Secretary of State

NOTICE OF PROPOSED RULEMAKING HEARING*

A Statement of Need and Fiscal Impact accompanies this form.

Department of Human Services, Office for Oregon Health Policy and Research (OHPR)	**409**
Agency and Division	Administrative Rules Chapter Number

Jennifer Bittel	**500 Summer St. NE, E-03, Salem, OR 97301**	**503-947-5250**
Rules Coordinator	Address	Telephone

RULE CAPTION

Health Care Acquired Infection Reporting and Public Disclosure

Not more than 15 words that reasonably identifies the subject matter of the agency's intended action.

June 19, 2008	**1:00-2:30pm**	**General Services Building, Neahkanie Room 1225 Ferry St., Salem, OR 97301**	**Jennifer Bittel**
Hearing Date	Time	Location	Hearings Officer

Auxiliary aids for persons with disabilities are available upon advance request.

RULEMAKING ACTION

Secure approval of new rule numbers (Adopted or Renumbered rules) with the Administrative Rules Unit prior to filing.

ADOPT: OAR 409-023-0000, 409-023-0005, 409-023-0010, 409-023-0015, 409-023-0020, 409-023-0025, 409-023-0030, 409-023-0035

Stat. Auth.: **ORS 442.838, 442.420(3)(d)**

Other Auth.: **ORS 442.455, 442.405**

Stats. Implemented: **ORS 442.838, 442.445, 442.015, 442.011, 192.502, 192.496, 192.410, 192.245, 192.243, 179.505**

RULE SUMMARY

The general purpose of these rules is to implement the health care acquired infection (HAI) reporting, public disclosure, and other applicable mandates of House Bill 2524, which was enacted by the 74th Legislative Assembly. Included was a mandate to adopt administrative rules to implement the bill by July 1, 2008. The proposed rule is intended to fulfill this mandate by prescribing the HAI that are reported, how they are reported, the health care facilities that report them, and how they are publicly disclosed.

Proposed rules are available on the DHS Website: http://www.oregon.gov/DHS/admin/dwssrules/index.shtml.
For hardcopy requests, call: (503) 947-5250.

The Department requests public comment on whether other options should be considered for achieving the rule's substantive goals while reducing the negative economic impact of the rules on businesses.

June 23, 2008; 5:00pm
Last Day for Public Comment (Last day to submit written comments to the Rules Coordinator)

Jennifer D. Bittel	**Jennifer Bittel, Rules Coordinator**	*5/12/08*
Signature	Printed name	Date

*Hearing Notices published in the Oregon Bulletin must be submitted by 5:00 pm on the 15th day of the preceding month unless this deadline falls on a weekend or legal holiday, upon which the deadline is 5:00 pm the preceding workday. ARC 920-2005

Secretary of State

STATEMENT OF NEED AND FISCAL IMPACT

A Notice of Proposed Rulemaking Hearing or a Notice of Proposed Rulemaking accompanies this form.

Department of Human Services, Office for Oregon Health Policy and Research (OHPR) **409**

Agency and Division | Administrative Rules Chapter Number

In the Matter of:
The adoption of OAR 409-023-0000, 409-023-0005, 409-023-0010, 409-023-0015, 409-023-0020, 409-023-0025, 409-023-0030, 409-023-0035.

Rule Caption: (Not more than 15 words that reasonably identifies the subject matter of the agency's intended action.)
Health Care Acquired Infection Reporting and Public Disclosure

Statutory Authority: **ORS 442.838, 442.420(3)(d)**
Other Authority: **ORS 442.455, 442.405**
Stats. Implemented: **ORS 442.838, 442.445, 442.015, 442.011, 192.502, 192.496, 192.410, 192.245, 192.243, 179.505**

Need for the Rule(s):
The purpose of these rules is to implement the health care acquired infection (HAI) reporting, public disclosure, and other applicable mandates of House Bill 2524, which was enacted by the 74th Legislative Assembly. Included was a mandate to adopt administrative rules to implement the bill by July 1, 2008. These rules are needed to fulfill this mandate by prescribing the HAI that are reported, how they are reported, the health care facilities that report them, and how the information is disclosed to the public.

Documents Relied Upon, and where they are available:
The Patient Safety Component Protocol of the NHSN Manual is freely available from the Centers for Disease Control and Prevention web site (downloaded March 21, 2008):
http://www.cdc.gov/ncidod/dhqp/pdf/nhsn/NHSN_Manual_PatientSafetyProtocol_CURRENT.pdf

Fiscal and Economic Impact:
The anticipated fiscal impact on the Department and OHPR was addressed in HB 2524 by allocating funds to OHPR sufficient to start and run the HAI reporting program for the current biennium. No fiscal impact to other agencies is intended or expected. Since the estimated costs of compliance are a very, very tiny fraction of total revenues, the proposed rules are not expected to cause any adverse fiscal impact for hospitals. In fact, some peer-reviewed studies suggest that increased vigilance on detecting and preventing HAIs generally results in cost savings for hospitals. No economic impact on individual members of the public is intended or expected.

Statement of Cost of Compliance:
1. Impact on state agencies, units of local government and the public (ORS 183.335(2)(b)(E)):
There are no compliance mandates for other state agencies. The direct costs of compliance only impact facilities. For hospitals owned by county governments, the estimated person hours and FTE costs of compliance are listed below:

Coos County, Southern Coos Hospital
Estimated total person hours: 45
Estimated FTE: .02

These person-hours are incurred over an entire calendar year and include an estimated 20 person hours due to non-recurring start-up activities. The Department is unable to estimate the fiscal impact of these changes for the hospital because it does not know what salary base the hospital will assign to individuals assigned to perform the duties required by these rules.

Some other rural units of local government may be indirectly impacted insofar as they may administer a special hospital taxing district and, furthermore, only insofar as administrative actions by the special hospital taxing district are allowed or required by local, state, or federal rules, regulations, or statutes. However, these rural units of local government are accustomed to much broader and more complex mandates, such as levying taxes and complying with reimbursement

regulations prescribed by the federal Centers for Medicare and Medicaid Services. Given this insight, the indirect cost of compliance (if any) on some other rural units of local government is expected to be negligible.

2. Cost of compliance effect on small business (ORS 183.336):
a. Estimate the number of small businesses and types of business and industries with small businesses subject to the rule:
The rule will impact only hospitals, none of which meet the statutory definition of small business (ORS 183.336). The rule implements no specific compliance mandates for small businesses.

b. Projected reporting, record keeping and other administrative activities required for compliance, including costs of professional services: **N/A**

c. Equipment, supplies, labor and increased administration required for compliance: **N/A**

How were small businesses involved in the development of this rule?
Persons with small business interests served on the advisory committee mandated to advise the Office for Oregon Health Policy and Research regarding development of this rule, although impact of this rule will not impact small businesses unless amended.

Administrative Rule Advisory Committee consulted?: If not, why?:
Yes. The Health Care Acquired Infection Advisory Committee was used as the advisory committee for these rules. In addition, members of the public and national experts have provided feedback through participation with the committee. The full roster of the committee can be found at http://www.oregon.gov/OHPPR/Healthcare_Acquired_infections.shtml.

Jennifer D. Bittel	**Jennifer Bittel, Rules Coordinator**	5/12/08
Signature	Printed name	Date

CHAPTER 409
DEPARTMENT OF HUMAN SERVICES,
OFFICE FOR OREGON HEALTH POLICY AND RESEARCH

DIVISION 23
HOSPITAL REPORTING

Health Care Acquired Infection Reporting and Public Disclosure

409-023-0000
Definitions

The following definitions apply to OAR 409-023-0000 through 409-023-0035:

(1) "Administrator" means the administrator of the Office for Oregon Health Policy and Research as defined in ORS 442.011, or the administrator's designee.

(2) "ASC" means ambulatory surgical center as defined in ORS 442.015(4) and that is licensed pursuant to ORS 441.015.

(3) "CBGB" means coronary bypass graft surgery with both chest and graft incisions, as defined in the Patient Safety Component Protocol of the National Healthcare Safety Network (NHSN) manual, version January 2008.

(4) "CBGC" means coronary bypass graft surgery with chest incision only, as defined in the Patient Safety Component Protocol of the NHSN manual, version January 2008.

(5) "CDC" means the federal Centers for Disease Control and Prevention.

(6) "CLABSI" means central line associated bloodstream infection as defined in the Patient Safety Component Protocol of the NHSN manual, version January 2008.

(7) "CMS" mean the federal Centers for Medicare and Medicaid Services.

(8) "Committee" means the Health Care Acquired Infections Advisory Committee as defined in ORS 442.838.

(9) "Dialysis facility" means outpatient renal dialysis facility as defined in ORS 442.015(29).

(10) "Follow-up" means post-discharge surveillance intended to detect CBGB, CBGC, and KRPO surgical site infection (SSI) cases occurring after a procedure.

(11) "HAI" means health care acquired infection as defined in ORS 442.838.

(12) "Health care facility" means a facility as defined in ORS 442.015(16).

(13) "Hospital" means a facility as defined in ORS 442.015(19) and that is licensed pursuant to ORS 441.015.

(14) “ICU” means an intensive care unit as defined in the Patient Safety Component Protocol of the NHSN manual, version January 2008.

(15) “KPRO” means knee prosthesis procedure as defined in the Patient Safety Component Protocol of the NHSN manual, version January 2008.

(16) “LTC facility” means long term care facility as defined in ORS 442.015(22).

(17) “Medical ICU” means a non-specialty intensive care unit that serves 80% or more adult medical patients.

(18) “Medical/Surgical ICU” means a non-specialty intensive care unit that serves less than 80% of either adult medical, adult surgical, or specialty patients.

(19) “Surgical ICU means” means a non-specialty intensive care unit that serves 80% or more adult surgical patients.

(20) “NHSN” means the CDC’s National Healthcare Safety Network.

(21) “Office” means the Office for Oregon Health Policy and Research.

(22) “Oregon HAI group” means the NHSN group administered by the Office.

(23) “Patient information” means individually identifiable health information as defined in ORS 179.505(c).

(24) “Person” has the meaning as defined in ORS 442.015(30).

(25) “Procedure” means an NHSN operative procedure as defined in the Patient Safety Component Protocol of the NHSN manual version January 2008.

(26) “Provider” means health care services provider as defined in ORS 179.505(b).

(27) “QIO” means the quality improvement organization designated by CMS for Oregon.

(28) “RHQDAPU” means the Reporting Hospital Quality Data for Annual Payment Update initiative administered by CMS.

(29) “SCIP” means the Surgical Care Improvement Project.

(30) “SCIP-Inf-1” means the HAI process measure published by SCIP defined as prophylactic antibiotic received within one hour prior to surgical incision.

(31) "SCIP-Inf-2" means the HAI process measure published by SCIP defined as prophylactic antibiotic selection for surgical patients.

(32) "SCIP-Inf-3" means the HAI process measure published by SCIP defined as prophylactic antibiotics discontinued within 24 hours after surgery end time (48 hours for cardiac patients).

(33) "Specialty ICU" means an intensive care unit with at least 80% of adults are specialty patients including but not limited to oncology, trauma, and neurology.

(34) "SSI" means a surgical site infection event as defined in the Patient Safety Component Protocol of the NHSN manual, version January 2008.

(35) "State agency" shall have the meaning as defined in ORS 192.410(5).

Stat. Auth.: ORS 442.838, ORS 442.420(3)(d)
Stats. Implemented: ORS 442.838, 442.011, 442.015, 442.400, 192.496, 192.502, 192.410, 179.505

409-023-0005
Review

Unless otherwise directed by the administrator, the committee shall review these rules (OAR 409-023-0000 through 409-023-0035) no later than July 1, 2009 and thereafter at least biennially.

Stat. Auth.: ORS 442.838, 442.420 (3)(d)
Stats. Implemented: ORS 442.838

409-023-0010
HAI Reporting for Hospitals

(1) Hospitals shall begin collecting data for HAI outcome and process measures for the HAI reporting program for services provided on and after January 1, 2009.

(2) Reportable HAI outcome measures are:

(a) SSIs for CBGB, CBGC, and KPRO procedures.

(b) CLABSI in medical ICUs, surgical ICUs, and combined medical/surgical ICUs.

(3) The infection control professional (ICP), as defined by the facility, shall actively seek out infections defined in sections 2(a) and (b) of this rule during a patient's stay by screening a variety of data that may include but is not limited to:

(a) Laboratory;

(b) Pharmacy;

(c) Admission;

(d) Discharge;

(e) Transfer;

(f) Radiology;

(g) Imaging;

(h) Pathology; and

(i) Patient charts, including history and physical notes, nurses and physicians notes, and temperature charts.

(4) The ICP should use follow-up surveillance methods to detect SSIs for procedures defined in section 2(a) of this rule using at least one of the following:

(a) Direct examination of patients' wounds during follow-up visits to either surgery clinics or physicians' offices;

(b) Review of medical records, subsequent hospitalization records, or surgery clinic records;

(c) Surgeon surveys by mail or telephone;

(d) Patient surveys by mail or telephone; or

(e) Other facility surveys by mail or telephone.

(5) Others employed by the facility may be trained to screen data sources for these infections, but the ICP must determine that the infection meets the criteria established by these rules.

(6) The HAI reporting system for HAI outcome measures shall be NHSN. Each Oregon hospital shall comply with processes and methods prescribed by CDC for NHSN data submission. This includes but is not limited to definitions, data collection, data reporting, and administrative and training requirements. Each Oregon hospital shall:

(a) Join the Oregon HAI group in NHSN.

(b) Authorize disclosure of NHSN data to the Office as necessary for compliance of these rules including but not limited to summary data and denominator data for all SSIs, the annual hospital survey and data analysis components for all SSIs, and summary data and denominator data for all medical ICUs, surgical ICUs, and combined medical/surgical ICUs.

(c) Report its data for outcome measures to NHSN no later than 30 days after the end of the collection month.

(7) Each Oregon hospital shall report on a quarterly basis, beginning January 1, 2009, the following HAI process measures:

(a) SCIP-Inf-1;

(b) SCIP-Inf-2; and

(c) SCIP-Inf-3.

(8) The reporting system for HAI process measures shall be the RHQDAPU program as configured on July 1, 2008. Each Oregon hospital shall:

(a) Comply with reporting processes and methods prescribed by CMS for the RHQDAPU program. This includes but is not limited to definitions, data collection, data reporting, and administrative and training requirements; and

(b) Report data quarterly for HAI process measures. Data must be submitted to and successfully accepted into the QIO clinical warehouse no later than 11:59 p.m. central time, on the 15th calendar day, four months after the end of the quarter.

Stat. Auth.: ORS 442.838, 442.420(3)(d)
Stats. Implemented: ORS 442.838, 442.405

409-023-0015
HAI Reporting for Other Health Care Facilities

ASCs, dialysis facilities, and LTC facilities shall begin collecting data for the HAI reporting program for services provided on and after January 1, 2010 pursuant to rules amended no later than July 1, 2009.

Stat. Auth.: ORS 442.838, ORS 442.420(3)(d)
Stats. Implemented: ORS 442.838, ORS 442.405

409-023-0020
HAI Public Disclosure

(1) The Office shall disclose to the public updated facility-level and state-level HAI rates at least biannually beginning in January 2010 and at least quarterly beginning in January 2011.

(2) The Office may disclose state-level and facility-level HAI data including but not limited to observed frequencies, expected frequencies, proportions, and ratios beginning in January 2010.

(3) The Office shall summarize HAI data by facilities subject to this reporting in an annual report beginning in January 2010. The Office shall publish the annual report no later than April 30 of each calendar year.

(4) The Office shall disclose data and accompanying explanatory documentation in a format which facilitates access and use by the general public and health care providers.

(5) The Office may use statistically valid methods to make comparisons by facility, and to state, regional, and national statistics.

(6) The Office shall provide a maximum of 30 calendar days for facilities to review facility reported data prior to public release of data.

(7) The Office shall provide facilities the opportunity to submit written comments and may include any submitted information in the annual report.

(8) Pending recommendations from the committee, the Office may publish additional reports intended to serve the public's interest.

Stat. Auth.: ORS 442.838, 442.420(3)(d)
Stats. Implemented: ORS 442.838, 442.405, 192.496, 192.502, 192.243, 192.245

409-023-0025
HAI Data Processing and Security

(1) The Office shall obtain hospital outcome measure data files directly from NHSN at least quarterly.

(2) The Office shall obtain hospital process measure data files from the CMS hospital compare web site at least quarterly.

(3) The Office shall calculate state-level and facility-level statistics to facilitate HAI public disclosure. These statistics may include but are not limited to observed frequencies, expected frequencies, proportions, rates, and ratios. The Office shall make public the methods used to calculate statistics and perform comparisons.

(4) The Office shall use statistically valid risk adjustment methods recommended by the committee including but not limited to NHSN methodology.

(5) The Office shall undertake precautions to prevent unauthorized disclosure of the raw data files. These precautions include but are not limited to:

(a) Storing the raw data files on the internal storage hardware of a password-protected personal computer that is physically located within the Office;

(b) Restricting staff access to the raw data files;

(c) Restricting network access to the raw data files; and

(d) If applicable, storing patient information within a strongly-encrypted and password-protected virtual drive or using other methods to reliably achieve the same level of security.

Stat. Auth.: ORS 442.838, 442.420 (3)(d)
Stats. Implemented: ORS 442.838, 192.496, 192.502

409-023-0030
Prohibited Activities

Unless specifically required by state or federal rules, regulations, or statutes, the Office is prohibited from:

(1) Disclosing of patient information;

(2) Intentionally linking or attempting to link individual providers to individual HAI events; and

(3) Providing patient-level or provider-level reportable HAI data to any state agency for enforcement or regulatory actions.

Stat. Auth.: ORS 442.838, 442.420(3)(d)
Stats. Implemented: ORS 442.838, 192.496, 192.502

409-023-0035
Compliance

(1) Health care facilities that fail to comply with these rules or fail to submit required data shall be subject to civil penalties not to exceed $500 per day per violation.

(2) The Office shall annually evaluate the quality of data submitted, as recommended by the committee.

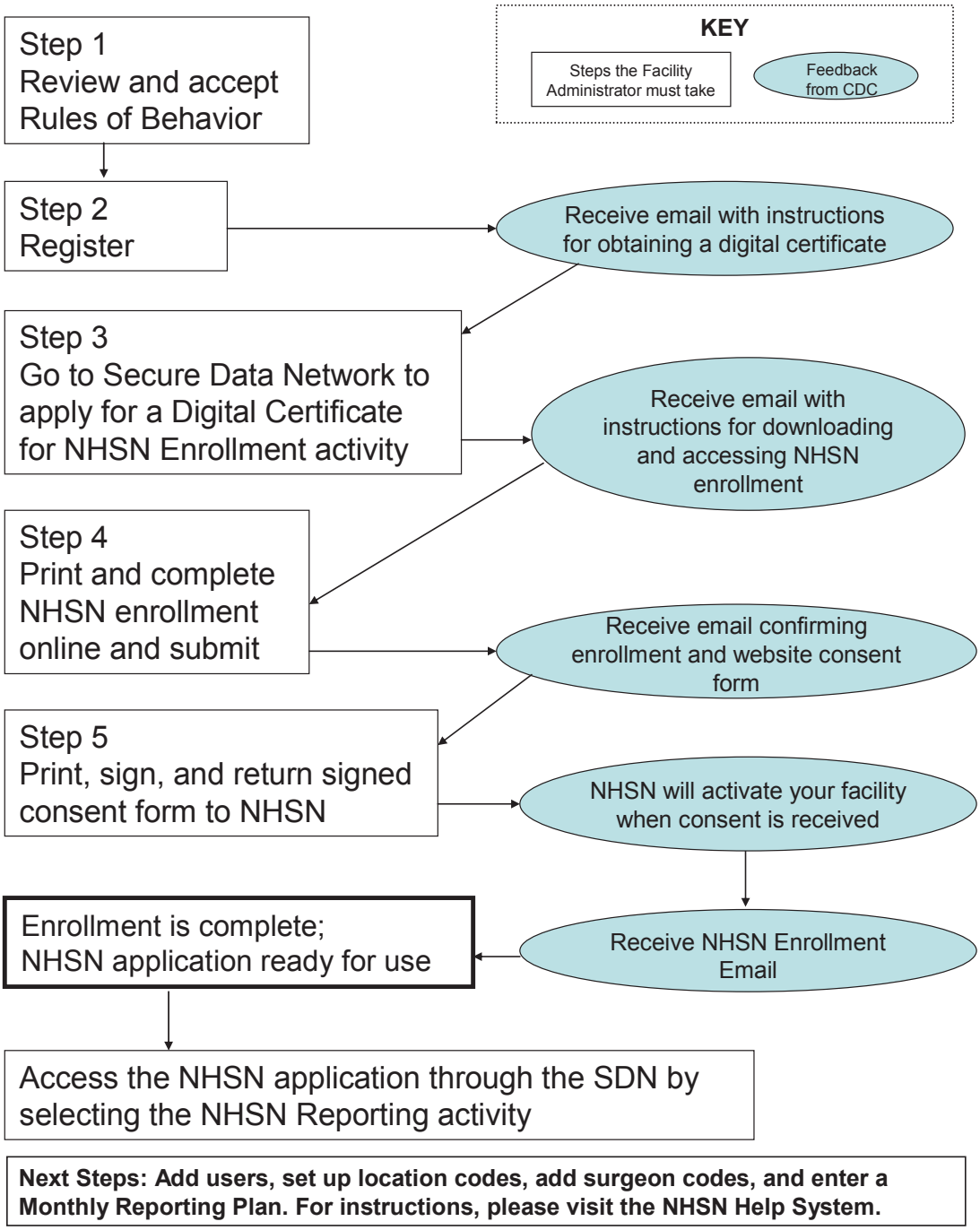
Stat. Auth.: ORS 442.445, 442.420(3)(d)
Stats. Implemented: ORS 442.445

NHSN Facility Administrator Enrollment Guide

DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS FOR DISEASE CONTROL AND PREVENTION
SAFER • HEALTHIER • PEOPLE™

TABLE OF CONTENTS

How do I get started in NHSN?

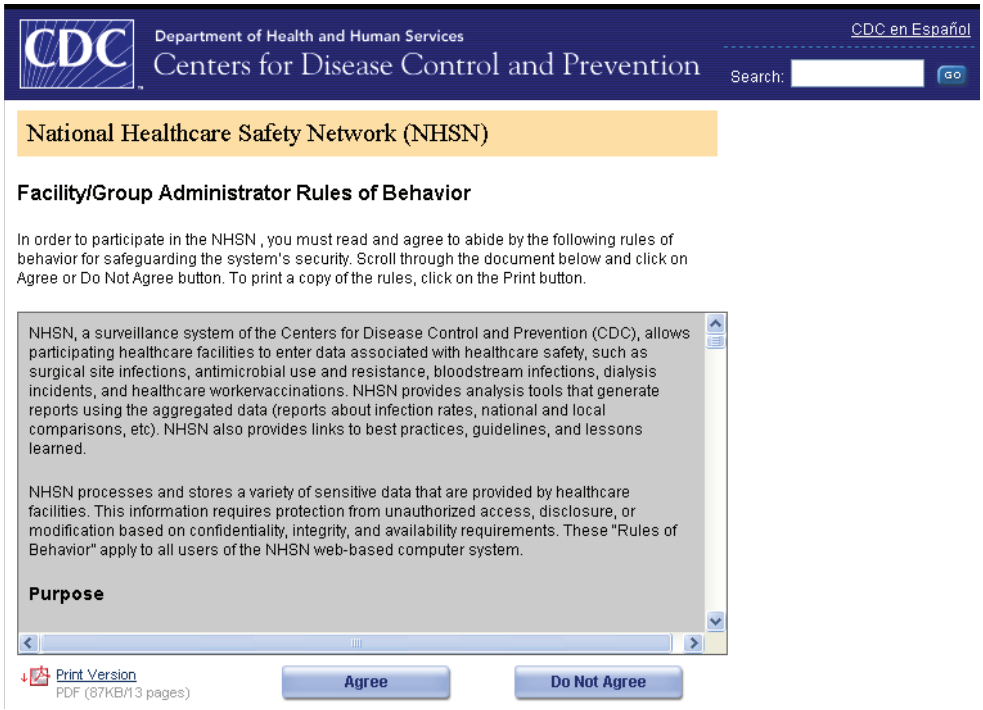


Next Steps: Add users, set up location codes, add surgeon codes, and enter a Monthly Reporting Plan. For instructions, please visit the NHSN Help System.

DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS FOR DISEASE CONTROL AND PREVENTION
SAFER·HEALTHIER·PEOPLE™

Step 1. Read the NHSN Rules of Behavior

The first step to NHSN Enrollment is for the person who will serve as the NHSN facility Administrator* to access and read the NHSN Rules of Behavior from the NHSN portal page http://www.ncid.cdc.gov/RegistrationForm/admin.htm



A copy of the NHSN Rules of Behavior may be printed by clicking the **Print** link at the bottom of the screen.
To indicate agreement with the terms and conditions as stated in the NHSN Rules of Behavior, click **Agree** and you will be guided to the NHSN Registration page. Otherwise, click **Do Not Agree** and discontinue enrollment.

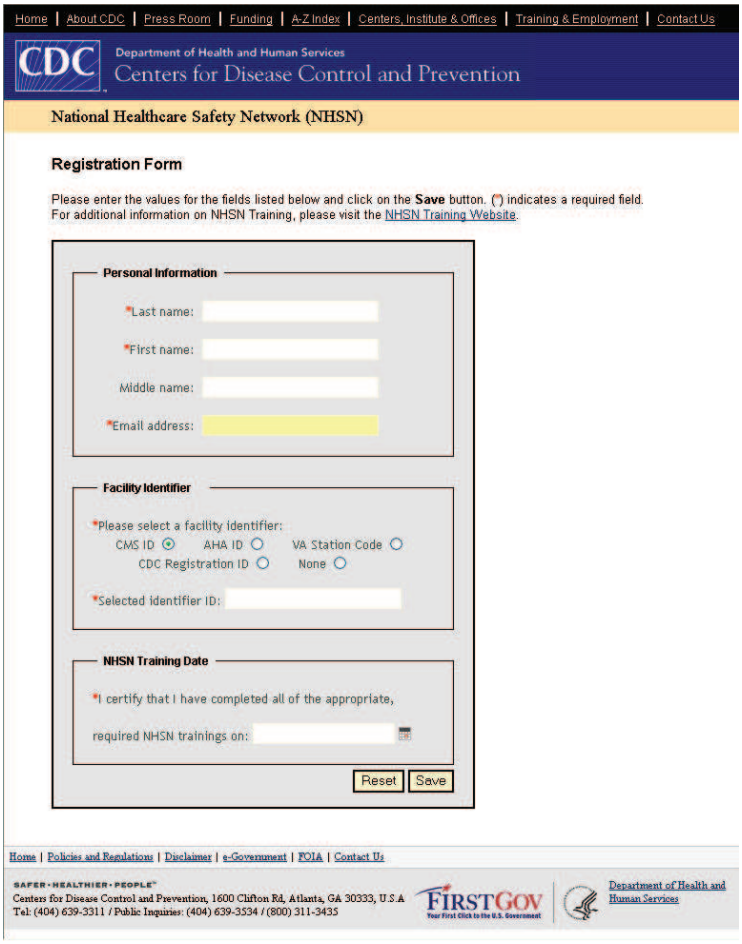
---

* NOTE: The person designated as the **NHSN Facility Administrator** is the person who will have all rights to your data and the ability to create other users of the NHSN at your facility and confer rights to them. This person will also have the ability to nominate groups, that is, entities with which your hospital wants to share some/all of its data (e.g., state or county health department, corporate headquarters). Therefore, this role should be given to an individual who has the authority to perform these functions within your hospital's organizational structure. In many hospitals participating only in the NHSN Patient Safety Component, this will likely be the lead Infection control Professional (ICP). In that case, the NHSN Facility Administrator may also be designated as the NHSN Patient Safety Primary Contact Person. For facilities participating only in the NHSN Healthcare Personnel Safety Component, the person responsible for the occupational health functions is a good candidate for both NHSN Facility Administrator and NHSN Healthcare Personnel Safety Primary contact Person. For facilities participating in both NHSN Patient and Healthcare Personnel Safety Components, the NHSN Facility Administrator should be a person with authority in both the infection control and occupational health departments.

Step 2. Register with NHSN

At the Registration Form page, you will be asked to provide a few key pieces of information, including:

- The name of the NHSN Facility Administrator
- Email address for the NHSN Facility Administrator
- Facility identifier
    - You will need either your hospital's American Hospital Association (AHA) ID# or CMS Provider ID# (may also be called HCFA or Medicare#) to proceed; VA hospitals will need their VA Station Code to proceed.
- Training completion date
    - **NOTE:** If you have participated in a face-to-face NHSN training session endorsed by the CDC (i.e., from State groups or CDC day training), we recommend that you also review our training sessions, especially for those protocols and topics which may not have been covered during CDC-endorsed trainings. When registering as a user of NHSN, you may enter the date of the CDC-endorsed training you attended as the training completion date.



Enter the correct information and click **Save.**

NOTE: To ensure that information sent by email is not blocked by your organization's anti-spam program, please contact your IT department and request that they specifically allow phintech@cdc.gov and nhsn@cdc.gov to get through.

After CDC receives your completed registration, you will receive the following email:

Welcome! You are now registered in the National Healthcare Safety Network (NHSN).

In order to begin the NHSN enrollment process, you will need to obtain and install a digital certificate onto your computer.

Follow the instructions in the document "NHSN Facility Administrator Enrollment Guide" beginning at Step 3, to obtain and install the digital certificate so that you will be able to access the NHSN application through CDC's Secure Data Network (SDN). This document can be accessed at: http://www.cdc.gov/ncidod/dhqp/nhsn_documents.html .

From the Centers for Disease Control and Prevention - Digital ID Enrollment page, https://ca.cdc.gov, you will be prompted for the enrollment password, which is: !cdc_sdn_apply! (Be sure to include the exclamation points and use lower case and underscores.) Follow the onscreen instructions to apply for a digital certificate.

During the process, you will be prompted to select a Program and a Program-specific Activity.

For Program, select: **National Healthcare Safety Network (NHSN)**
For Activity, select: **NHSN Enrollment**

VERY IMPORTANT: After you obtain and install your digital certificate (Step 3d in the NHSN Facility Administrator Enrollment Guide), access the SDN (https://sdn.cdc.gov), enter your challenge phrase and select NHSN Enrollment from the list in the upper left corner titled "My Applications". This will launch the NHSN Enroll Facility page. ***Be sure to indicate yourself as the NHSN Facility Administrator.***

If you have difficulties obtaining a digital certificate, please contact SDN at 800-532-9929 or 770-936-3636 or PHINTech@cdc.gov.

If you have any questions about NHSN, please contact us at 800-893-0485 or nhsn@cdc.gov. Information on NHSN is also available on the members' website at http://www.cdc.gov/ncidod/dhqp/nhsn_members.html .

Step 3. Obtain your Digital Certificate

Before you apply for a digital certificate, make sure you have administrative rights for your computer and you have the following system requirements:

System Requirements

Intel-based system with a 486 CPU or greater
Windows 98, Windows NT 4.0 or greater
Internet connectivity
Internet Explorer 5.x or greater
Browser cipher strength – 128 bit or greater

Administrative Rights

You must have administrative rights on your computer before you can apply for a digital certificate. To determine if you have administrative rights do the following steps or ask your IT support to verify them for you. These steps vary depending on the type of system you have.

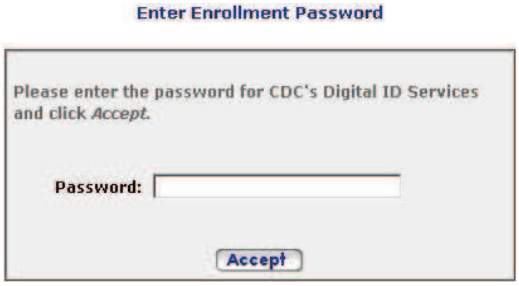
For Windows XP

- Click **Start** > **Control Panel** > **Administrative Tools** > **Computer Management**. The **Computer Management** dialog opens.
- Expand **Local Users and Groups** and then select **Groups**. A list of **Groups** appears in the panel on the right.
- Open the **Administrators** Group. The **Administrators Properties** dialog opens.
- Select the **General** tab and then verify your user ID appears in the **Members**.
- If your user ID does not appear, contact your IT Support to give you privileges.

NOTE: If you have Windows XP with Service Pack 2 installed, this can cause problems in installing the certificate. It will be necessary to open the browser and click **Tools**, then either disable the pop-up blocker or add https://ca.cdc.gov/ and https://sdn.cdc.gov/ to the list of sites where pop-ups are allowed. Then, also under **Tools**, click **Internet Options** > **Security**. Highlight Internet and click **Custom Level**. Make sure that the option for **"Automatic Prompting for ActiveX controls"** is set to "enable". It will also be necessary to disable any pop-up blockers, such as those that come with Norton Anti-Virus or McAfee anti-virus software**.**

Access the Secure Data Network and Accept Subscriber Agreement

- Go to https://ca.cdc.gov. The **Centers for Disease Control and Prevention – Digital ID Enrollment** page appears.



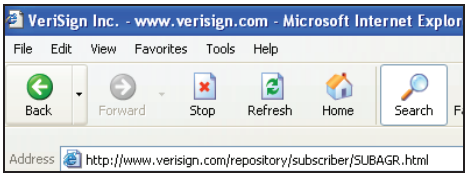
- In the Password field, type **!cdc_sdn_apply!** And then click **Accept**. Information about system requirements and digital ID certificates appears. Remember that passwords are case sensitive.

- Scroll to the bottom of the page to the Digital ID Subscriber Agreement heading, go to the second paragraph which reads:
  "Complete terms for the VeriSign CPS and Digital ID Subscriber Agreement can be found here."

- Click on the **here** link under the **Digital ID Subscriber Agreement** heading on the website. The VeriSign **Products and Services** page appears.

- Under the **Digital ID Practices** heading, click on **Subscriber Agreements**, then under the **Managed PKI Subscriber Agreements** heading, click on **Digital ID Subscriber Agreement.**

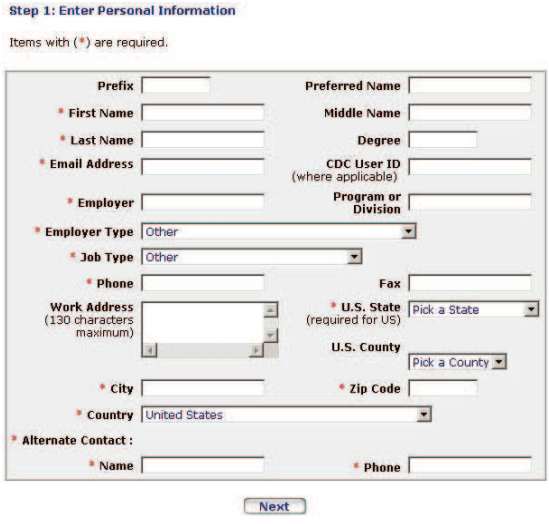
- Read the **Client ID Subscriber** agreement and then click the **Back** button on your browser three times to go back to **the CDC Digital ID Enrollment** page.



- Click the **Enroll** button. The enrollment form appears.

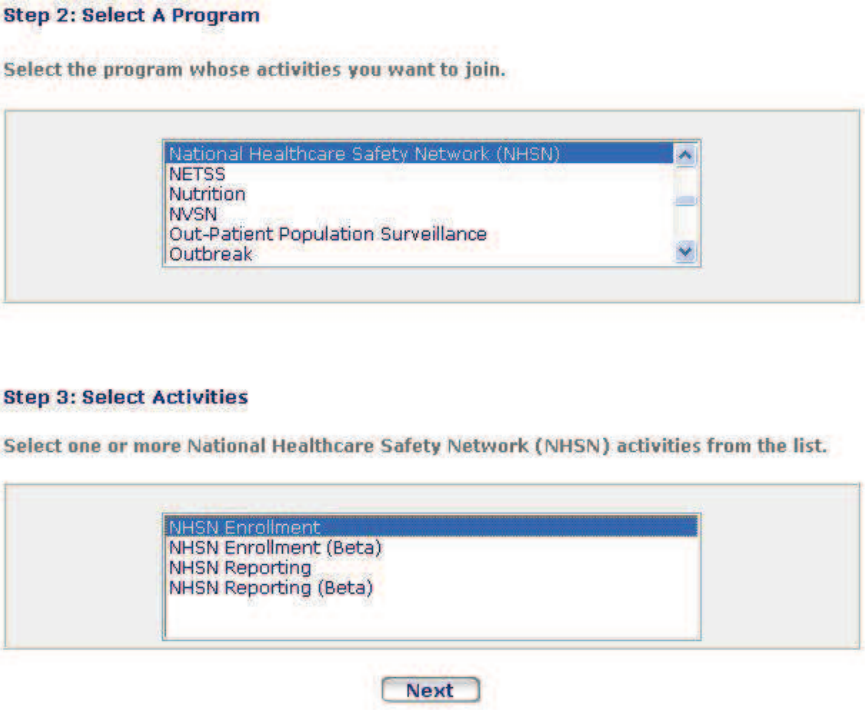
3a. Apply for a CDC Digital ID Certificate

Digital certificates ensure that you and the CDC are communicating privately and securely. They are also expensive and are paid for by your federal tax dollars. You will need to create a password (called a challenge phrase) during this process



- All fields with a red asterisk are required on the first page of the enrollment form. Make sure you enter your work email address, not your personal email address. The information you need to install your digital certificate will be sent to the email address you indicate. If you submit an email address with an error in it, you will not be sent a digital certificate. NOTE: Be sure to use the same email address for each step in the SDN and NHSN enrollment process.

- A pop-up message appears. Verify that the email address listed in the message is correct and then click **OK**. If your email address is incorrect, click Cancel, change your email address, and then click **Next.** The **Request Activities** page appears:



- From the first list box, select **National Healthcare Safety Network (NHSN).**

- From the Select Activities box, select **NHSN Enrollment**. Click **Next**.

3b. Create and Safely Store your Challenge Phrase

For security, you will create a challenge phrase (password) that you will use every time you access SDN (this challenge phrase is different from the password you used to log on to the SDN enrollment site). You will use this challenge phrase along with your Digital ID to authenticate yourself as an SDN user.

To make sure you remember your challenge phrase, we recommend you store your challenge phrase in a safe place. Open MS Word or Notepad and create a file – type the challenge phrase and then save the file, or write the challenge phrase on a piece of paper and put it in a secure place such as your wallet or a locked desk drawer. Make sure you write down which letters are upper case and which are lower case. The challenge phrase is case sensitive.

Use the following guidelines to create your challenge phrase:

- Be at least eight characters long
- Contain only English letters and numbers
- Uses one of more of the following symbols:

  - + : ‘ .

- Cannot contain any part of your name or email address
- Cannot spell a word unless the word has three or more numbers or symbols before or after the word or the word has numbers or symbols within the word
- Cannot contain more than two consecutive characters
- Contain at least four different numbers or letters
- Challenge phrases are case-sensitive. Note the letters that are upper and lower case.

To enter your challenge phrase

- In the **Challenge phrase** field, type your challenge phrase.

- In the **Confirm** field, type your challenge phrase exactly the same way you typed it in the **Challenge Phrase** field.

- BEFORE you click the **Next** button, open MS Word or Notepad and create a file. Make a note of the letters that are upper and lowercase. Type the challenge phrase and then save the file. If you do not want to create a file, write down the challenge phrase, note the letters that are upper or lower case, and then safely store the note in a locked drawer or your wallet.

- Click **Next**. The **Digital Certificate Request Received** message appears.

- Within 12-72 hours, you will receive an email with more instructions. Check your email daily. If you do not receive and email within 72 hours, contact CDC SDN Support at **(800)532-9929** option 1 or 770-216-1276 or PHINTech@cdc.gov.

3c. Check your Email

- You will receive an email from **CDC SDN Enrollment.** The subject line will read "Action Required – Your CDC Digital Certificate is Ready to Install" and the body of the message will look similar to the following:

```
Your request for a CDC digital certificate has been approved. The next step is
the installation of your digital certificate. Your computer settings may be
different from other computers. These differences may make installing your
digital certificate more difficult than we would like. We are working to make
this process easier.

We recommend that your IT Specialist install the digital certificate for you.
We have provided instructions for the IT Specialist at
https://ca.cdc.gov/sdncode/sdnapp/doc/DigitalCertificateInstallation.htm. After
reviewing these instructions, your IT Specialist can begin the process of
installing your digital certificate by going to your installation link.

    Digital Certificate Installation Link:
    https://ca.cdc.gov/sdncode/sdnapp/servlet/CertServlet?usertoken=xxxx

If you do not have an IT Specialist or need further information, contact CDC
SDN Support:
    e-mail:    PHINTech@cdc.gov
    telephone: 1-800-532-9929 and select option 1
```

- NOTE: Please ask your IT staff to add https://*.cdc.gov/ and https://*.verisign.com/ to the list of trusted sites under Tools>Internet Options>Security>Trusted Sites. This will make the installation process go smoother.

- Before you open the link in your email, open the MS Word or Notepad file you created (or open the note you wrote to yourself and stored in a locked drawer or your wallet).

- When you are certain that you have Administrative Rights to your computer (see Step 3), click on the link provided in your email. The **Digital ID Enrollment** page appears.

- Type your challenge phrase (remember that the letters are case-sensitive) and then click **Login**. The **Confirm Personal Information** page appears.

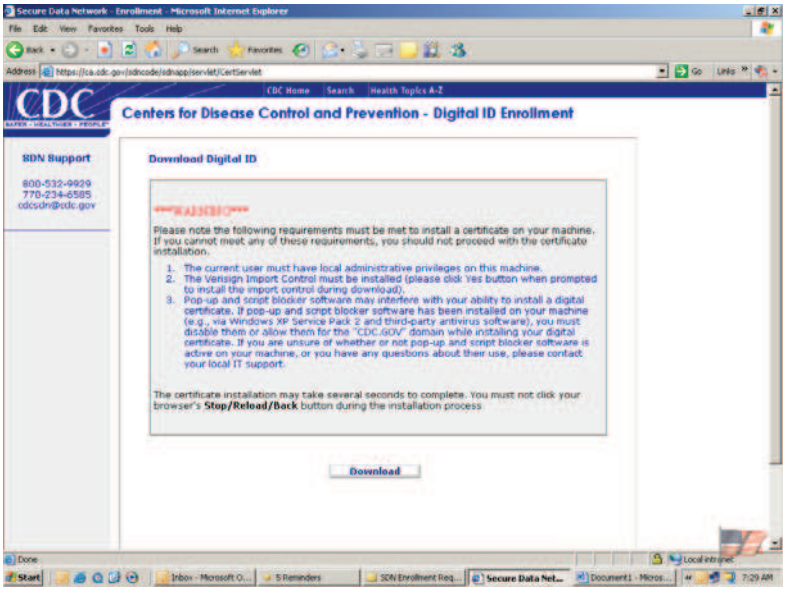
- **Verify your information and do one of the following:**

    - If your information is correct, click **Confirm**. The **Download Digital ID** page appears. Proceed with directions "To Download and Install Your Digital ID Certificate Using Internet Explorer".

- If you need to change your information, click **Update,** make changes and then click **Submit.** Your request will be reviewed and you will receive another email within 12-72 hours with further instructions.

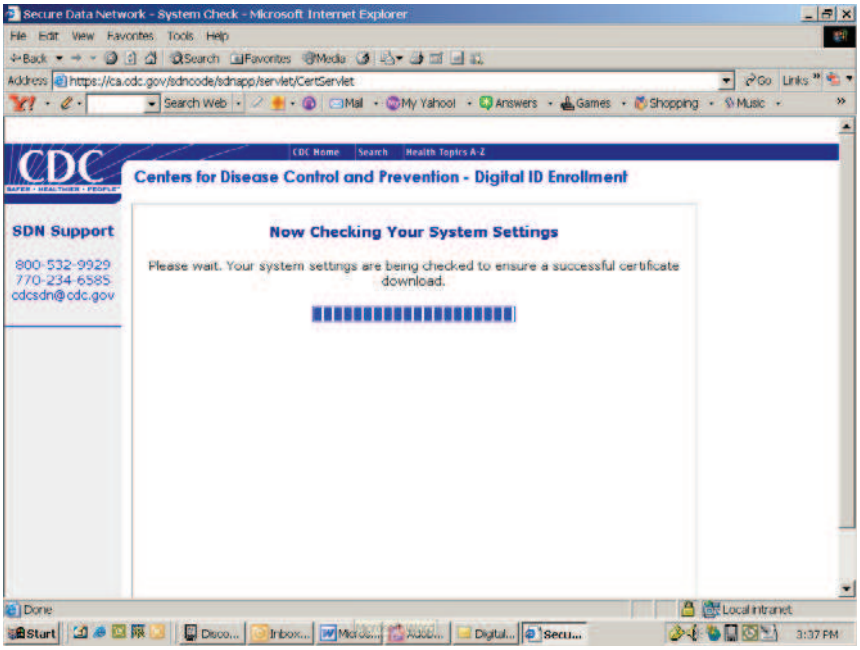
3d. Download and Install your Digital ID Certificate Using Internet Explorer

After you have confirmed the information is correct in the Personal Information page, the **Download Digital ID** page appears.

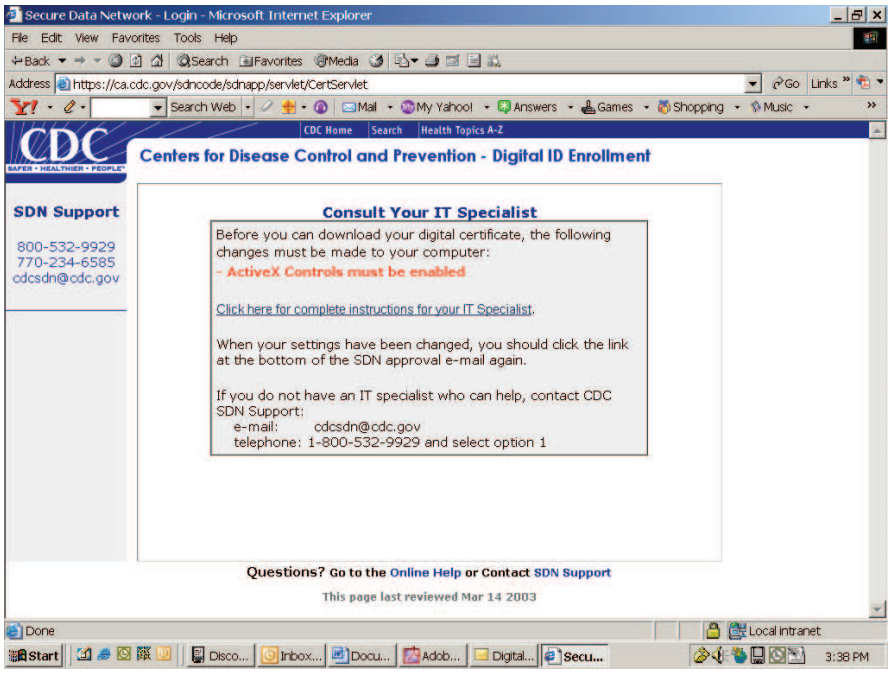


To download your digital ID certificate onto your computer, do the following:

- From the **Download Digital ID** page, click the **Download** button. Prior to downloading, the SDN will check your system settings to ensure that you will be able to download your digital certificate.

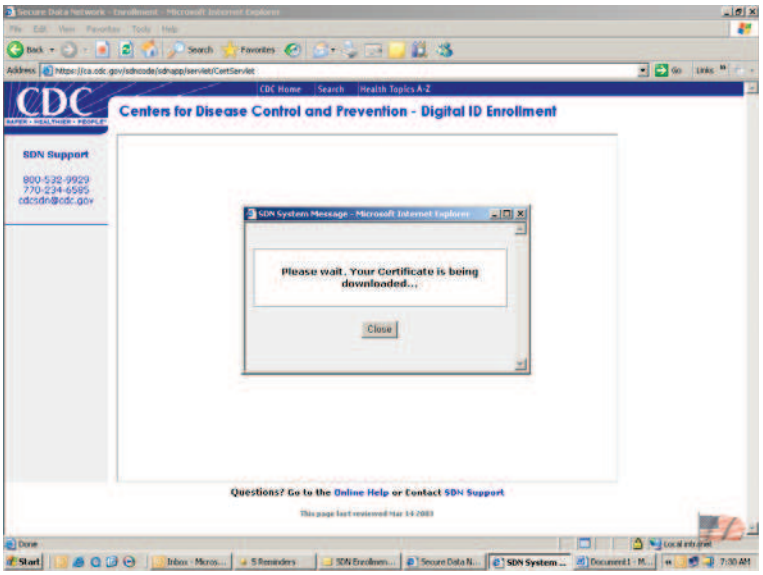


- If your system settings are not correct, you will receive a message similar to the following:



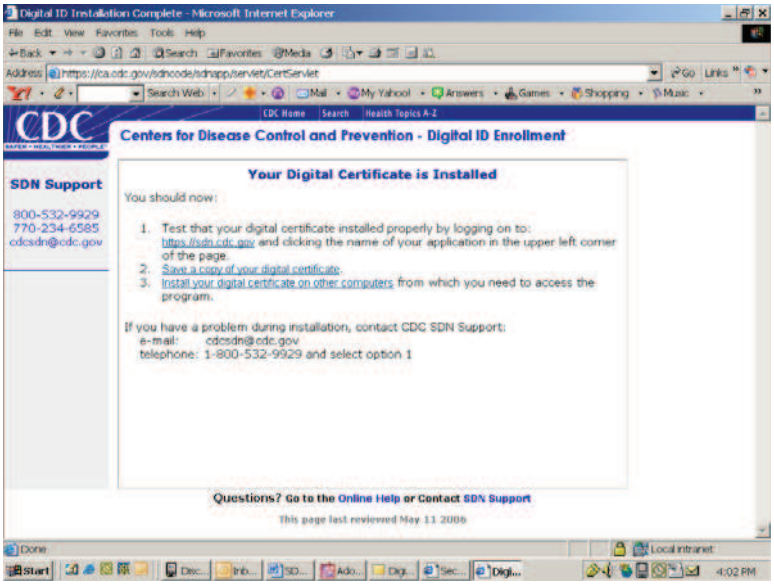
If you receive this message, be sure to contact your IT specialist before attempting to download your digital certificate again.

- If your system settings are correct, the SDN will automatically begin downloading your digital certificate. Please wait while your digital certificate is downloading.



- You will receive a Security Warning message that asks if you want to install and run VeriSign Import Control. Click **Yes**.

- You will receive the following message, which indicates your digital ID certificate was successfully downloaded and installed:



- You should stop here and make a copy of your digital certificate (see 3e below). NOTE: If you do not make a backup copy of your digital certificate, you will need to repeat the SDN enrollment process and apply for a new digital certificate should you need to move to a new computer or should your computer crash. There is no other backup copy of your digital certificate besides the one you create.

- Your digital certificate will expire one year from the date of its original installation. You will receive an email from the NHSN with instructions on how to apply for a new digital certificate thirty days prior to your digital certificate's expiration. When you apply for a new digital certificate, you may use the same challenge phrase.

Verify that your digital certificate was installed:

Please review the following information with your IT staff in order to verify that your certificate was installed properly, and for suggestions on what may need to be modified if it was not installed.

1. Click Tools, Internet Options, Content, and Certificates.
2. Locate and highlight your certificate under the Personal tab and click View.
3. Click the tab for Details.
4. Locate and highlight the line "Subject".
5. Find the Employee ID number which corresponds to the SDN user key.
6. Reference this number when contacting SDN support.

If a certificate is there, try accessing https://sdn.cdc.gov/ .

If no certificate shows up when you follow these steps, then the certificate was not successfully installed. NOTE: If an administrator logged in for the user to download the certificate, have that person log back in and check to see if the certificate was installed under the admin profile. Please show the portion of this note at the very bottom, to someone on your IT staff.

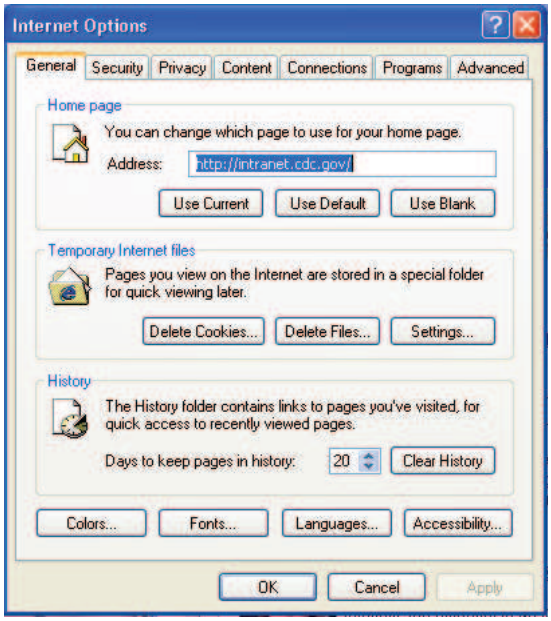
If no certificate issued in your name can be found, you will need to reapply. If this has happened more than once, please have your IT staff contact the SDN support before attempting the next download.

3e. Make a Backup Copy of your Digital ID Certificate

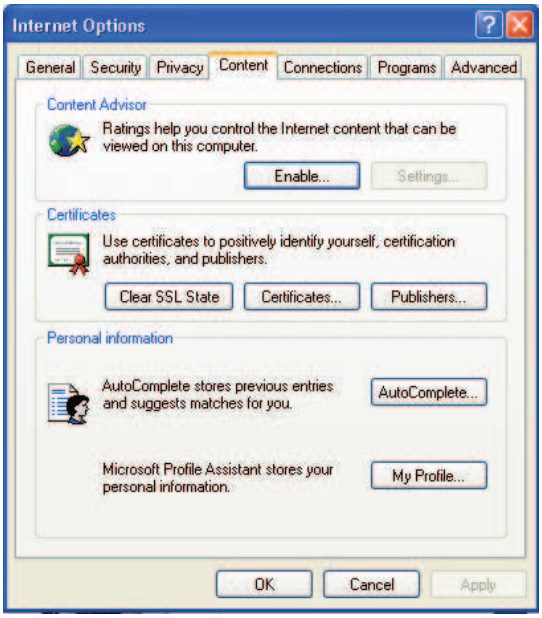
Digital ID certificates are expensive and you pay for them with your federal tax dollars. To minimize the cost of replacing certificates, we strongly recommend you create a copy of your digital ID certificate by saving it to an external storage device (e.g., floppy disk, CD, "thumb drive"). This procedure is also called "backing up" or "exporting" your certificate.

- If you are looking at the Congratulations message, your Internet Explorer should already be open. If not, open Internet Explorer: Click **Start** > **All Programs** > Internet Explorer.

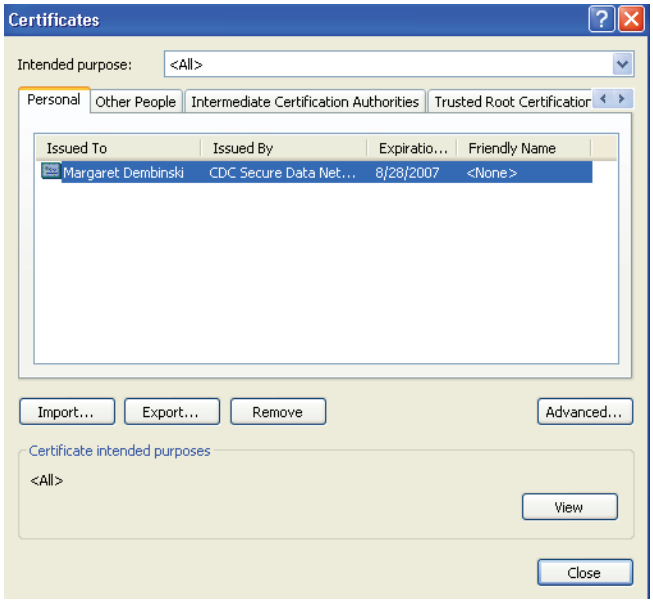
- From the **Tools** menu, select **Internet Options**. The **Internet Options** dialog opens and looks similar to the following:



- Select the **Content** tab. Your **Internet Options** dialog box should look like the following:



- Click on the **Certificates** button. The **Certificates** dialog box opens:

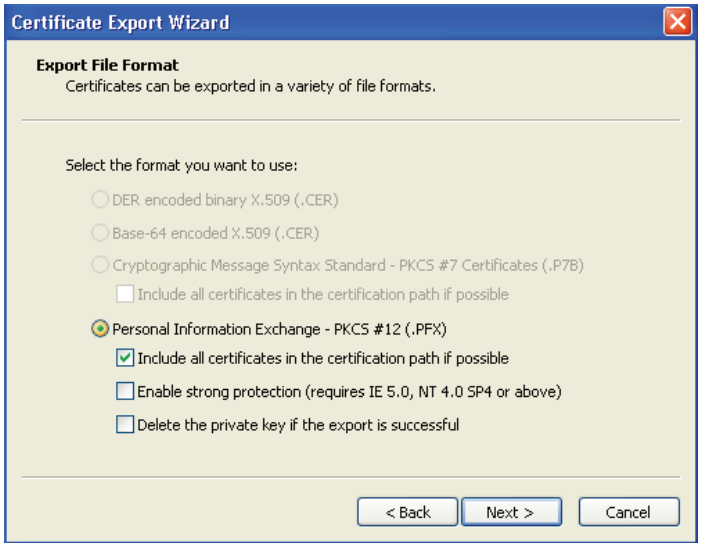


- If you have more than one certificate, look at the date in the **Expiration Date** column and the name in the **Issued To** column. Select the certificate which has the appropriate date and name, and then click **Export**. The **Certificate Export Wizard** dialog box opens.

- Click **Next**

- Select the **"Yes, export the private key"** radio button.

- Click **Next**. Your **Certificate Explorer Wizard** should look similar to the following:

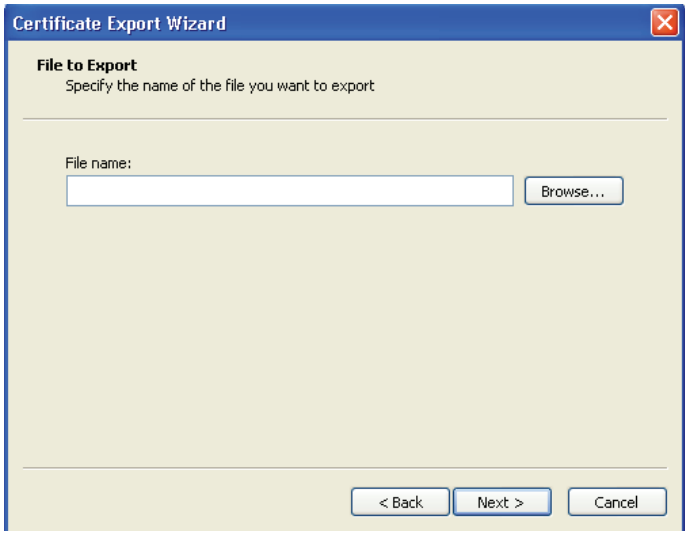


- Check "**Include all certificates in the certification path if possible"** and deselect (uncheck) the "**Enable strong protection"** and **"Delete the private key if the export is successful"** check boxes, then click **Next.**

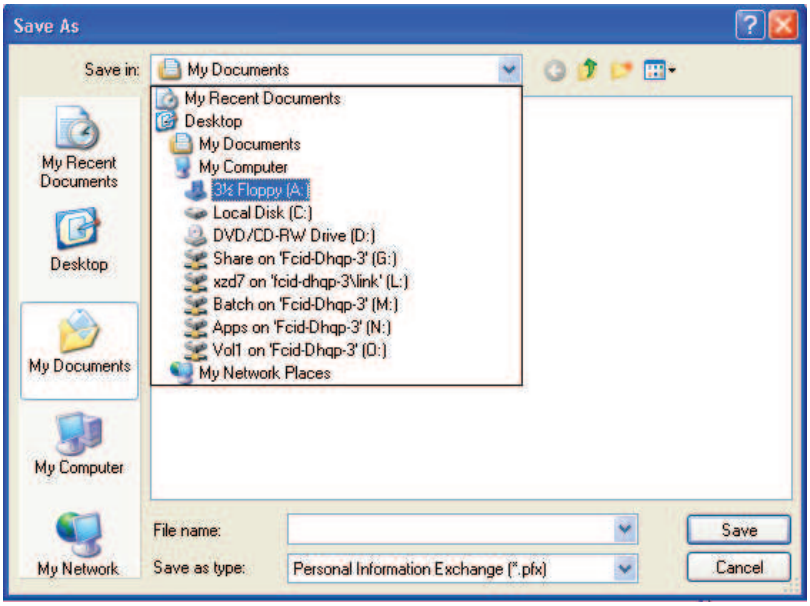
- The password dialog appears:

- We recommend you use the challenge phrase that you created for the original digital certificate for this backup copy of the digital certificate. Type your password in the **Password** and **Confirm Password** fields.

- Click **Next.** The **File to Export** dialog opens.



- Click the **Browse** button and navigate to an external storage device, (e.g., floppy disk, CD, "thumb drive"). When you click the **Browse** button, the **Save As** dialog box appears and looks similar to the following:



- Select the appropriate drive for your external storage device, type **sdncert** in the file name field at the bottom of the **Save As** dialog and then click **Save.** The **Certificate Export Wizard** appears and lists the location of the cert as **C:\SDN Certificate\sdncert.pfx**.

- Click **Next**, then click **Finish**. A **Certificate Export** message appears which reads **"The export was successful"**.

- Click **OK**. The **Certificates** dialog is still open. Click **Close.**

- The **Internet Options** dialog is still open. Click **OK.**

- Remove the external storage device from your computer, label it **SDN Digital ID Certificate** and then store it in a safe place. Keep your password and the certificate separate.

3f. Installing your Digital ID Certificate on Another Computer

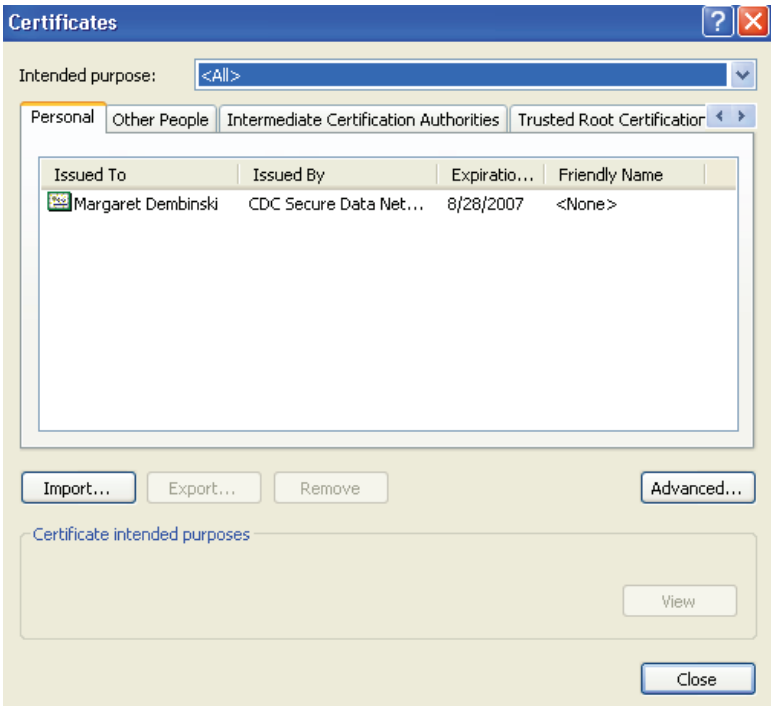
- If you are installing your digital ID certificate onto a computer other than the computer to which you originally downloaded it, or restoring your digital ID certificate on the original computer, make sure you have administrative privileges on the second computer and that the second computer meets the system requirements. See **System Requirements** on page 4.

- Open Internet Explorer. Click **Start** > **All Programs** > **Internet Explorer**.

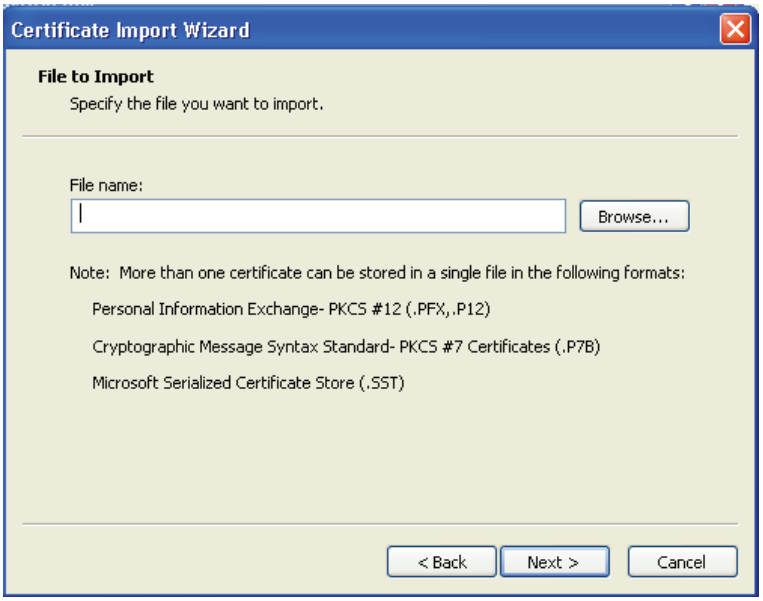
- Insert the external storage device with the backup digital ID certificate into the computer onto which you want to install the certificate.

- From Internet Explorer, click on the **Tools** menu and then select **Internet Options**. The **Internet Options** dialog opens and looks similar to the following:

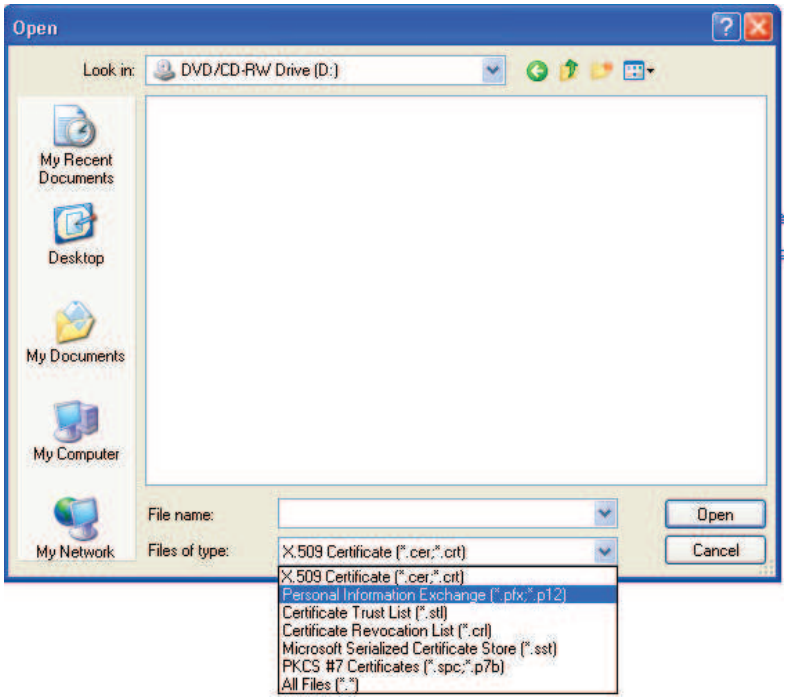
- Select the **Content** tab and then click on the **Certificates** button. The Certificates dialog opens and looks similar to the following:



- Click the **Import** button. The **Certificate Wizard Import** dialog appears. Click the **Next** button. The **File to Import** panel appears and looks similar to the following:

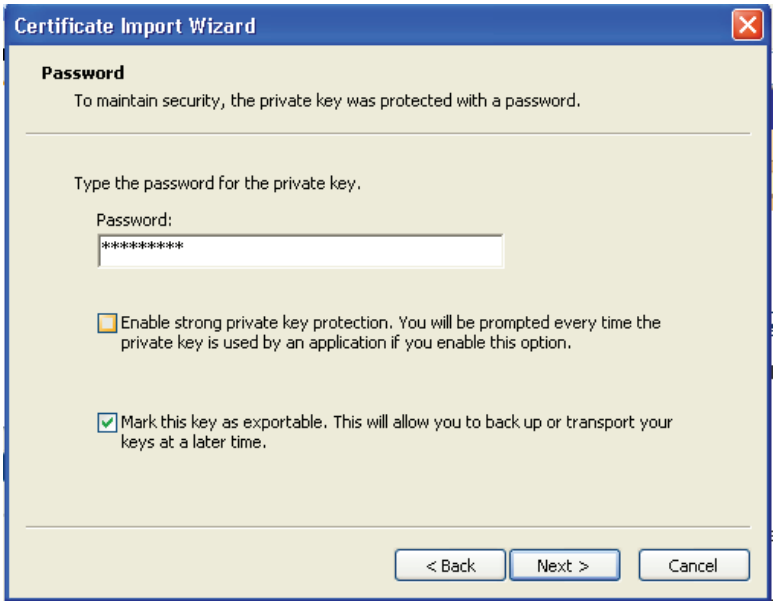


- Click the **Browse** button and then navigate to the appropriate drive for your external storage device.



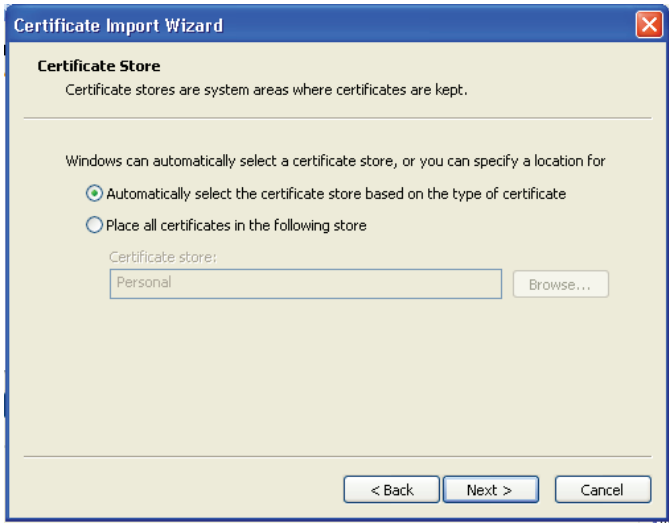
- Click on the **Files of type** list box and select **Personal Information Exchange (*.pfx;*.p12)**. Your certificate should appear.

- Select the certificate and then click the **Open** button. When the **File to Import** panel appears, click **Next.** The **Password** panel appears in the **Certificate Import Wizard** and looks similar to the following:



- Type the password and check the box next to "**Mark this key as exportable"** and then click **Next**.

- The **Certificate Store** panel appears and looks similar to the following:



- Select the **"Automatically select the certificate store based on the type of certificate"** radio button and then click **Next**. The **Completing the Certificate Import Wizard** appears.

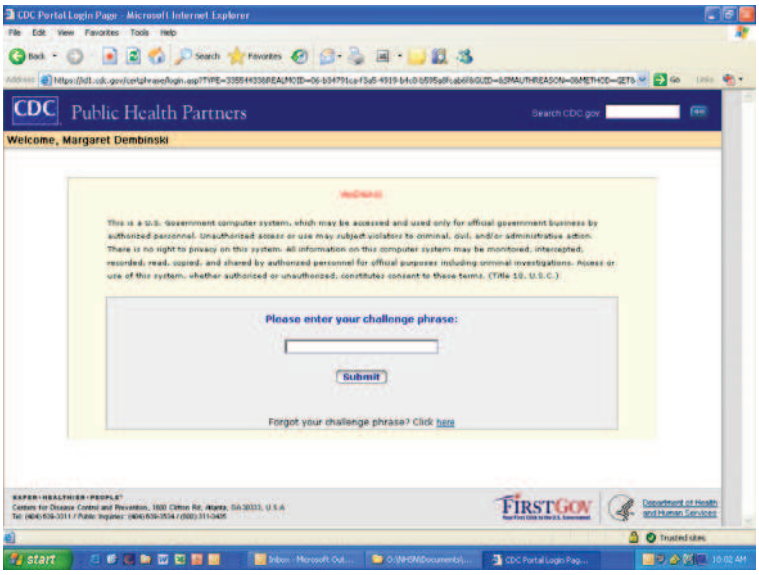
- Click **Finish.** You will receive a message that reads, **"The import was successful."** Click **OK**, close the **Certificates** dialog, and then click **OK** to close the **Internet Options** dialog.

Step 4. Enroll in NHSN

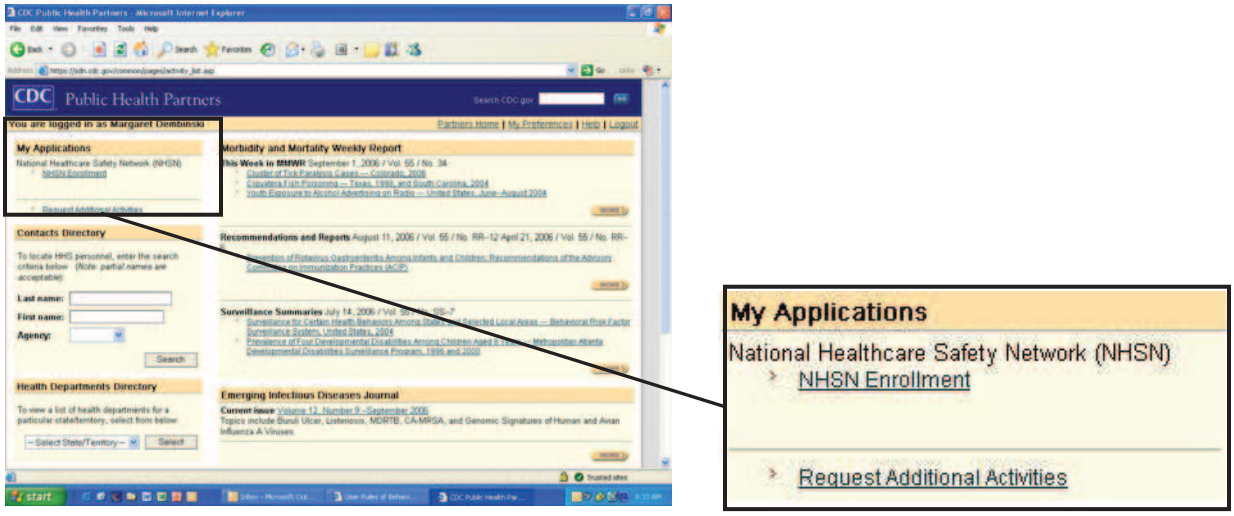
Once you have successfully downloaded and installed your digital certificate, you can access NHSN by going to the SDN website at: https://sdn.cdc.gov

When you arrive at the SDN website (called the CDC Public Health Partners page), you may want to bookmark the page, either individually or in a special NHSN bookmark folder. If you are unsure how to bookmark a web page, please contact your IT department for assistance.

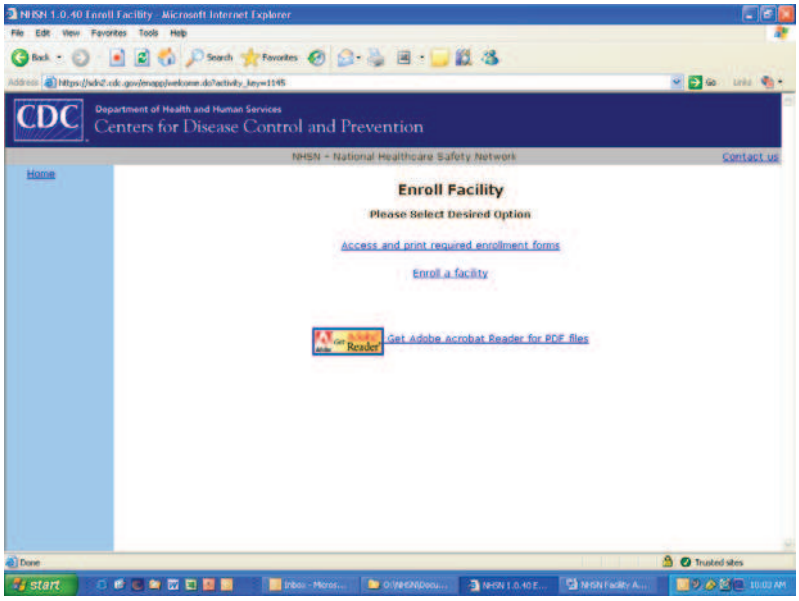
- Enter your challenge phrase and click **Submit**.



- After entering your challenge phrase, you will be brought to the SDN homepage. Under "My Applications" in the upper left corner of the page, you should see a link to the National Healthcare Safety Network labeled 'NHSN Enrollment'.



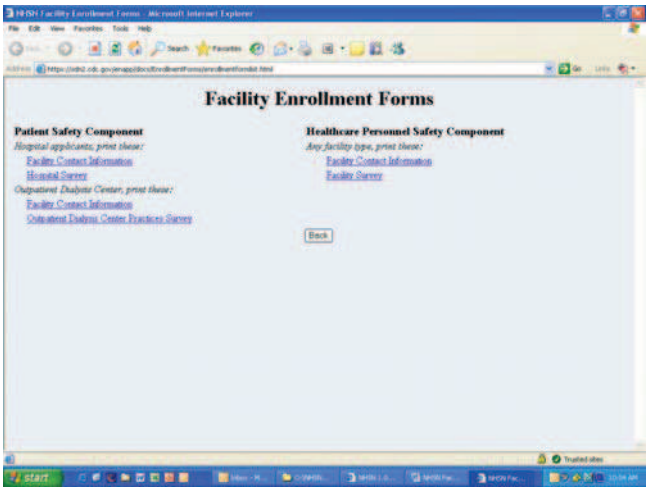
- Click on the **NHSN Enrollment** link to go to the **NHSN Enrollment** page.



NOTE: Do not use the browser's Back button. Always use the buttons provided on a page or use the navigation bar on the left to move around within the NHSN web pages.

4a. Download and Print Enrollment Forms

- From the **Enroll Facility** page, click on Access and print required enrollment forms option.



- From the **Facility Enrollment Forms** page, print the forms needed for the Component into which you are enrolling (i.e., Patient Safety as a hospital or as an Outpatient Dialysis Center, or Healthcare Personnel Safety). Complete these forms before attempting to enroll online.

  - You will need either your hospital's American Hospital Association (AHA) ID# or CMS Provider ID# (may also be called HCFA or Medicare#) to proceed; VA hospitals will need their VA Station Code to proceed. Click the box of those IDs that are not applicable.
  - You must also indicate a facility type from the drop down list. If you are unsure of which type to select, contact us (contact information at the end of this document).

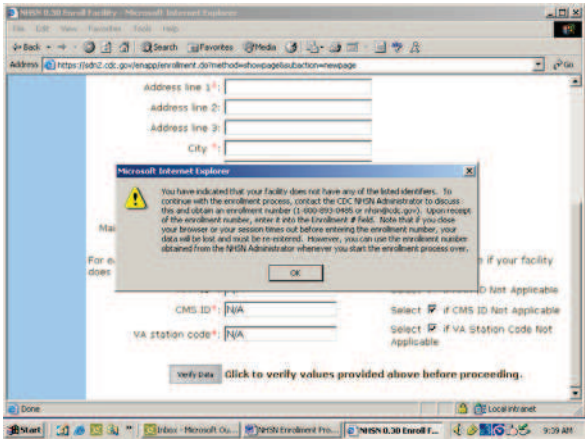
4b. Complete Enrollment in the NHSN

- Once you're ready to enroll, go to the **Enroll Facility** page, and click on the **Enroll a facility** option. Enter the data from the completed forms onto the screen and click **Submit.**

- NOTE: Facility verification is based on the city, state, and zip code. If you are having difficulties enrolling with your CMS or AHA numbers or VA station code, please make sure your entries are correct. If you continue to have problems, please email NHSN with the ID you are using to enroll.

- NOTE: It is not necessary to enter all of these verification numbers. For example, if you choose to enter your facility's CMS number, you may check the "not applicable" box next to the AHA ID# and the VA Station Code.

- NOTE: In the unlikely event that your facility does not have an AHA ID#, CMS Provider ID# or VA Station Code, a prompt will appear that will instruct you to contact the CDC NHSN Administrator who will assign an enrollment number to your facility. When you click OK on the prompt, a new data entry field will appear, called "Enrollment Number".



- Once submitted successfully, you can close the browser.

Step 5. Send Consent Form to CDC

After you have successfully completed the enrollment process, you will be sent an email that looks like the following:

```
From: NHSN
To: NHSN Facility Administrator
Sent:

Subject: NHSN facility enrollment submitted


The following facility has been submitted for enrollment in the NHSN:

Facility Name:
Tracking Number:

NHSN Facility Administrator:

The NHSN Facility Administrator has 30 days to access the Agreement to Participate and Consent form at the
following URL:

http://server/enapp/enrollment.do?method=displayAgreement&trackingnum=xxxxx

If this URL appears to be broken, please type the link on your browser address line. The complete address
including trackingnum=xxxxx must be included in order to access the form.

Once the form has been accessed, the CDC system administrator must receive the original, signed copy of the
Consent Form within 60 days or enrollment will be suspended.  Mail the form to: NHSN Administrator, MS A-24,
Centers for Disease Control and Prevention, 1600 Clifton Rd, NE, Atlanta, GA 30333.

If you have questions about NHSN, please contact us at nhsn@cdc.gov or 800-893-0485. For information on the
NHSN, please visit the member's website at http://www.cdc.gov/ncidod/dhqp/nhsn_members.html .
```

5a. Print the Agreement to Participate

Click on the URL provided in the email, print the Agreement to Participate and Consent form, read it and get it signed by the appropriate hospital administrator. This individual should be a person who has authority to give permission to submit facility and patient data to the CDC (i.e., CEO, COO, etc.). Send the **original signed** copy of the Consent page to CDC by surface mail within 60 days. If it is not received during that time period, the enrollment process will be terminated. Send the Consent to:

National Healthcare Safety Network
Division of Healthcare Quality Promotion
MS-A24
Centers for Disease Control and Prevention
1600 Clifton Road, NE
Atlanta, GA 30333

Step 6. Begin Using the NSHN Reporting Application

Once CDC receives the signed Consent from your facility, we will activate your NHSN account and notify you by email with instructions to access NHSN Reporting through the SDN. The email will look like this:

To: NHSN Facility Administrator
From: NHSN
Date:
Subject: NHSN enrollment approved

Your facility has been approved as a new member of NHSN. Welcome!

Facility Name:
Facility ID #:

As the Facility Administrator, you will now need to access the NHSN through the SDN (https://sdn.cdc.gov) by selecting the NHSN Reporting activity. Once in the NHSN, your first task should be to add those individuals who need to use the NHSN ("users") in the "Manage Users" section of the navigation bar. Add locations and surgeons from the navigation bar under the heading Facility.

Once you add a user, that person will receive an email prompting her/him to obtain a digital certificate. It is important that you verify the email address and inform the user to use the same address when applying for their digital certificate.

If you have any questions about NHSN, please contact us at 800-893-0485 or nhsn@cdc.gov. Information on NHSN is also available on the members' web site at http://www.cdc.gov/ncidod/dhqp/nhsn_members.html

Once you receive this email, you can go to the SDN (https://sdn.cdc.gov), enter your challenge phrase, and select **NHSN Reporting** activity. At this point you can begin to add users and set up location codes, surgeon codes, and enter a Monthly Reporting Plan.

If you have any questions, please contact NHSN at:

Telephone:800-893-0485

Email address:nhsn@cdc.gov

Website: http://www.cdc.gov/ncidod/dhqp/nhsn_members.html