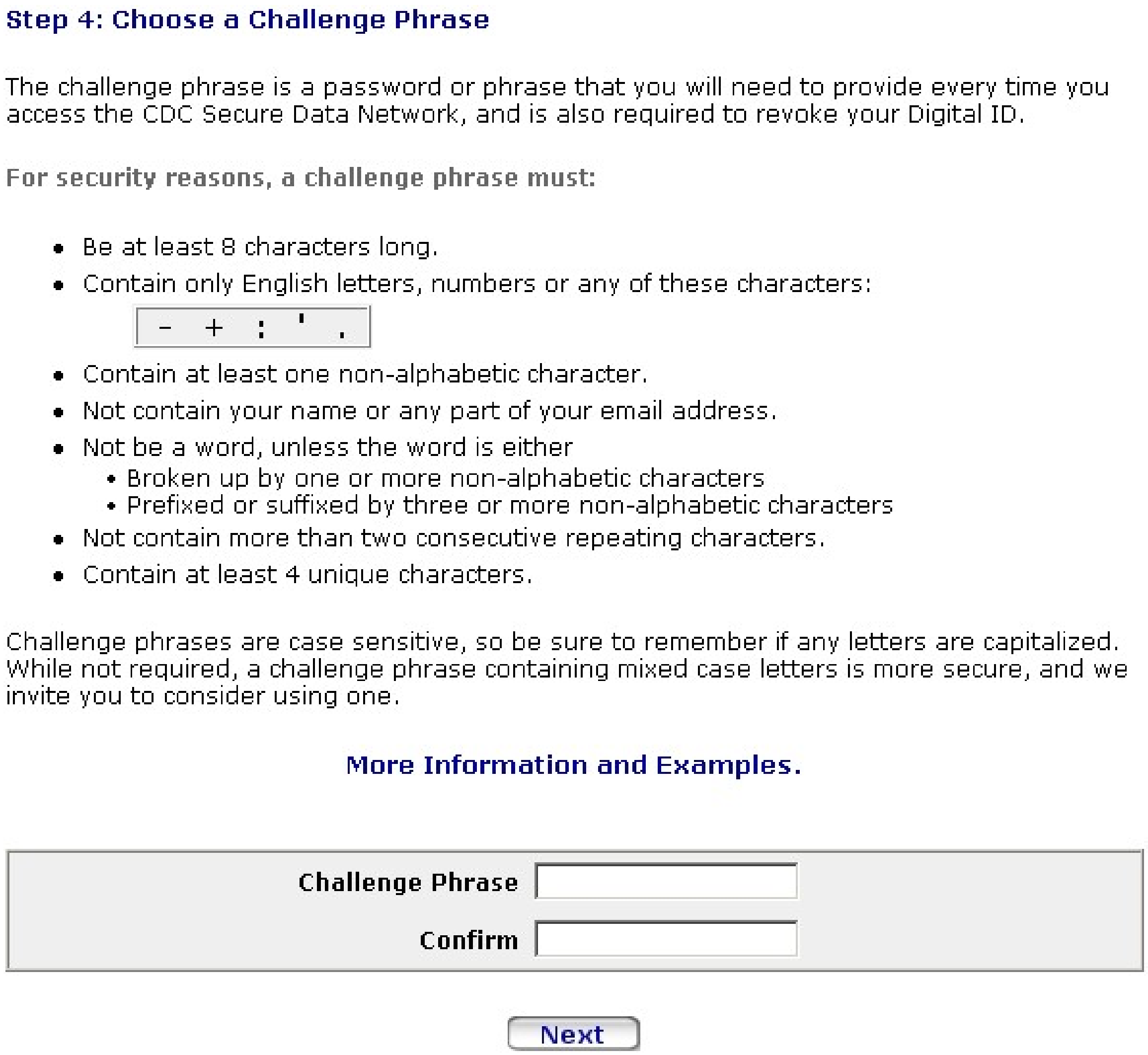
This page last reviewed Mar 14 2003

Choose Challenge Phrase

To ensure the security of your access to SDN, a challenge phrase must be created. This challenge phrase is used in conjunction with your Digital ID to authenticate you as a user of SDN. ***It is important to remember your challenge phrase. Do not share it with other SDN users.***

A general overview of the challenge phrase, which is required for use and management of your digital certificate, is provided below.

You must select a challenge phrase based on the guidelines presented and enter it twice (once in the Challenge Phrase field and once in the Confirm field). After your challenge phrase has been entered in both fields, click the *Next* button to continue.



Step 4: Choose a Challenge Phrase

The challenge phrase is a password or phrase that you will need to provide every time you access the CDC Secure Data Network, and is also required to revoke your Digital ID.

For security reasons, a challenge phrase must:

- Be at least 8 characters long.
- Contain only English letters, numbers or any of these characters: - + : ' .
- Contain at least one non-alphabetic character.
- Not contain your name or any part of your email address.
- Not be a word, unless the word is either
  - Broken up by one or more non-alphabetic characters
  - Prefixed or suffixed by three or more non-alphabetic characters
- Not contain more than two consecutive repeating characters.
- Contain at least 4 unique characters.

Challenge phrases are case sensitive, so be sure to remember if any letters are capitalized. While not required, a challenge phrase containing mixed case letters is more secure, and we invite you to consider using one.

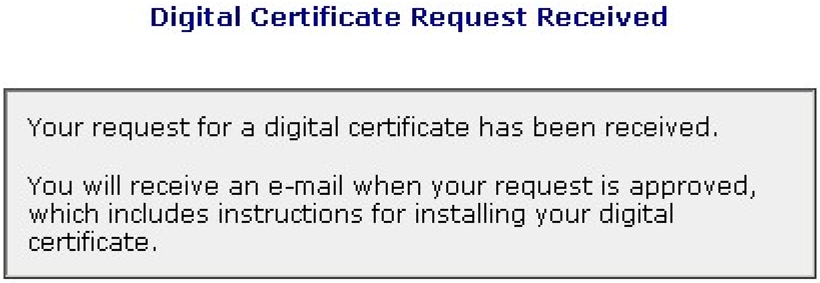
More Information and Examples.

Challenge Phrase

Confirm

Check E-mail

When the request for a digital certificate has been received by SDN, a notification to check your e-mail account (the one provided during enrollment) will appear.

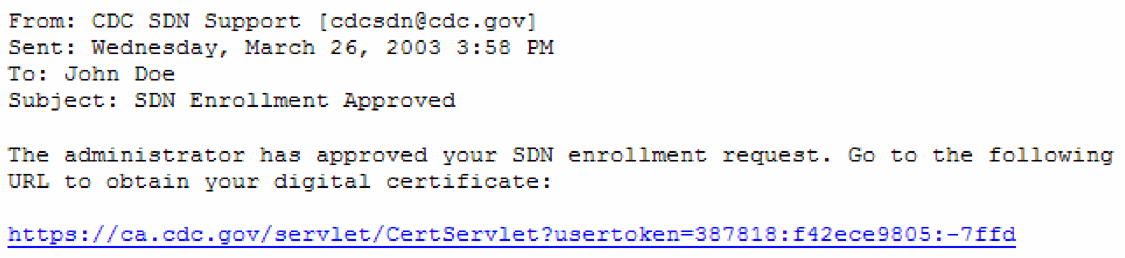


Digital Certificate Request Received

Your request for a digital certificate has been received.

You will receive an e-mail when your request is approved, which includes instructions for installing your digital certificate.

When your digital certificate request (including program activities) has been approved, an e-mail will be sent to your account with instructions to access a specific URL for obtaining your digital certificate.



```
From: CDC SDN Support [cdcsdn@cdc.gov]
Sent: Wednesday, March 26, 2003 3:58 PM
To: John Doe
Subject: SDN Enrollment Approved

The administrator has approved your SDN enrollment request. Go to the following
URL to obtain your digital certificate:

https://ca.cdc.gov/servlet/CertServlet?usertoken=387818:f42ece9805:-7ffd
```

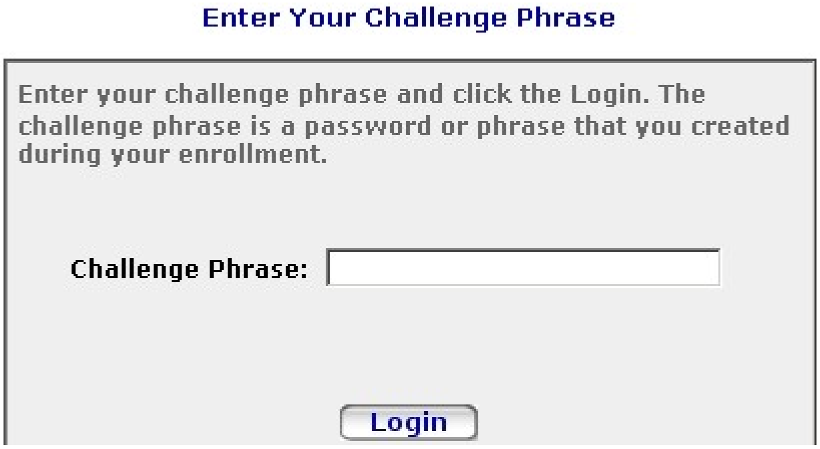
Certificate Issuance

Re-Access Enrollment Site

To re-access the SDN enrollment site and begin the process of downloading your digital certificate, use the URL provided to you in your e-mail notification by clicking on the hyperlink or copying and pasting the URL into your browser.

The URL provided in your e-mail notification is unique and must be entered exactly as provided if entered manually into your browser address field.

Upon re-access of the enrollment site, you will be prompted to enter the challenge phrase you created during the initial enrollment process. After you have entered your challenge phrase, click the *Login* button to continue.



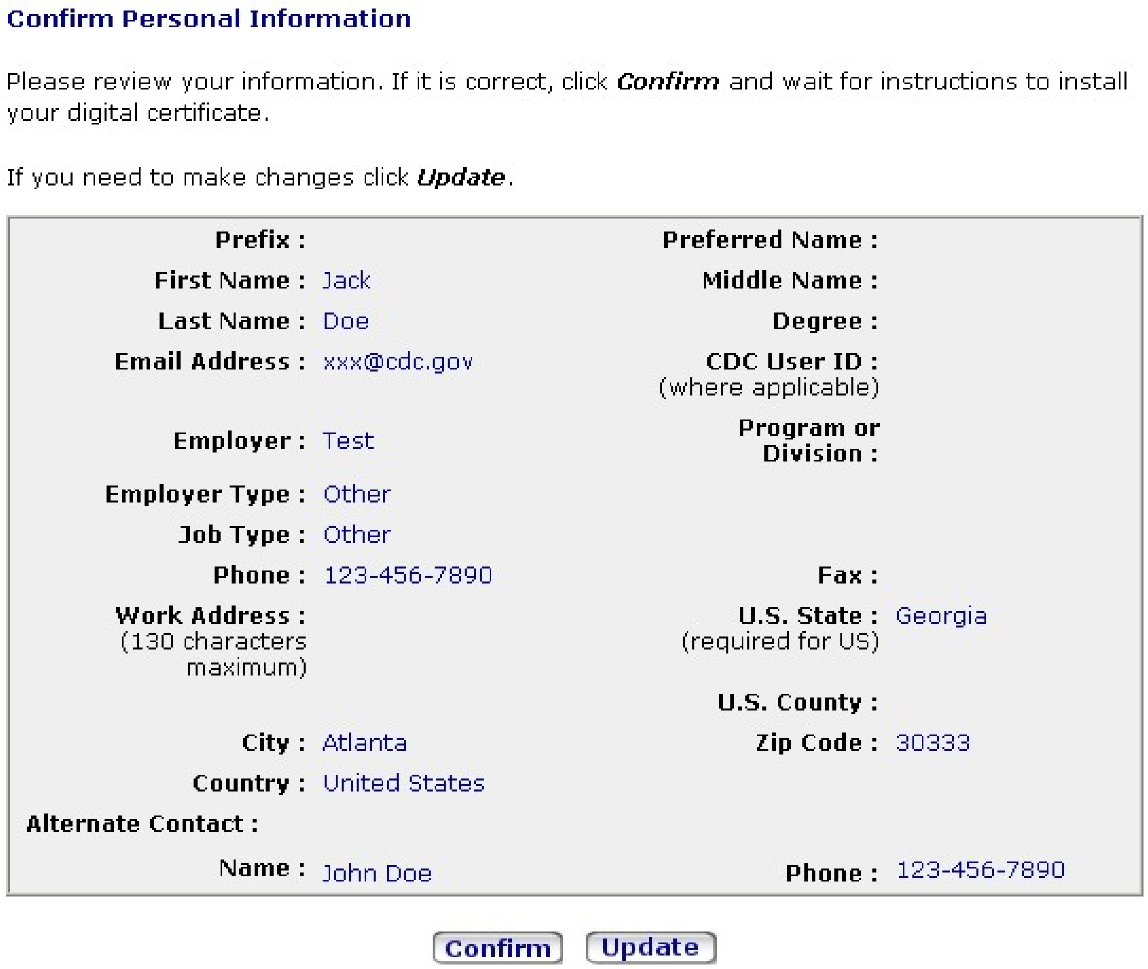
Enter Your Challenge Phrase

Enter your challenge phrase and click the Login. The challenge phrase is a password or phrase that you created during your enrollment.

Challenge Phrase:

Confirm Personal Information

Upon successful re-authentication, the personal information you entered during the initial enrollment will be presented.



Confirm Personal Information

Please review your information. If it is correct, click ***Confirm*** and wait for instructions to install your digital certificate.

If you need to make changes click ***Update***.

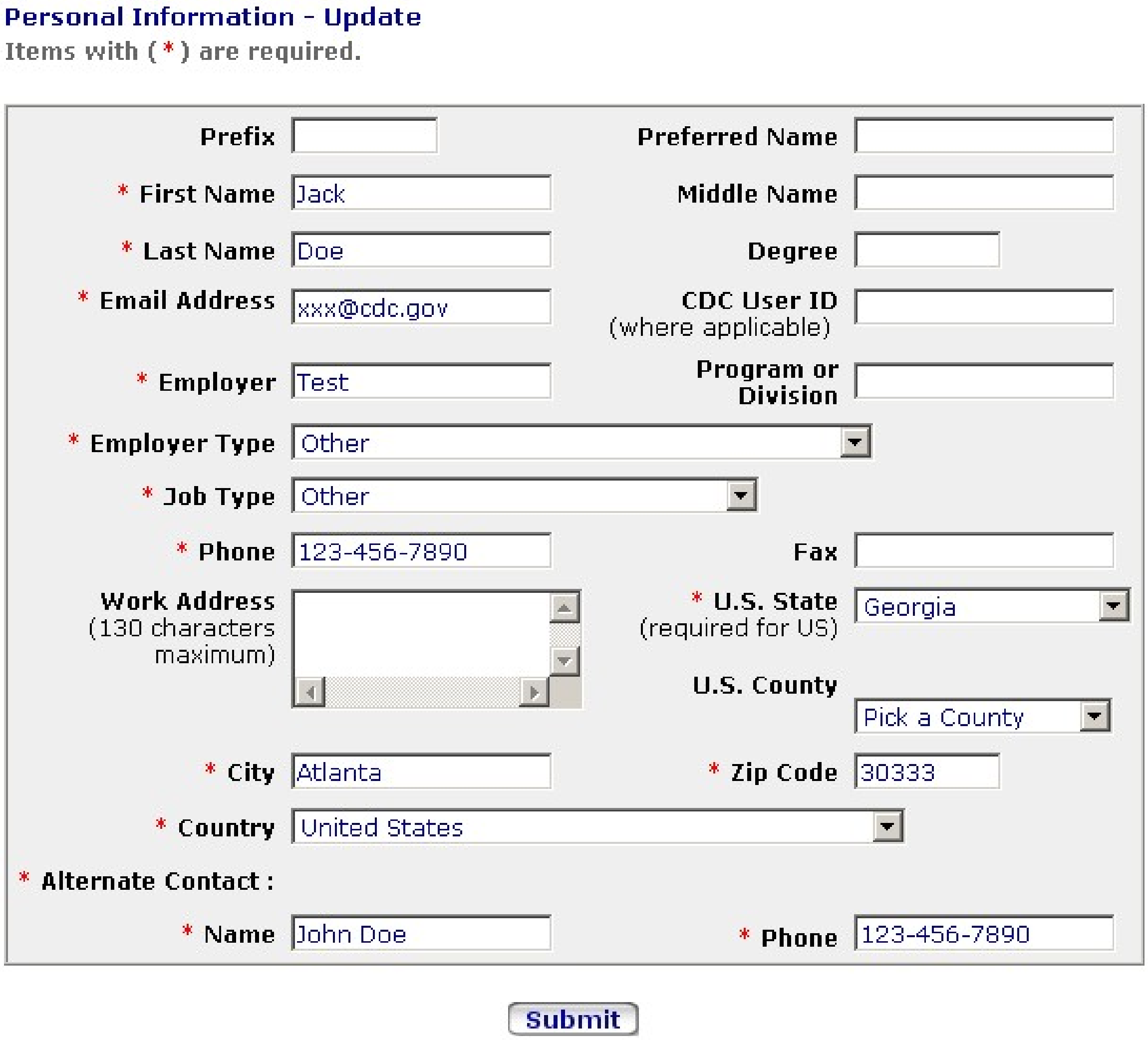
Prefix :		**Preferred Name :**	
First Name :	Jack	**Middle Name :**	
Last Name :	Doe	**Degree :**	
Email Address :	xxx@cdc.gov	**CDC User ID :** (where applicable)	
Employer :	Test	**Program or Division :**	
Employer Type :	Other		
Job Type :	Other		
Phone :	123-456-7890	**Fax :**	
Work Address : (130 characters maximum)		**U.S. State :** (required for US)	Georgia
		U.S. County :	
City :	Atlanta	**Zip Code :**	30333
Country :	United States		
Alternate Contact :			
Name :	John Doe	**Phone :**	123-456-7890

If the information entered during initial enrollment is incorrect, click the *Update* button, otherwise click the *Confirm* button to continue.

It is important that all information entered is correct before the digital certificate is issued, as it will be permanently associated with the digital certificate itself and can thereafter be only changed within SDN and will not be reflected by the certificate.

Update Personal Information

If you choose to update your personal information, a form with the information entered during initial enrollment will be presented.



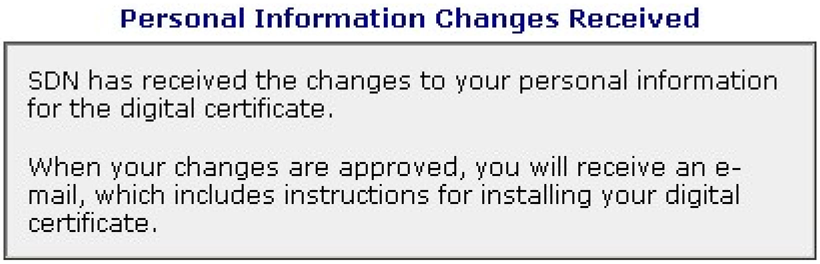
Personal Information - Update

Items with (*) are required.

Prefix		Preferred Name	
* First Name	Jack	Middle Name	
* Last Name	Doe	Degree	
* Email Address	xxx@cdc.gov	CDC User ID (where applicable)	
* Employer	Test	Program or Division	
* Employer Type	Other		
* Job Type	Other		
* Phone	123-456-7890	Fax	
Work Address (130 characters maximum)		* U.S. State (required for US)	Georgia
		U.S. County	Pick a County
* City	Atlanta	* Zip Code	30333
* Country	United States		
* Alternate Contact :			
* Name	John Doe	* Phone	123-456-7890

To add, modify, or remove information, simply edit the appropriate field on the form. As with initial enrollment, certain fields on the form are required and denoted with an asterisk. Although the data in these fields may be modified, they cannot be left blank. Once the information on the form has been updated, click the *Submit* button to continue.

If any data in one of the required fields is modified, the enrollment information must be reviewed and re-approved by the nutrition program administrator. If a required field has been updated, a confirmation dialog will appear.



Personal Information Changes Received

SDN has received the changes to your personal information for the digital certificate.

When your changes are approved, you will receive an e-mail, which includes instructions for installing your digital certificate.

Install Digital Certificate

After confirmation of the enrollment information, your browser will be automatically directed to begin creation of the digital certificate based on the type of browser being used. For Internet Explorer users, certificate generation and installation will be done automatically. For Netscape users, certificate generation will be done automatically, and instructions for the installation of the certificate will be provided.

For Netscape users, the installation instructions must be followed as specified because the certificate cannot be installed into the browser automatically.

If the generation or installation of the certificate fails, and you are unable to obtain your digital certificate using your current enrollment request, contact the CDC PNSS and PedNSS staff at nccddnpapednss@cdc.gov, attention SDN Nutrition Administrator, for assistance.

Transferring PNSS Files to CDC

Access the SDN

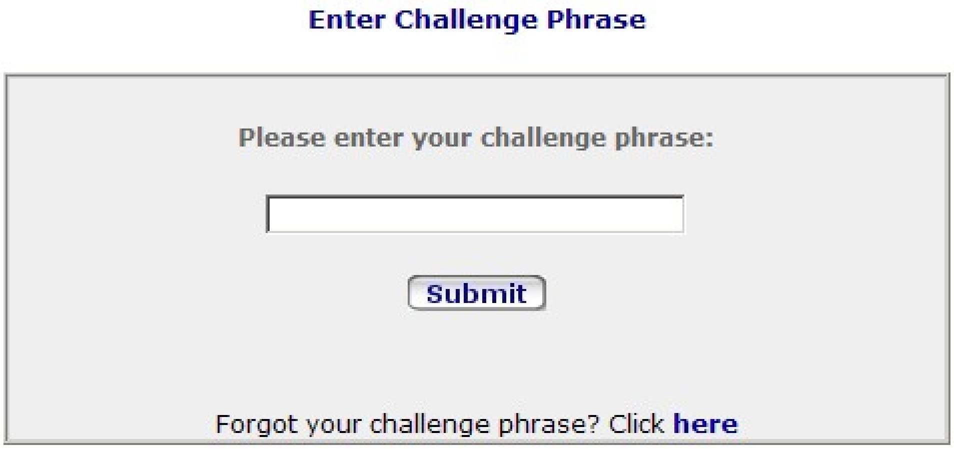
When the digital certificate has been successfully installed, the SDN website can be accessed by going to the following URL:

https://sdn.cdc.gov

Depending upon the security settings of the browser, a prompt may appear.

It is possible that more than one digital certificate associated with your name will appear when you first access the URL, if your prior digital certificate has expired. In this case, choose the certificate that has not expired. Click the *OK* button to continue.

After selection and/or presentation of the digital certificate, the SDN challenge phrase page will be presented.


Enter Challenge Phrase

Please enter your challenge phrase:

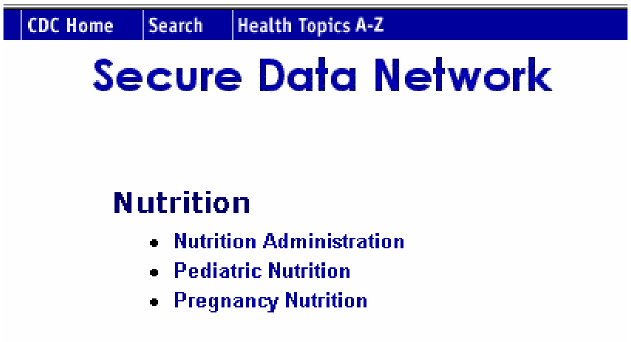
Forgot your challenge phrase? Click here

The challenge phrase entered when enrolling as an SDN user must be provided. After entering the challenge phrase, click the *OK* button to continue.

If the challenge phrase has been lost or forgotten, it is possible to establish a new one by clicking the link provided and entering a replacement. If a new challenge phrase is requested, all activities will be disabled and must be re-approved by the CDC SDN Nutrition Administrator.

Select Program Activity

Once the challenge phrase has been verified, the main SDN page will be displayed providing a list of all available activities. Select the Nutrition activity, Pregnancy Nutrition.



Secure Data Network

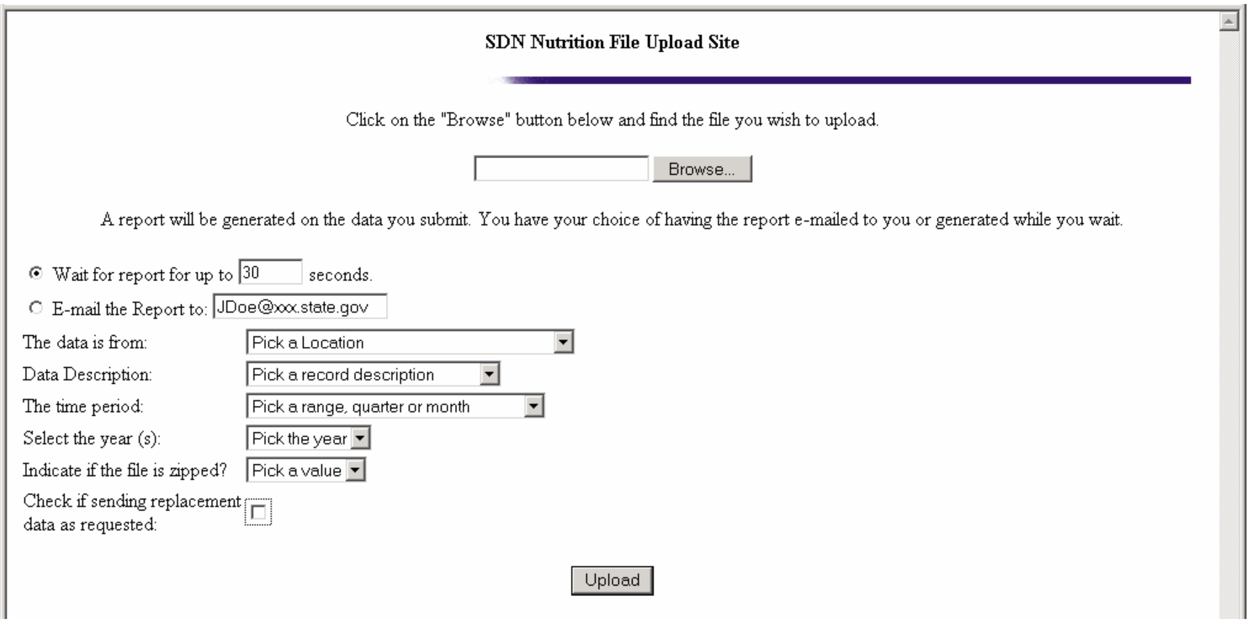
Nutrition

- Nutrition Administration
- Pediatric Nutrition
- Pregnancy Nutrition

Select, Describe and Upload the PNSS File You Want to Transfer

The SDN Nutrition Upload Site appears. Click browse to locate the file you wish to upload and then identify where 'the data is from' (state), complete the 'data description' (identify whether the file is a routine transaction file, a transaction file containing school data, a transaction file containing test data, if the transaction file personal identifiers have been encrypted, or if the file is a code file), the 'time period' and 'year' of data being transmitted. CDC also needs to know if the file is a 'zipped' file and if the file is a 'replacement' file to one previously transmitted to CDC. Once your description is complete, click the Upload button to transmit the file to CDC.

It is also possible to transfer a PNSS/PedNSS code file to CDC via the SND (an option under the 'data description' window on the SDN Nutrition Upload Site.



SDN Nutrition File Upload Site

Click on the "Browse" button below and find the file you wish to upload.

A report will be generated on the data you submit. You have your choice of having the report e-mailed to you or generated while you wait.

● Wait for report for up to 30 seconds.

○ E-mail the Report to: JDoe@xxx.state.gov

The data is from: Pick a Location

Data Description: Pick a record description

The time period: Pick a range, quarter or month

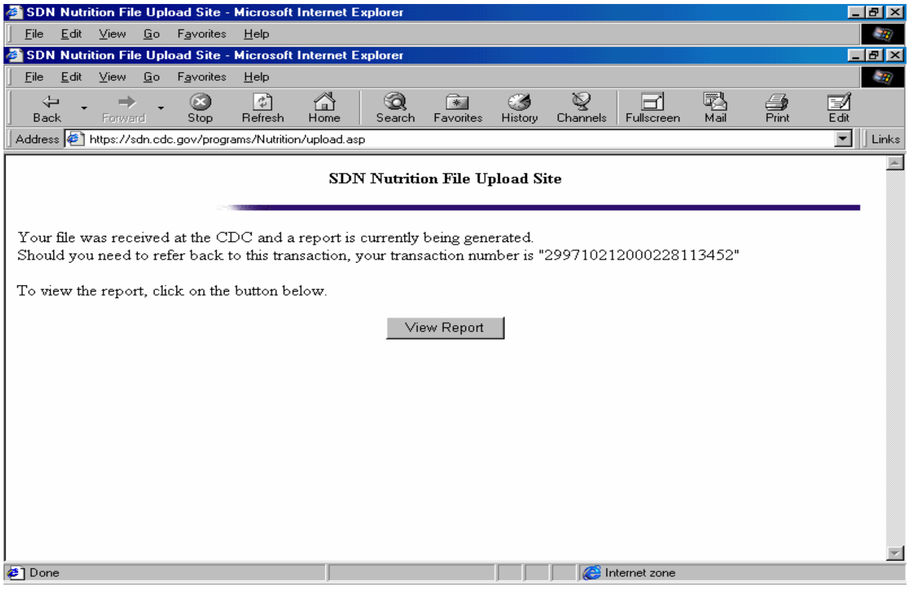
Select the year (s): Pick the year

Indicate if the file is zipped? Pick a value

Check if sending replacement data as requested: □

Receive Confirmation of File Transfer

Within a few minutes of transferring your files, you should receive a web page that either confirms the success of your transfer and gives you a confirmation number, or tells you that the transfer failed.


SDN Nutrition File Upload Site - Microsoft Internet Explorer
File Edit View Go Favorites Help
SDN Nutrition File Upload Site - Microsoft Internet Explorer
File Edit View Go Favorites Help
Back
Forward
Stop
Refresh
Home
Search
Favorites
History
Channels
Fullscreen
Mail
Print
Edit
Address
Links
View Report
Done
Internet zone

https://sdn.cdc.gov/programs/Nutrition/upload.asp

SDN Nutrition File Upload Site

Your file was received at the CDC and a report is currently being generated.
Should you need to refer back to this transaction, your transaction number is "29971021200022811345 2"

To view the report, click on the button below.

If you are successful, send an email to CDC at nccddnpapednss@cdc.gov, with the confirmation number so that CDC can track your file. If you are not successful in transferring your files after two or three attempts, report this to CDC using the above email address. Emailing CDC is only necessary for your first few file submissions, to confirm the SDN process is working successfully for you.

Challenge Phrase and Digital Certificate Back-Up For SDN Users

It is important to backup your digital certificate and challenge phrase, ideally before you begin transmitting PNSS data to CDC. If you lose your digital certificate, you can re-apply for another one, but this will result in delays. If you lose your challenge phrase, you can also be approved to use a different phrase, but this too creates delays.

Challenge Phrase Back-up

The 'challenge phrase' is used each time you access the CDC Secure Data Network (SDN) to transmit PNSS or PedNSS data files or code files to CDC. Please type the challenge phrase in a text document and save the file as a back-up to disk or CD-Rom. You may want to store one back-up disk in a secure 'on-site' as well as an 'off-site' location in the event your computer crashes or is replaced at a later time.

Digital Certificate Back-Up

The original digital certificate installed on your computer must be used each time you transmit data via the SDN. ***Therefore, when you first receive your digital certificate, you need to export the certificate to a disk as a backup copy for use in the event your computer ever has to be replaced or upgraded.***

You may want to store your back-up disks in a secure 'on-site', as well as 'off-site' location in the event your computer crashes or is replaced at a later time.

To Export an Internet Explorer 5.5 (and up) Digital Certificate:

Click on Tools | Internet Options.
Click the Content tab.
In the certificates section in the middle, click the "Certificates" button.
The available certificates are shown in the dialog box.
Click on the certificate to export.
The "Export" and "Remove" buttons below the list become enabled.
Click the "Export" button.
The Certificate Manager Export Wizard starts.
On the Welcome screen, click Next.
Keep the default to "...export the private key" and click Next.
Keep the default to file type of Personal Information Exchange BUT
*****UNCHECK the Enable Strong Protection if that's checked (for IE 5.0 or NT 5.0 or above).**
*****and CHECK the "Include all certificates in the certification path".**
Click Next.
Complete the Password screen. We suggest using the SDN Challenge Phrase if it was kept private.
Type the path and filename of the file to export. It will automatically give it the .pfx extension. Specify a path other than your hard drive, for example A:\mycerts.pfx, otherwise it will export to a default directory on the hard drive.
Click Next.
Review the information and click Finish.
The next message should indicate the success of the export.

To Import an Internet Explorer 5.5 (and up) Digital Certificate:

Click on Tools | Internet Options.
Click the Content tab.
In the certificates section in the middle, click the "Certificates" button.
The available certificates are shown in the dialog box.
Click the "Import" button.
The Certificate Manager Import Wizard starts.
On the Welcome screen, click Next.
Browse to the certificate file on the floppy disk and click Next.
Enter the password used to protect the certificate. Leave the check boxes unchecked and click Next.
Select the "Automatically select the certificate store..." (which may be the default) and click Next.
Review the information and click Finish.
The next message should indicate the success of the import.

To Export a Netscape 4.6–4.8 (for Netscape versions over 6.0, see below) Digital Certificate:

Click the toolbar option for "Security".
The Security Info screen appears.
Under the heading "Certificates", click "Yours". Your certificates are displayed.
Click on the certificate to export.
Click the Export button.
If your Netscape DB is protected with a password, you will be prompted to enter it (see Netscape Communicator Certificate DB password instructions below).
Type the path and filename to export in the dialog box, then click Save.
The next message should indicate the success of the export.

To Import a Netscape 4.6–4.8 Digital Certificate:

Click the toolbar option for "Security".
The Security Info screen appears.
Under the heading "Certificates", click "Yours". Your certificates are displayed.
Scroll down to see that under the box showing the certificates, there is a button "Import a Certificate".
Click the "Import a Certificate" button.
Browse to the certificate file on the floppy disk and click Open.
If your Netscape DB is protected with a password, you will be prompted to enter it (see Communicator Certificate DB password instructions below).
The next message should indicate the success of the import.

To Export a Netscape 6.0 (and Above) Digital Certificate:

Click Edit, then Preferences.
Click the triangle beside Privacy and Security.
Click to highlight Certificates and press Manage Certificates.
Click Backup and follow the instructions. Be sure to put an A:\ in front of your filename to send it to the A: drive if not otherwise prompted.

You may be prompted beforehand to enter or set a Master Password. We typically recommend you use your challenge phrase. Netscape may ask you for this password whether or not you have set one and if this is preventing your from exporting the certificate, your only option is to reset the password (see Communicator Certificate DB password instructions below). This will also wipe out any certificates you have in your browser.

Note: the Master Password is not the same as the password used to encrypt the certificate, which Verisign should have given you.

To Import a Netscape 6.0 (and Above) Digital Certificate:
Click Edit, then Preferences.
Click the triangle beside Privacy and Security.
Click to highlight Master Passwords.
Click Reset Password and press Okay.
Click to highlight Certificates and press Manage Certificates.
Click Restore, then browse to the directory where you saved your certificate.
If you're in doubt, you can click Start Button, Search, then look for a file with the three-digit extension p12.
Browse to the file and click to select it, then enter the password used to encrypt the file (Verisign should have given you this when it downloaded the file).
If prompted to set a Master Password, use your challenge phrase.

Netscape Communicator Certificate DB Password

The Communicator Certificate DB password is specific to the Netscape browser you're using and should have been set during the initial application process.

If you are getting this dialog box and cannot recall the password, or if someone else set the password, or if you suspect you've been locked out, do the following:

1) **Close Netscape and click the Start button.**
2) **Select Search or Find.**
3) **Enter *.db as your search criteria and search the C: drive or wherever your program files are installed.**
4) **Locate files cert7 (may be cert7.db), key3, signed0, and secmod in your Netscape directory and delete them.**

This will wipe out any certificates that have been installed in Netscape, but you should be able to import successfully afterwards.