National Program of Cancer Registries

Registry Plus Software for Cancer Registries

WCRS - Web Plus
User Manual

Web Plus Version 3.6.0
Customized for the Wisconsin Cancer Reporting System

Table of Contents

Chapter 1: Introduction 3
Overall Learning Objectives 3
Overview of the Web Plus User Manual 3
Web Plus Features 3
Users 3
System Requirements 4
Computer Specifications 4

Chapter 2: The Basics 5
Learning Objectives 5
Overview 5
Log In 5
File Uploader Menu Options 7
Log Out 8

Chapter 3: File Uploader Menu Options in Detail 9
Learning Objectives 9
New Upload 9
Previous Uploads 11
Download Files 12
Change Password 14

Chapter 4: Additional Web Plus System Information 15
Application Security Features 15
Operating System Network Infrastructure 15

Chapter 5: Data Reporting Protections 19
Overview 19
Chapter 255.04, Wisconsin Statutes 19
HIPAA and Cancer Surveillance 20

Appendix A: WCRS Contact Information 22

Chapter 1: Introduction

Overall Learning Objectives

These are the overall learning objectives for this Web Plus training manual.

- Learn the major functions of the File Upload role within Web Plus V3.6.0.
- Learn how to log on to Web Plus.
- View information regarding file uploads.

Overview of the Web Plus User Manual

The Web Plus User Manual provides you with the information to log on to Web Plus and use the File Uploader Role. This manual describes the functions available to the staff assigned to submit cases to the state central cancer registry, the Wisconsin Cancer Reporting System (WCRS) using Web Plus.

Web Plus Features

Web Plus is a Web-based application that submits cancer data securely over the public Internet from a facility to the Wisconsin Cancer Reporting System.

Submissions are saved in a secure database at WCRS, downloaded to the registry's secure LAN network location and edited in Prep Plus, the WCRS batch edit program. Users' display types, accounts, submission specifications and other configurations are managed at WCRS.

Web Plus is hosted on a secure Web server that has a digital certificate installed; the communication between the client and the server is encrypted with Secure Socket Layer (SSL) technology.

Users

The following user role is available:

Users	Description
File Uploader	Uploads files of abstracts in the appropriate NAACCR format or any non-NAACCR format.

System Requirements

Web Plus is a Web application that runs on Microsoft® Internet Information Services (IIS) and stores the data in a Microsoft SQL Server database. The application must be accessible from the Internet with support for encrypted communication between clients and the Web server.

In a typical setup, a server computer hosts the application, and another runs SQL Server. The Web server is placed in the demilitarized zone between the external and internal firewalls, while the SQL Server sits behind the internal firewall as part of the internal trusted network. A router connects the demilitarized zone to the Internet.

A secure sockets layer (SSL) digital certificate is installed on the Web server for site authentication, and for SSL encryption of data transferred between the clients and the Web server.

Computer Specifications

Intel® Pentium® IV processor or better, 500 MB RAM, and at least 500 MB free space on the hard drive with Windows 2000 Server or later server operating system, IIS version 5 or later, and .NET framework version 1.1. Although Web Plus works at 800 X 600 resolution, it can be best viewed at 1024 X 768 or higher resolution.

Chapter 2: The Basics

Learning Objectives

In this chapter, you will learn to:

- Identify Web Plus File Uploader menu options.
- Log in and log out of Web Plus.

Overview

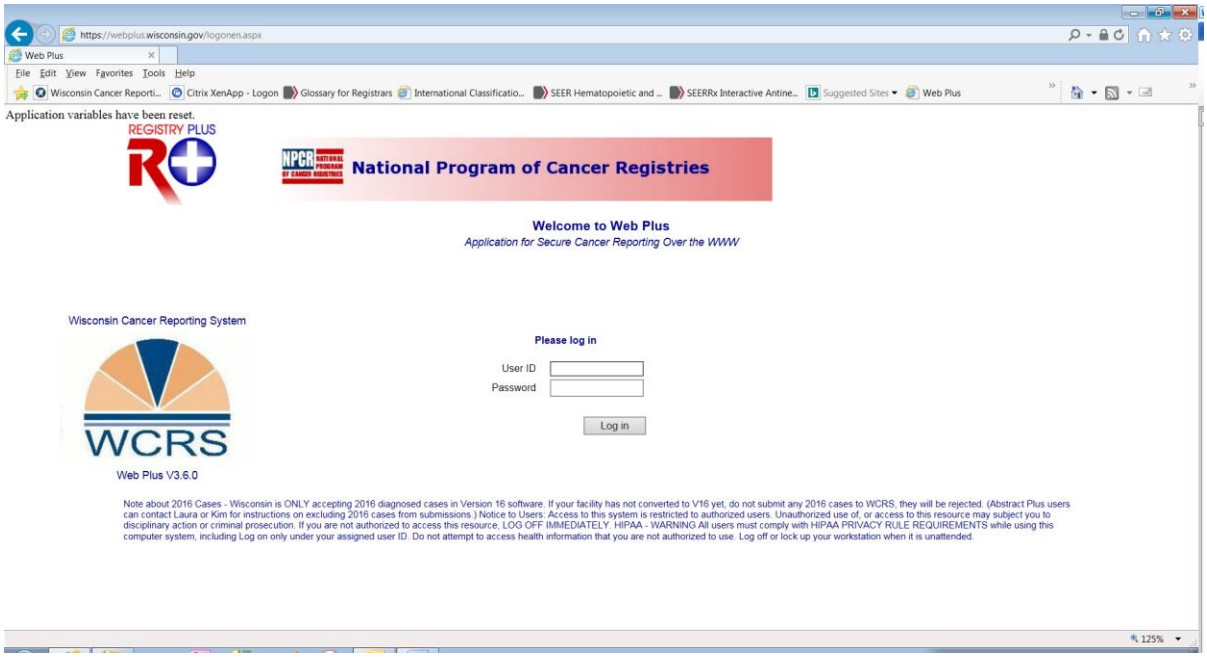
This chapter covers the basics of the Web Plus File Uploader role. It includes a description of the Web Plus menu options available to that role, and the means of logging in and logging out of Web Plus.

Log In

To log in, complete these steps.

1. Open your Internet browser and type the following web address (URL) in the Address field:
   https://webplus.wisconsin.gov/logonen.aspx
2. Press **Enter**.

   Result: The Web Plus main Log in page is displayed.



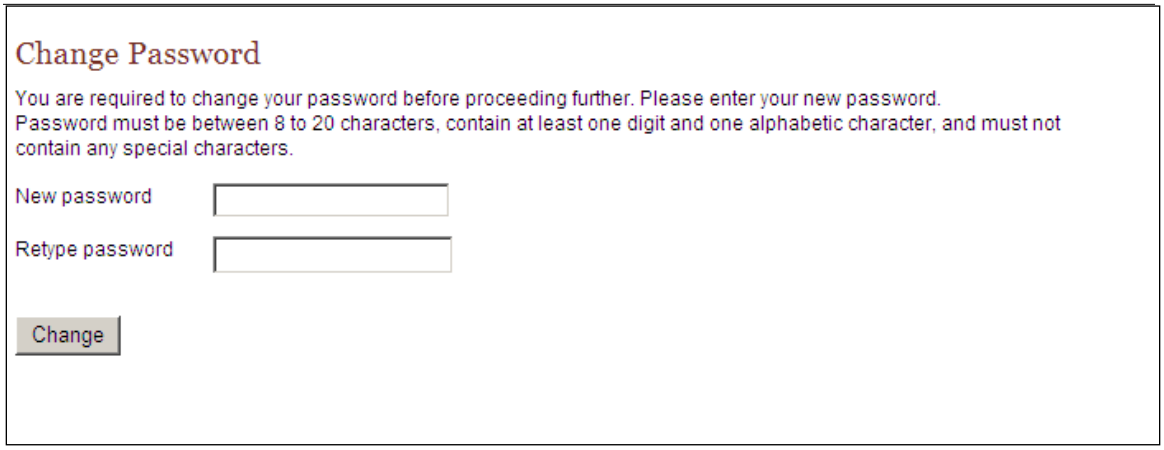
3. Type in your User ID and password. If you are a first time user, you received this information in an email from the Web Plus system administrator at the DHSWCRSdata@dhs.wisconsin.gov email address.

   The email message from the Web Plus Administrator will look like this:

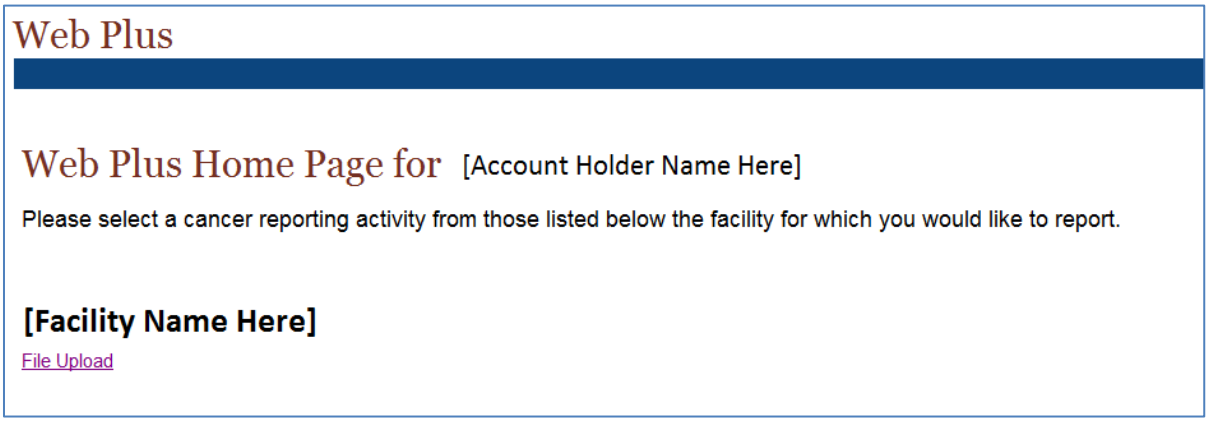
> Dear [Name of Account Holder],
>
> Your account has been created in Web Plus. You will need the following credentials to log in to Web Plus.
>
> User ID: KMO01234 [Example of what the WCRS-assigned will look like]
> Password: RmzCx1Tx [Example of what the password will look like]

   Note: User IDs and passwords created in an earlier version of Web Plus will work in Version 3.6.0. You will not need a new User ID and password.

4. Click **Log in** or **Enter**.
5. The **Change Password** window will open. Follow the directions in this window to change your password.



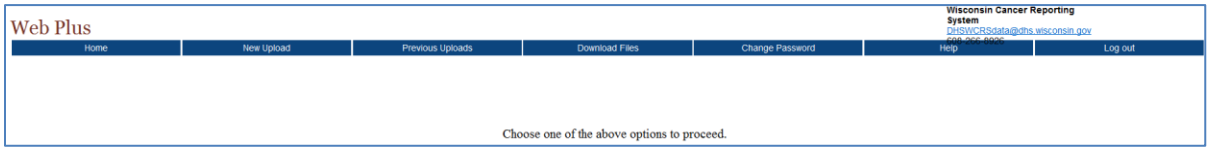
6. **Result**: The Web Plus File Uploader home page opens.



7. You have now successfully logged in, changed your password and located the File Uploader role under your account.

File Uploader Menu Options

After you log in and click on the File Upload reporting activity, the Web Plus File Uploader home page is displayed.



From this page you can access the different menu options under the file uploader role. The next table describes the menu options for this role.

Menu option	Sub-option	Function . . .
Home		Takes user back to File Upload home page.
New Upload		Opens window to select type of file to submit to WCRS, browse to find the file, and then submit.
Previous Uploads	Track File Uploads	Tracking log of previously submitted files.
Download Files		Allows download of file that WCRS posted.
Reports		View activity reports or rejected file reports.
Change Password		Allows user to change his/her password.
Help	About	Lists the Web Plus, NAACCR, and Collaborative Staging Algorithm Version information.
Log out		Log out of Web Plus activity. Returns user to the Log in page.

Log Out

To log out of Web Plus, click the **Log out** menu option (far right).

Result: The system logs the user out of Web Plus, and returns to the Login page.

Chapter 3: File Uploader Menu Options in Detail

Learning Objectives

In this chapter you will learn the specifics on the following File Uploader roles.

- New Upload
- Previous Uploads
- Download Files
- Reports
- Change Password

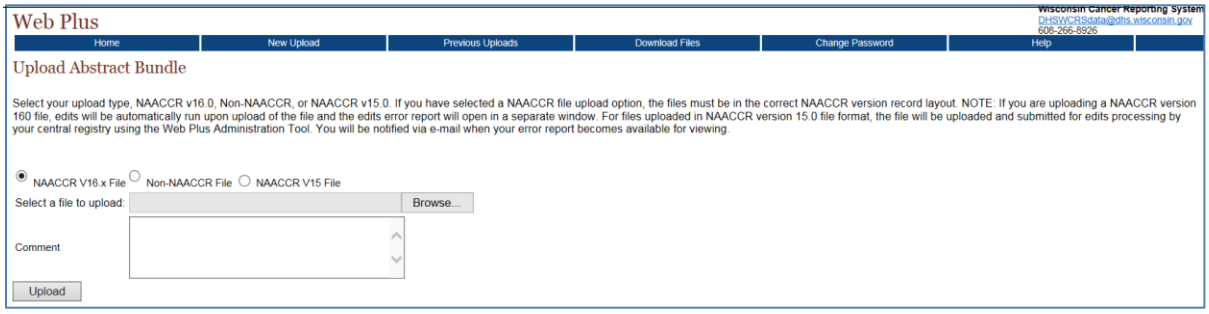
Caution: Files can not contain more than 1,000 cases in the NAACCR layout due to size limitations on the file transfer process.

New Upload

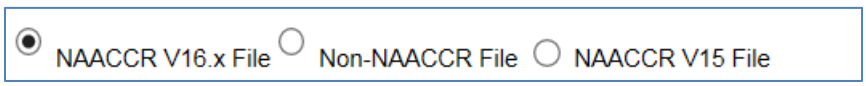
Click on the New Upload option when you are ready to submit a file to WCRS.

1. Click on **New Upload**.

Result: The Upload page opens.



Note: This screen has specific buttons for files in the NAACCR Version 15 and 16.x layouts. If submitting a case in one of those layouts, please check the correct button.



You may also submit other NAACCR Version layout files but you MUST click on the Non-NAACCR button to submit them.

2. Select the NAACCR V16.x File button for NAACCR V16.x file submissions.
3. Select the NAACCR V15 File button if you are reporting using this NAACCR version.
4. Select the Non-NAACCR file button for any other type of file that you need to send to WCRS.
5. Click on the **Browse** button; the **Choose file** window opens. Locate the file you are sending to WCRS. Click on that file and then click on **Open** or **Enter** (your window may show either prompt). The file name now appears in the **Select a file to upload** slot.

Many facilities submit files with the same name such as "state.dat." **This is an unacceptable file name**. Facilities need to name their file as follows:

WCRS facility number + abstractor initials + submission date.txt
[example: 00101_KMO_12072016.txt]

This will eliminate the possibility of the file being overwritten when exported out of Web Plus to the WCRS network server. If you submit more than one file on the same day for the same facility, put an 'a' or 'b' behind the initials to distinguish between the different files (again, so one does not get overwritten). Example: 00101_KMOa_12072016.txt and 00101_KMOb_12072016.txt

6. Enter the number of cases on the file in the Comment box and any other comment if necessary or requested by WCRS ("test file," "last of 2016 cases," "here's that disease index file you asked me to send," "3 DCOs included in this file," etc.)
7. Click on the **Upload** button. A message will appear stating "The file has been uploaded as a [type of file here] file."

You will also receive an immediate automatic email from DHSWCRSdata@dhs.wisconsin.gov confirming the file upload to the WCRS web server. **If you do NOT receive this email, then the file did not upload successfully!** Below is an example of a NAACCR V16.x submission confirmation.

Dear [name of Web Plus account holder],

Your NAACCR-formatted data file: [name of file here] was successfully uploaded to Web Plus and received by Wisconsin Cancer Reporting System on 8/15/2016 10:00:24 AM

Data quality edits will be applied to the uploaded file, and you will receive an e-mail when edits error report is available for your review in Web Plus.

Web Plus System Administrator
Wisconsin Cancer Reporting System

If you do not receive this email confirmation, please contact Kim Ortman at kim.ortman@dhs.wisconsin.gov or (608) 267-0239.

Please note that Web Plus contains the following default language on the File Upload window regarding processes that WCRS **does not conduct**:

NOTE: If you are uploading a NAACCR version 160 file, edits will be automatically run upon upload of the file and the edits error report will open in a separate window. For NAACCR version 15 file format, the file will be uploaded and submitted for edits processing by your central registry using the Web Plus Administration Tool. You will be notified via e-mail when your error report becomes available for viewing.

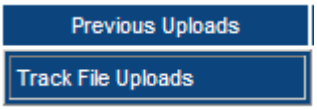
Similar language also appears in the automatically generated email confirmation (highlighted in yellow on the previous page).

Files are edited off-line in a batch process once they are downloaded from Web Plus. WCRS follows up on discrepancies that cannot be fixed in-house with the facility via email or phone. Complete error reports are available upon request; please contact Kim Ortman (contact information on page 22).

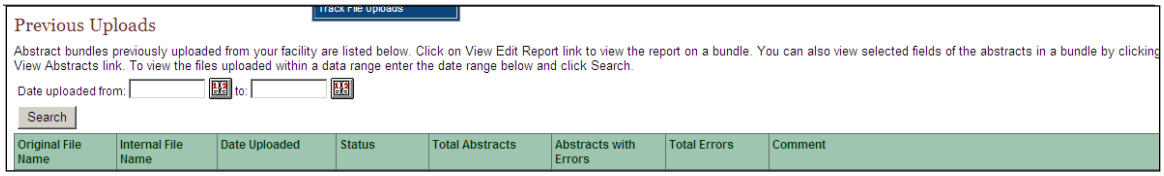
Previous Uploads

This allows the user to track previously uploaded files.

1. Click on **Previous Uploads** / **Track File Uploads**.



Result: The file tracking system page opens.



The following fields are available in the tracking system:

Original File Name	Name of file facility submits to WCRS.
Internal File Name	Name assigned to incoming file by Web Plus system.
Date Uploaded	Date and time file was uploaded.

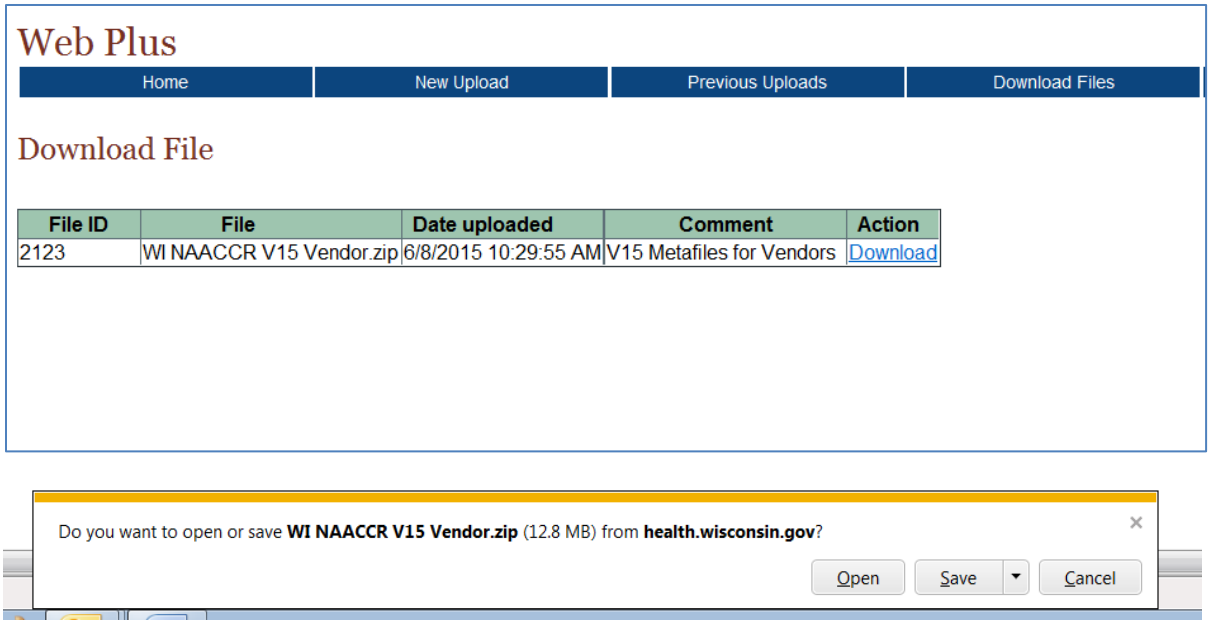
Status	Status of upload – will identify if the file was successfully uploaded or if upload was not successful.
Total Abstracts	If submitting a NAACCR file, the number of abstracts in the file will appear in this box. If a non-NAACCR file, this field will display 'N/A.'
Abstracts with Errors	Not applicable in this version.
Total Errors	Not applicable in this version.
Comment	When submitting a case file, make sure to include the number of cases on the file in the comment box.
Action Fields	Not activated in this version (View Abstracts, View Edit Report, Delete)

Download Files

This option will allow you to download a file from WCRS. WCRS will notify a facility separately if a file to download has been posted on the server.

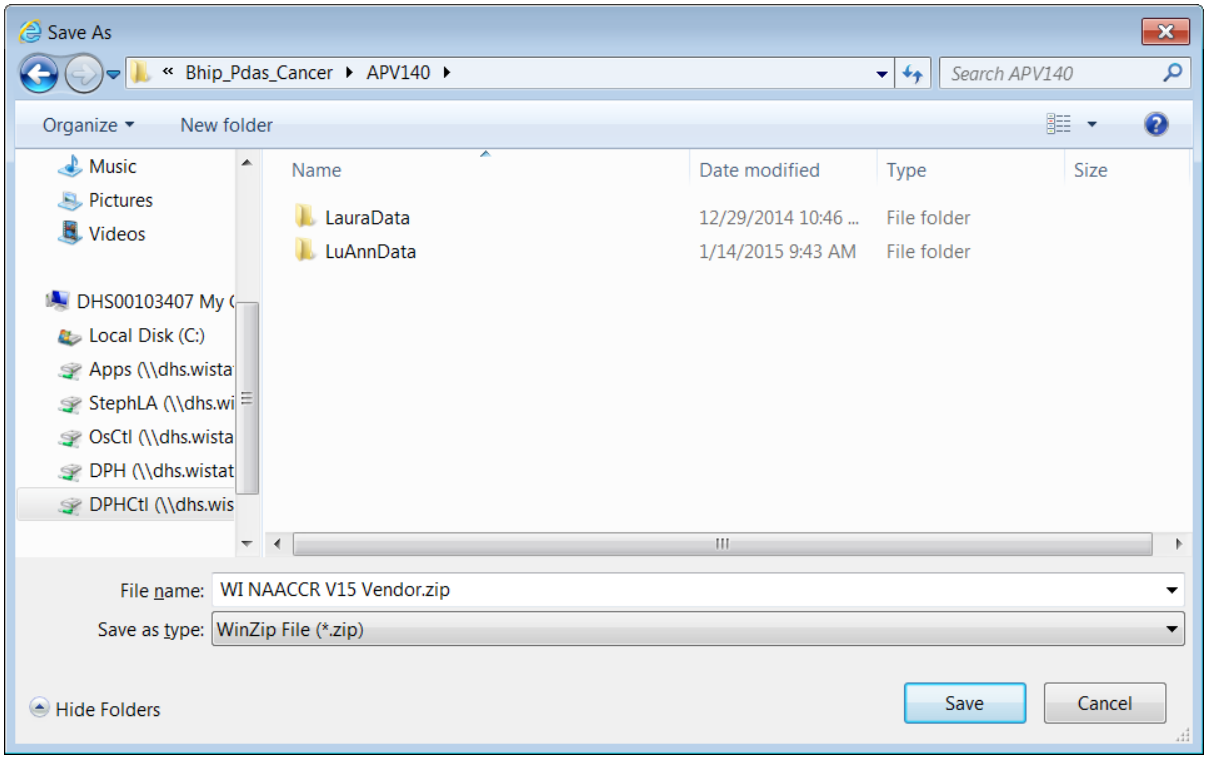
To download a file, click on **Download Files**. You should see the file available for download appear in the window, similar to the example below.

Click on the **Action** hyperlink **Download** and choose to **Open** the file (not recommended if the file contains confidential data), **Save,** or **Save As**. WCRS recommends the **Save As** option – it allows you to pick the location where you want to download the file.



(Click on the pull down arrow next to **Save** to see the **Save As** option.)

Then follow the prompts once you have the correct file location (see example).

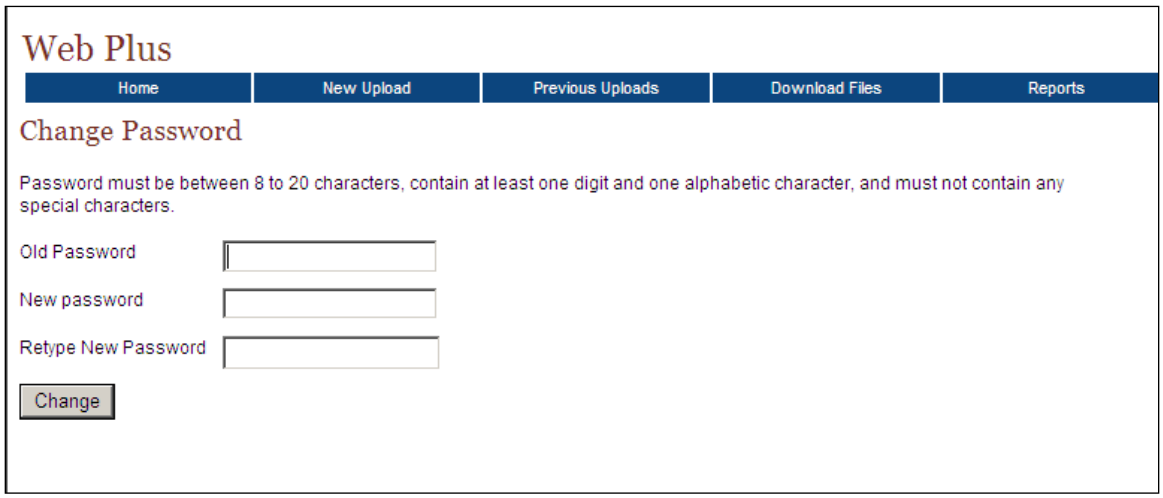


Change Password

Allows the user to change their password at any time.

1. Click on **Change Password**.

   Result: The Change Password page opens.



2. Follow the instructions above to change your password.

Chapter 4: Additional Web Plus System Information

Web Plus is a highly secure application that can be used to transmit confidential patient data between reporting locations and a central registry safely over the Internet. Security is achieved by a combination of software features and network infrastructure.

Application Security Features

Form-based authentication. Web Plus requires each user to enter his or her user ID and password to access the system.

Passwords. Web Plus provides several options to configure password attributes. These options are set by the central registry administrator (see Role-Based Access below). Attributes in this version of Web Plus include:

1. Enforcing the complexity of passwords required to login to Web Plus by using a regular expression.

2. Keeping a password history and requiring new passwords to be different from the ones used before.

3. Setting password expiration to force users to change their passwords after a specified time interval.

4. Forcing users to change the password after the first login when the administrator resets a forgotten password.

This version of Web Plus is set up as follows:

- Maximum invalid logins = 3
- Password history = 3
- Password expires every 180 days
- Lockout reset interval = 60 seconds
- Strong Passwords enforced
- Session Timeout = 1200 seconds
- Force password changes after first-time successful login

Role-based access. Web Plus grants users different levels of access depending on their role. Seven roles are defined in Web Plus—

Facility abstractor: Works in a local facility or doctor's office and handles patients' medical records. When a patient is diagnosed with cancer, the facility abstractor reports the case to the state's central cancer registry.

Central registry abstractor/reviewer: Reviews abstracts submitted to the central registry for completeness and accuracy and may abstract additional data items from submitted text; also abstracts new cases.

Central registry administrator: Sets up the local facilities with access to Web Plus to report their data, manages facility accounts and users at both central registry and facilities, configures display types, edit sets, and system preferences, manages assignment of abstracts to central registry staff, exports data, and views reports.

Local administrator: Manages the users who are allowed to access Web Plus at one facility.

File uploader: Uploads files of abstracts in the appropriate NAACCR format that were not abstracted using Web Plus, views EDITS error report, and cleans errors on rejected files prior to re-uploading. **This is the only option currently enabled.**

Follow-back supervisor: Uploads files of partially-filled follow-back abstracts, manually adds follow-back abstracts online, tracks follow-back abstracts by uploaded file or by facility, and generates and views Web Plus follow-back reports.

Follow-Back monitor: Tracks follow-back abstracts by assigned facility and generates and views Web Plus follow-back reports.

Other Web Plus features include—

All users of a facility have access to all abstracts entered for the facility.

Web Plus keeps an extensive log of user logins, data accesses, and updates for auditing purposes.

Users' accounts can be configured to be locked out after a set number of failed attempts to login.

Users' accounts can be deactivated temporarily by the WCRS administrator.

The WCRS administrator can see what page the user has accessed.

Display types and edit set configurations are centrally controlled.

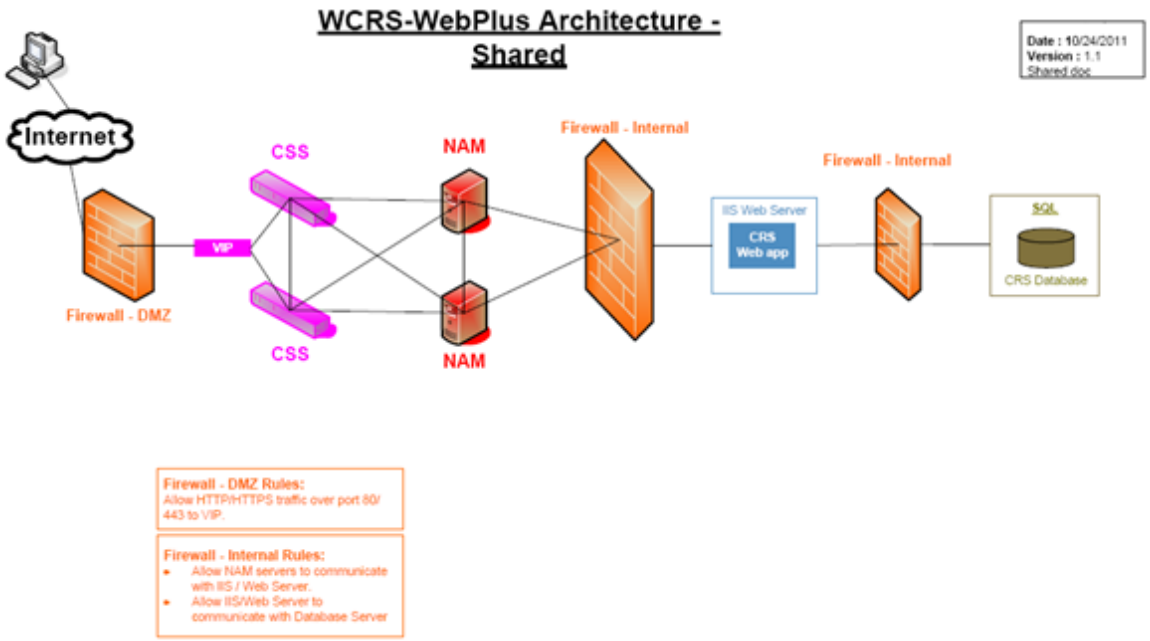
User passwords are encrypted using a one-way hash method.

The connection string to the server database can be encrypted.

Operating System Network Infrastructure

Client computer security. WCRS recommends that anti-virus and anti-spyware software be installed on the client computer, and these programs should be updated regularly.

Secure communication channel. Web Plus relies on a Secure Socket Layer (SSL) channel between the Web server and the client browser to protect the data exchanged over the Internet. This secure communication channel is not part of Web Plus, but is required for Web Plus to send data securely. To set up an SSL channel, a server certificate must be installed on the Web server and SSL encryption must be enabled on the Web site containing the application. The WCRS Web Plus server uses DigiCert, Inc. certificates to encrypt the data/communication between reverse proxy and user desktops. The WCRS Web Plus certificate is of 128-bit cyber strength and has a 2048 key length.



The security of Web Plus depends mostly on the security of the client computer, the communication channel between the client and the Web server, the Web server, the base operating system, and the configurations of the firewalls on either side of the Web server.

WCRS, through the Department of Health Services and the Division of Enterprise Technology (DET), Department of Administration, has a security policy in place and documents the users (and their assigned roles) who will have access to the Web Plus

application and the database. DET is responsible for encrypting the Web Plus database, preventing security breaches, enforcing strong passwords, administering accounts, setting up the firewall protections and all other aspects related to database security.

WCRS Web Plus Server Backups. Backups are scheduled every four hours when an active transaction takes place during the day. There is also a nightly full backup regardless of any active transaction.

DET does the following to ensure security:

- Applies monthly Microsoft patches.
- Disables unnecessary protocols including NetBIOS and Server Message Block (SMB) on the Internet-facing Network Interface Card (NIC) and removes Web Distributed Authoring and Versioning (WebDAV).
- Deletes or disables unused accounts. System administrators use special administrative rights domain accounts (separate from their normal work ID) to manage the server.
- Uses strong access controls to protect sensitive files and directories. Sets access at the directory level whenever possible.
- Enforces strong password policies such as:
    - Server passwords must be greater than 7 characters.
    - Must contain at least three of the following:
        - English uppercase characters
        - English lowercase characters
        - Numeric digits
        - Non-alphanumeric (ex: !, #, %)
        - New password can not be the same as the last 8 passwords
        - Password can not contain three or more characters from the user's account name.
        - Passwords must be changed every 60 days
        - Reminder emails are sent starting 14 days before expiration to prompt the password change.

Chapter 5: Protections to Facilities Reporting Data to WCRS

Overview

This chapter lists the applicable statute and HIPAA statements relating to cancer registry reporting.

Chapter 255.04, Wisconsin Statutes

The entire statute is listed; sub.(4) describes the protection to persons submitting data.

255.04 Cancer reporting.

(1) Any hospital, as defined under s. 50.33 (2), any physician and any laboratory certified under 42 USC 263a shall report information concerning any person diagnosed as having cancer or a precancerous condition to the department as prescribed by the department under sub. (2).

(2) The department shall prescribe:
- (a) The form on which the report under sub. (1) shall be submitted.
- (b) The time schedule under which the report under sub. (1) shall be submitted.
- (c) The types of cancer and precancerous conditions to be reported under sub. (1).

(3) Any information reported to the department under sub. (1) or (5) which could identify any individual who is the subject of the report or a physician submitting the report shall be confidential and may not be disclosed by the department except to the following:
- (a) A central tumor registry in another state if the individual who is the subject of the information resides in the other state.
- (b) A national tumor registry recognized by the department.
- (c) A researcher who proposes to conduct research, if all of the following conditions are met:
  - 1. The researcher applies in writing to the department for approval of access to individually identifiable information under sub. (1) or (5) that is necessary for performance of the proposed research, and the department approves the application. An application under this subdivision shall include all of the following:
    - a. A written protocol to perform research.
    - b. The researcher's professional qualifications to perform the proposed research.
    - c. Documentation of approval of the research protocol by an institutional review board of a domestic institution that has a federalwide assurance approved by the office for human research protections of the federal department of health and human services.
    - d. Any other information requested by the department.
  - 2. The proposed research is for the purpose of studying cancer, cancer prevention, or cancer control.

(4) The report of information under sub. (1) or (5) may not be construed as a violation of any person's responsibility for maintaining the confidentiality of patient health care records, as defined under s. 146.81 (4).

(5) The department may, to the extent feasible, collect information related to the occupation of cancer patients in order to fulfill the purpose of s. 250.04 (3) (b) 4.

(6) The department may charge a reasonable fee for disclosing information to a researcher under sub. (3) (c).

(7) Information obtained by the department under sub. (1) or (5) or obtained by a person under sub. (3) (c) is not subject to inspection, copying, or receipt under s. 19.35 (1).

(8) No person to whom information is disclosed under sub. (3) (c) may do any of the following:

(a) Use the information for a purpose other than for the performance of research as specified in the application under sub. (3) (c)1., as approved by the department.

(b) Disclose the information to a person who is not connected with performance of the research.

(c) Reveal in the final research product information that may identify an individual whose information is disclosed under sub.(3) (c).

(9) Whoever violates sub. (8) (a), (b), or (c) is liable to the subject of the information for actual damages and costs, plus exemplary damages of up to $1,000 for a negligent violation and up to $5,000 for an intentional violation.

(10) (a) Whoever intentionally violates sub. (8) (a), (b), or (c) may be fined not more than $15,000 or imprisoned for not more than one year in the county jail or both.

(b) Any person who violates sub. (8) (a), (b), or (c) may be required to forfeit not more than $100 for each violation. Each day of continued violation constitutes a separate offense, except that no day in the period between the date on which a request for a hearing is filed under s. 227.44 and the date of the conclusion of all administrative and judicial proceedings arising out of a decision under this paragraph constitutes a violation.

(c) The department may directly assess forfeitures under par. (b). If the department determines that a forfeiture should be assessed for a particular violation or for failure to correct the violation, the department shall send a notice of assessment to the alleged violator. The notice shall specify the alleged violation of the statute and the amount of the forfeiture assessed and shall inform the alleged violator of the right to contest the assessmentunder s. 227.44.

History: 1985 a. 29; 1989 a. 173 ss. 2, 13; 1993 a. 16; 1993 a. 27 s. 48; Stats. 1993 s. 255.04; 1993 a. 183; 1997 a. 114; 2009 a. 28.

HIPAA and Cancer Surveillance

1. What is the HIPAA Privacy Rule?

In 1996 the U.S. Congress passed a law requiring, among other things, uniform federal privacy protections for individually identifiable health information. This law is called the Health Insurance Portability and Accountability Act of 1996, or "HIPAA." The U.S. Department of Health and Human Services recently issued final regulations implementing the privacy provisions of HIPAA. These regulations are called the "Privacy Rule." Copies of the HIPAA Privacy Rule, as well as helpful explanatory materials, may be found at the HHS Office of Civil Rights website: http://www.hhs.gov/ocr/hipaa/.

2. What is a 'Public Health Authority' under HIPAA?

Under HIPAA, a 'Public Health Authority' refers to "an agency or authority of the United States, a State or territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate."1 "...Such agencies are authorized by law to collect or receive such information for the purposes of preventing or controlling disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions."2 Central cancer registries are considered public health authorities because state laws mandate their duties.

45 CFR 164.501 and 45 CFR 164.512

3. Is it a violation of HIPAA for a covered entity to report information about cases of cancer to the state cancer registry?

No. Reporting information about cases of cancer in accordance with the requirements of state authorizing statutes and regulations is permitted by HIPAA. The Privacy Rule contains a specific provision authorizing covered entities to disclose protected health information as required by law.[1] In fact, penalties for failure to comply with state reporting are specified in state law and often consist of significant fines.

45 CFR 164.512(a)(1)

Public health surveillance systems, such as the Wisconsin Cancer Reporting System, are HIPAA-exempt. The following links provide academic and legal interpretations of the exempt status.

Academic Interpretation of HIPAA
http://www.naaccr.org/LinkClick.aspx?fileticket=6m3L0DRTi4U%3d&tabid=120&mid=460

Legal Interpretation of HIPAA
http://www.naaccr.org/LinkClick.aspx?fileticket=7gG6216GjE0%3d&tabid=120&mid=460

Appendix A: WCRS Contact Information

Primary contact:

Kim Ortman
Data Submission Coordinator
Wisconsin Cancer Reporting System
(608) 267-0239
kim.ortman@dhs.wisconsin.gov

Secondary contact:

Laura Stephenson
QA Manager
Wisconsin Cancer Reporting System
(608) 266-8926
laura.stephenson@dhs.wisconsin.gov