



PENINSULA RSN

MANAGEMENT INFORMATION SERVICES POLICIES AND PROCEDURES

Policy Name: LOADING OF STATE ENROLLMENT DATA **Policy Number:** 4.01

Reference: DSHS Contract

Effective Date: 8/2005

Revision Date(s): 12/2011

Approved by: PRSN Executive Board

CROSS REFERENCES

- Policy: Corrective Action Plan

PURPOSE

To ensure that all updates to Medicaid enrollment and eligibility are downloaded in a timely way into the on-line Peninsula Regional Support Network (PRSN) database.

PROCEDURE

The Peninsula Regional Support Network contracts with Kitsap Mental Health Services (KMHS) to manage the Information Services network on behalf of the PRSN.

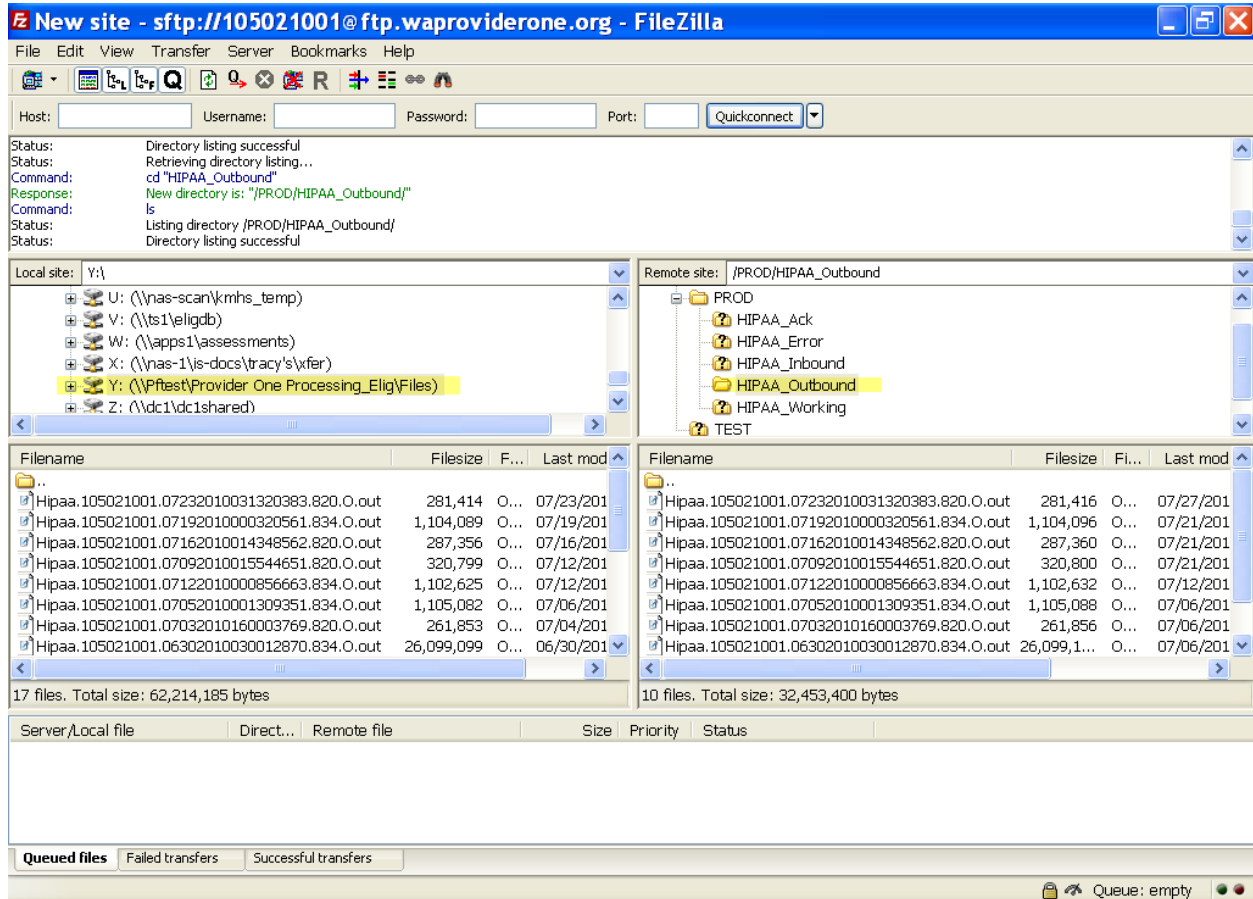
Kitsap Mental Health Services IS staff are responsible to update enrollment information in the PRSN's database monthly.

In order to load enrollment data from the Mental Health Division into the PRSN Information Services database, KMHS staff adhere to the following specific procedures and checks:

Download Files from Provider One

Using Filezilla – connect to ftp.waproviderone.org – type of connection is SFTP
Username is 105021001, Password is peni0010

When connected, navigate to /PROD/HIPAA_Outbound directory



Place new files in the PFTEST server, D:\Provider One Processing\Files for processing.

As the directory grows, you would be best to sort by Last modified to get most recent on top. Keep the spreadsheet updated so it will be easier to determine files for download.

Every week there should be at least two files – a .834.O.out (eligibility records) and .820.O.out (RSN Payment records).

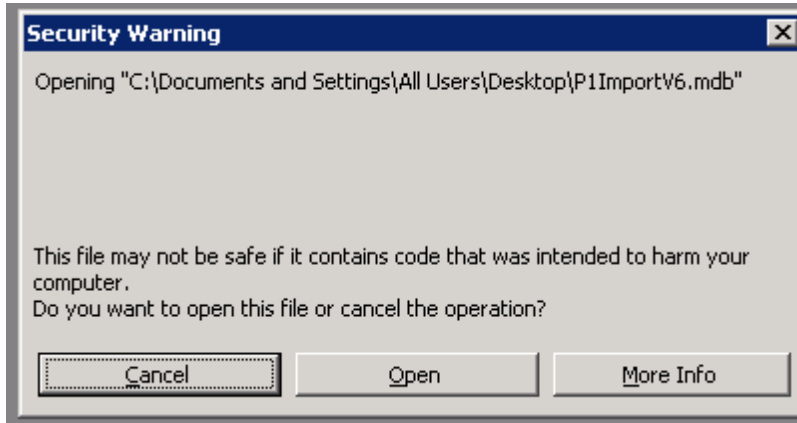
Update the spreadsheet [\\IS-DOCS\Elig\P1 Eligibility\FileLog.xls](#) with the file name(s) downloaded

Import file(s) into the Access Database

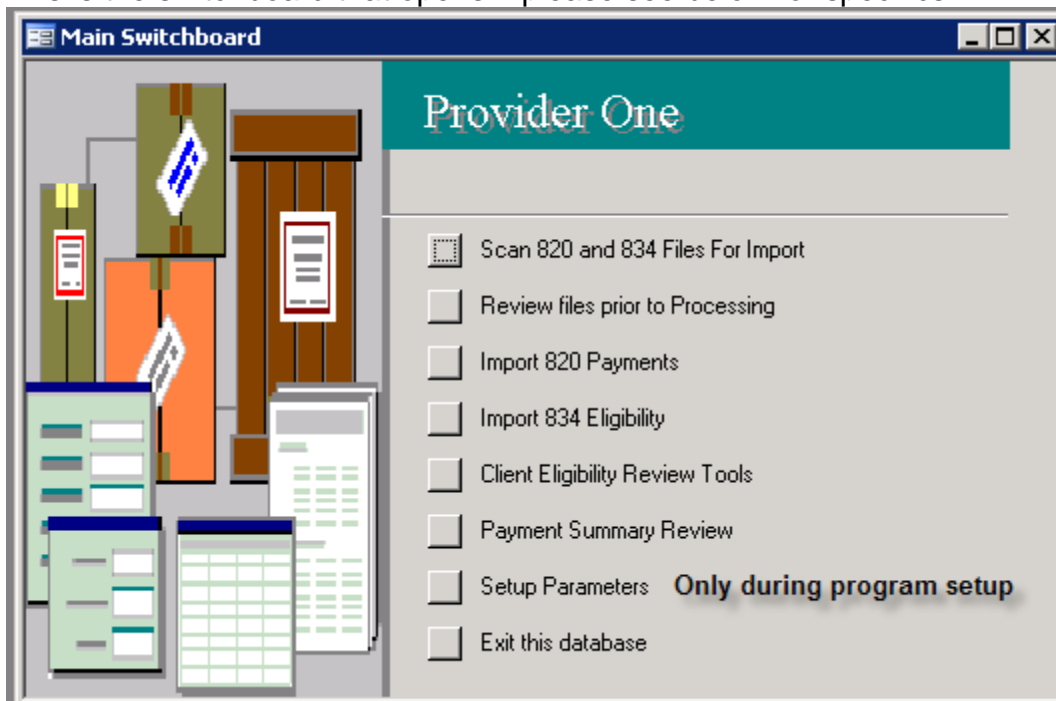
The Access Database is only available on PFTEST server and is called P1ImportV6.mdb There is a shortcut for all users called P1ImportV6.mdb



When you select the Shortcut – you will see the following message – click Open



This is the switchboard that opens – please see below for specifics.



1 – Scan files. This process reads the PFTEST D:\Provider One Processing\Files to determine what is new, etc. This runs very quickly.

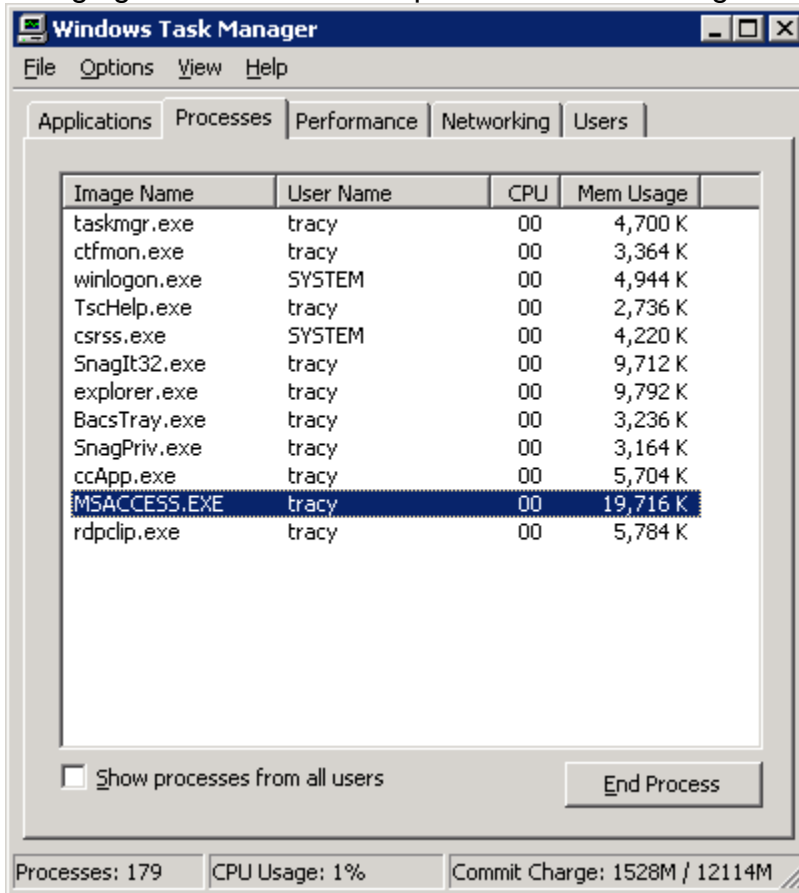
2 – Review files prior to Processing. This displays the files from the above directory and if they are identified and ready for import. It determines if this is a monthly/full file based on the file size. Check to ensure the file(s) you just placed in the directory is there.

	FileName	DateImpo	DateTimePo	blImport	EffectiveDate	MonthlyFullFile	FileType	FileSize	TStamp	blBadFile
▶	Hipaa.105021001.05312010084628278.834.O.out		8:02:03 AM	<input checked="" type="checkbox"/>	5/31/2010	<input checked="" type="checkbox"/>	834	25116809	084628	<input type="checkbox"/>
*				<input type="checkbox"/>		<input type="checkbox"/>		0		<input type="checkbox"/>

3 – Import 820 Payments. If there is a new 820.O.out file ready to be read, select this option.

4 – Import 834 Eligibility. This will import the 834.O.out file into the database. NOTE – a full monthly file may take hours to complete. This will tie up your PFTEST connection

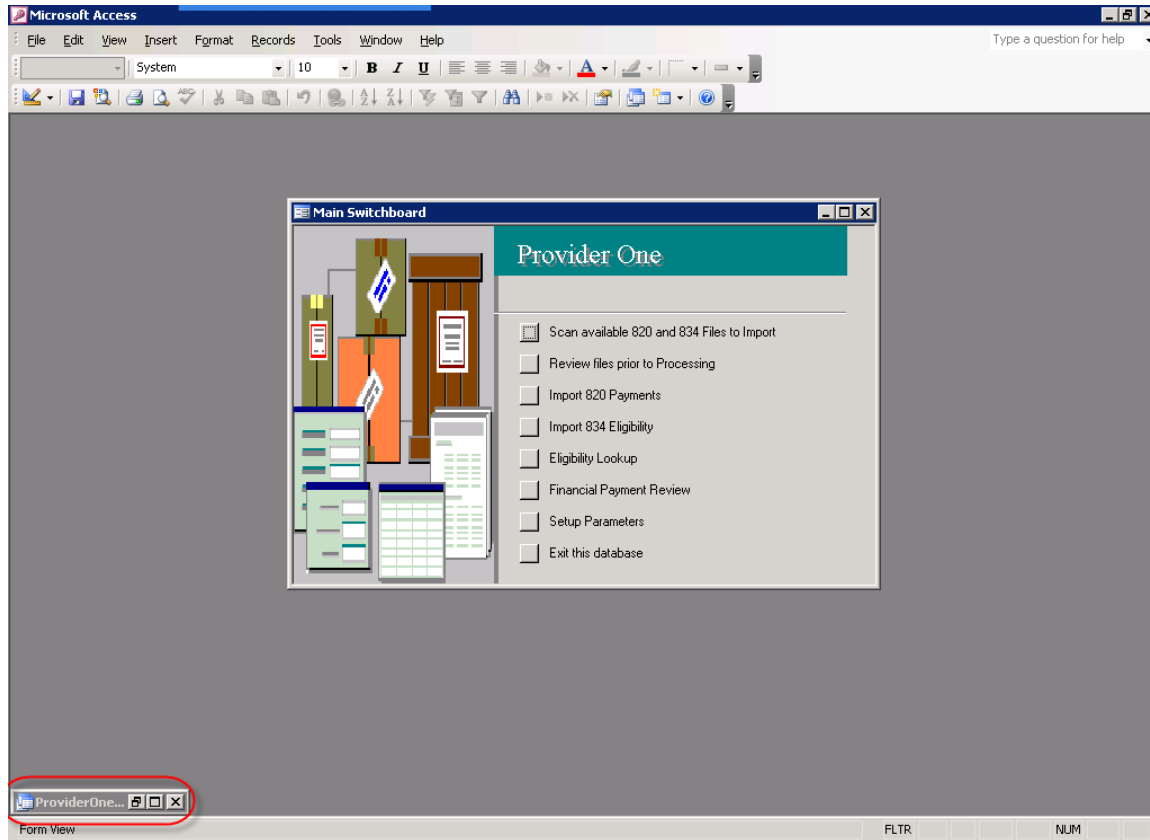
during the import. If you are concerned about the process you can click Start/Run and type taskmgr. Here you will see the Access process running and using memory. Here you would see MSACCESS.EXE using around 20% of CPU and the Mem usage will be changing – this indicates the process is still running.



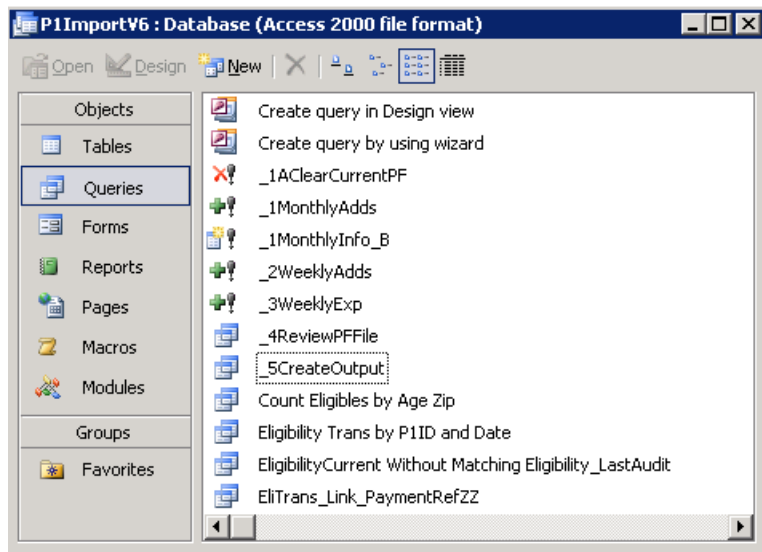
When completed, you will return to the Switchboard window. Notify Anders (337-4886 – aedgertn@co.kitsap.wa.us) the 820 Payment file has been imported (if processing 820 file).

Export for ProFiler processing – 834 Files only

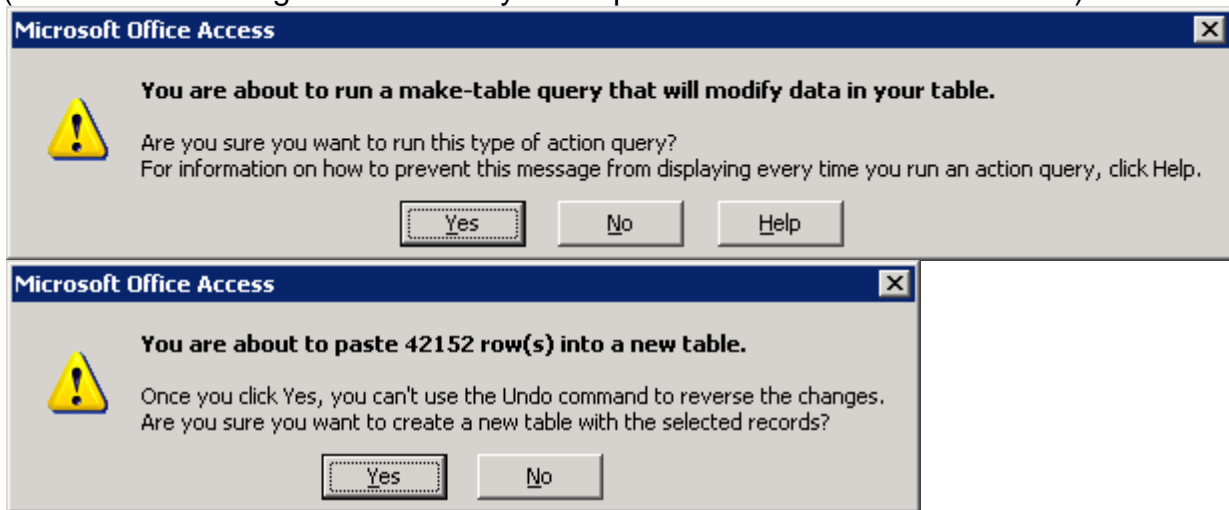
Once the 834 (Eligibility) data is imported you need to run a query to create the file for yet another Access DB to use for reading/processing in ProFiler. Open the window that is minimized in the bottom left of the screen:



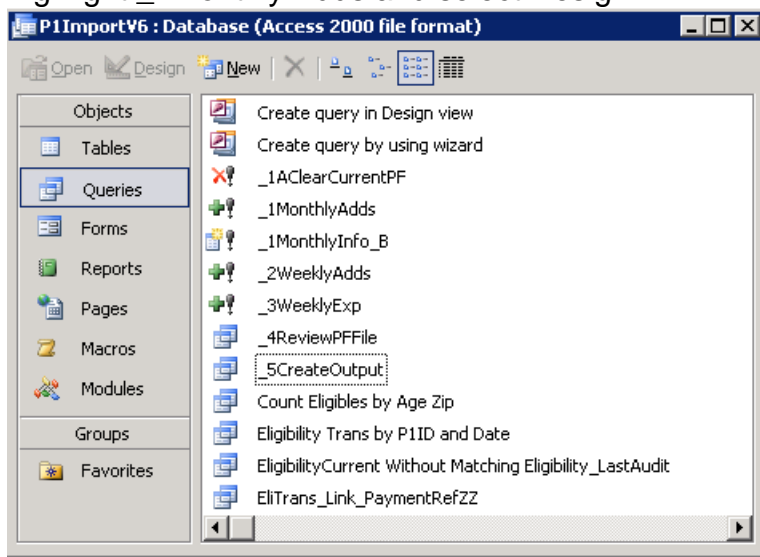
Select Queries –



First run _1AClearCurrentPF (for both Monthly and Weekly files) – this empties the current database. NOTE: For each query you will get two warnings – Click YES to both (the second message is either that you will paste or delete rows – this is OK)

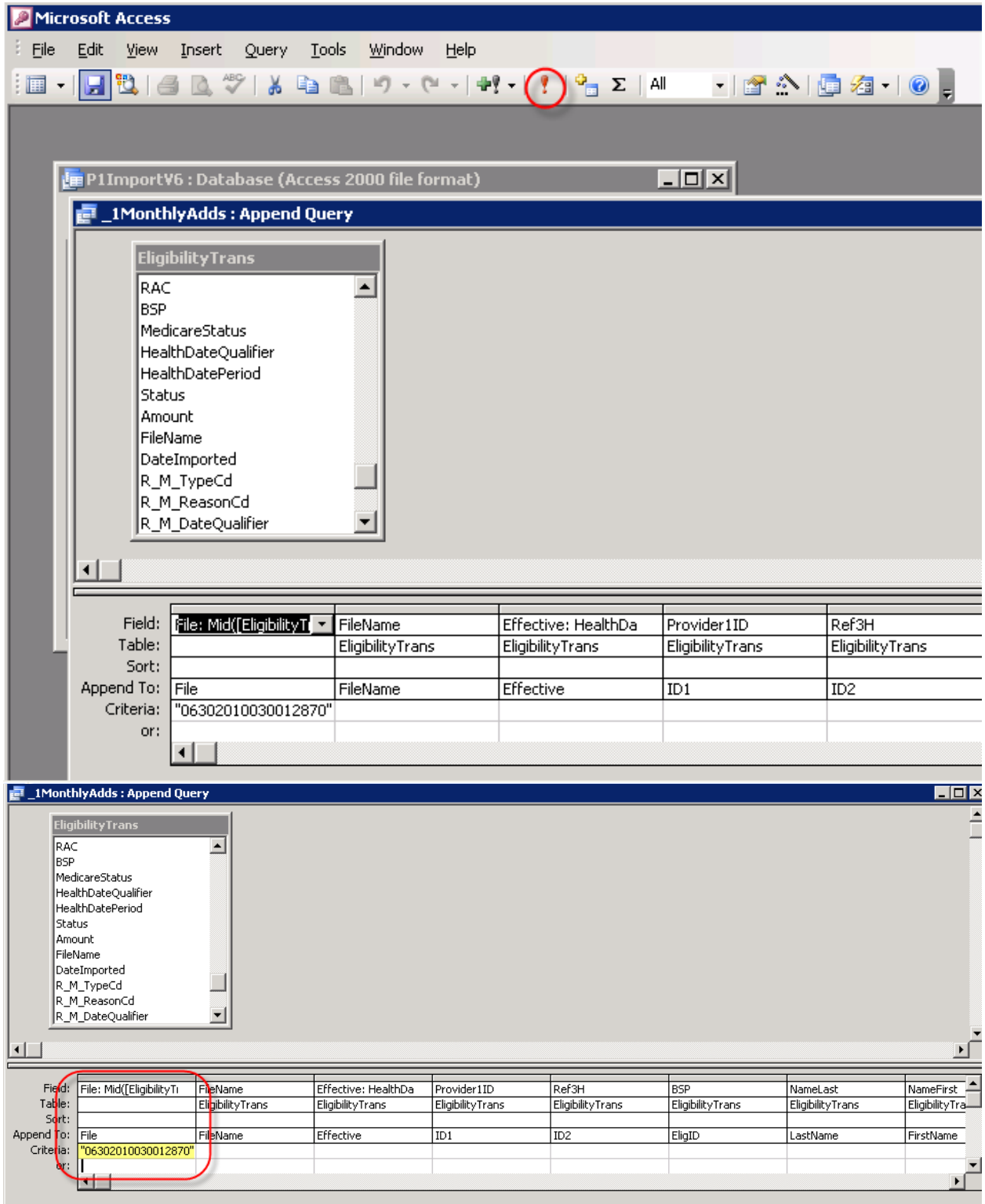


Monthly Files Only (If doing a weekly update – skip to Weekly Files section)
 Highlight _1Monthly Adds and select Design



Open the field File: Mid([EligibilityTrans.FileName],17,17) and enter the filename being used (The filename is the bold/highlighted section of the overall filename: Hipaa.105021001.**05312010084628278**.834.O.out) This name is used throughout the process.

Select the Run command (Red !)

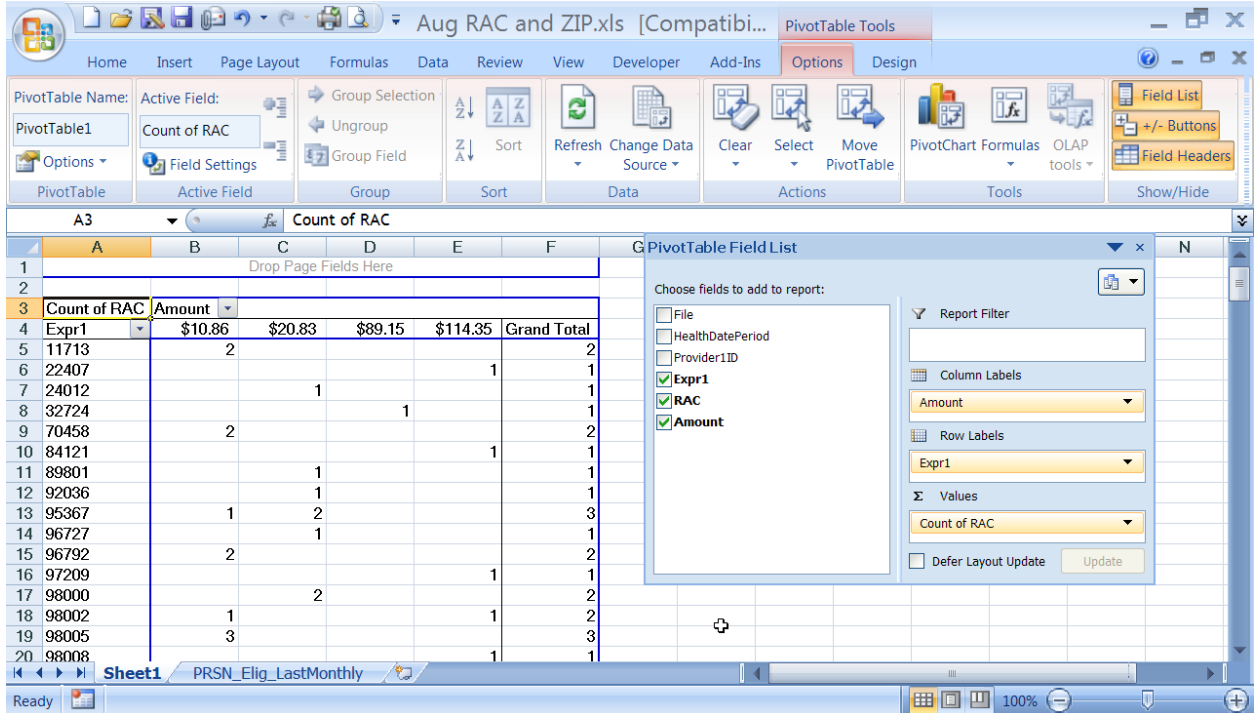


Again, you will get the messages (OK for both) and then close the query (this creates a new DB called CurrentPF)

Run query _1MonthlyInfo_B, changing the file name as above.

Open the Table PRSN_Elig_LastMonthly and select File/Export (file type Excel)
 Save this output file in PRSN Provider/RSN/P1 Elig with the name MMM RAC
 and ZIP.

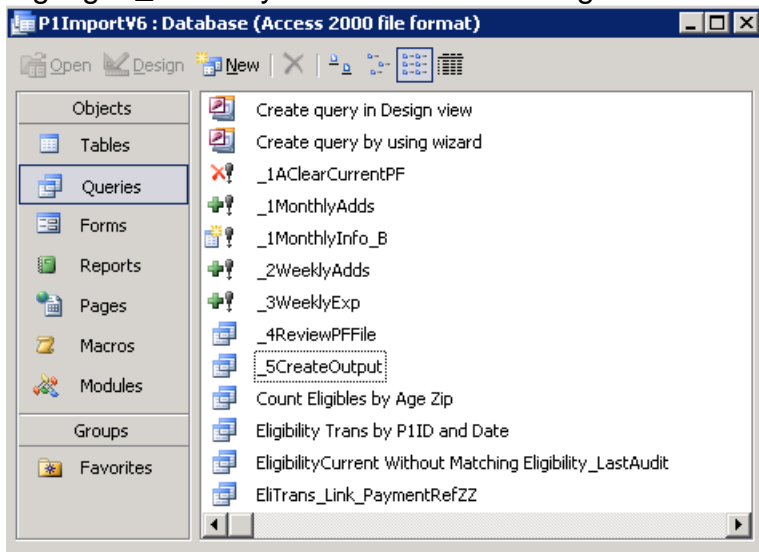
Open this spreadsheet and create a pivot table as shown below



Save the file with the same file name and notify Anders (aedgertn@co.kitsap.wa.us) notifying him of the monthly file for Zip codes.

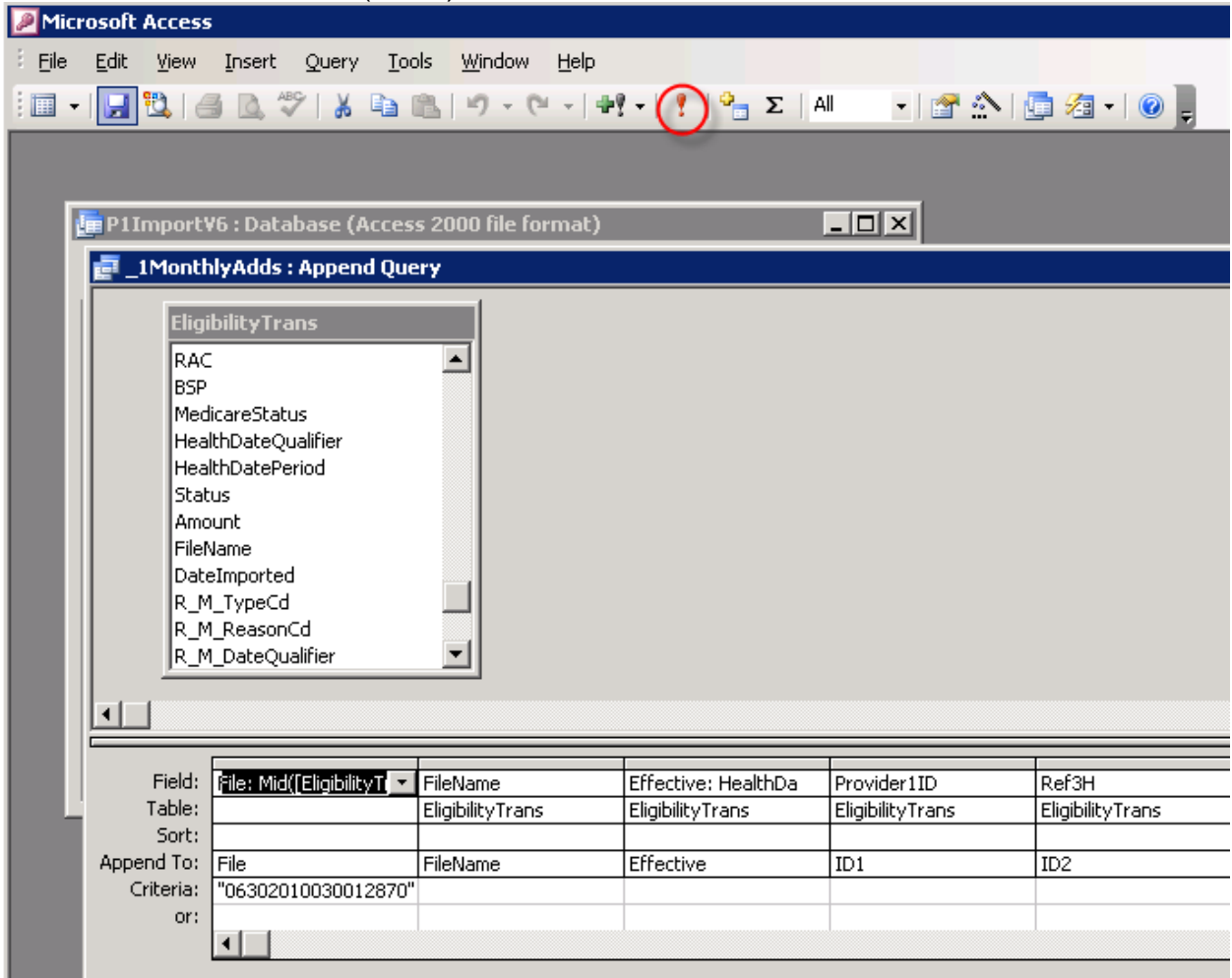
Weekly Files Only

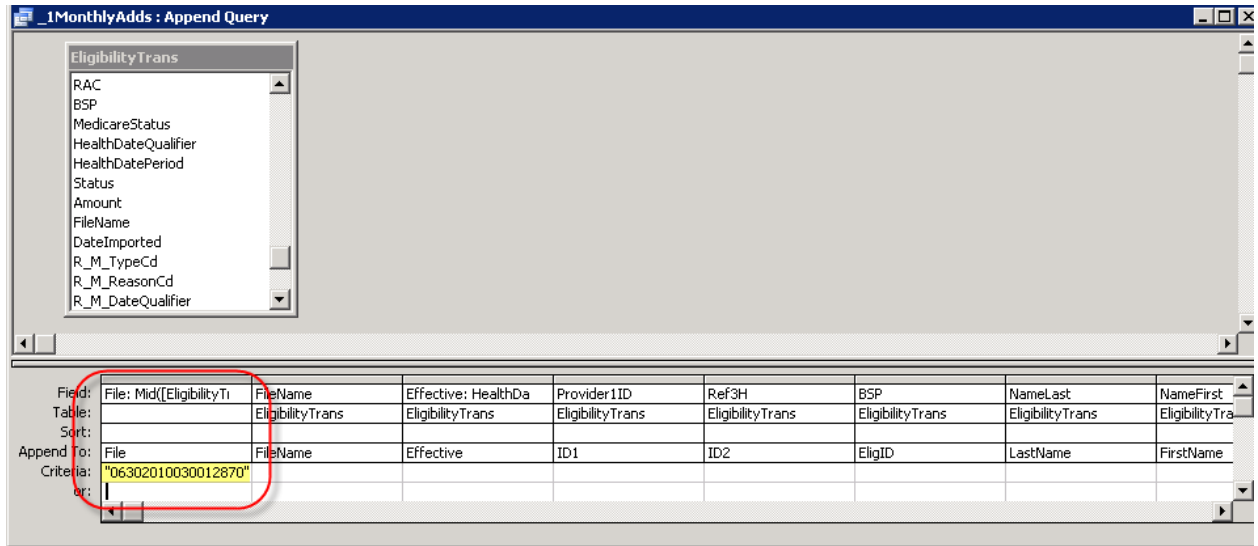
Highlight **_2WeeklyAdds** and select Design and then the same for **_3WeeklyExp**



Open the field File: Mid([EligibilityTrans.FileName],17,17) and enter the filename being used (The filename is the bold/highlighted section of the overall filename: Hipaa.105021001.**05312010084628278**.834.O.out) This name is used throughout the process.

Select the Run command (Red !)





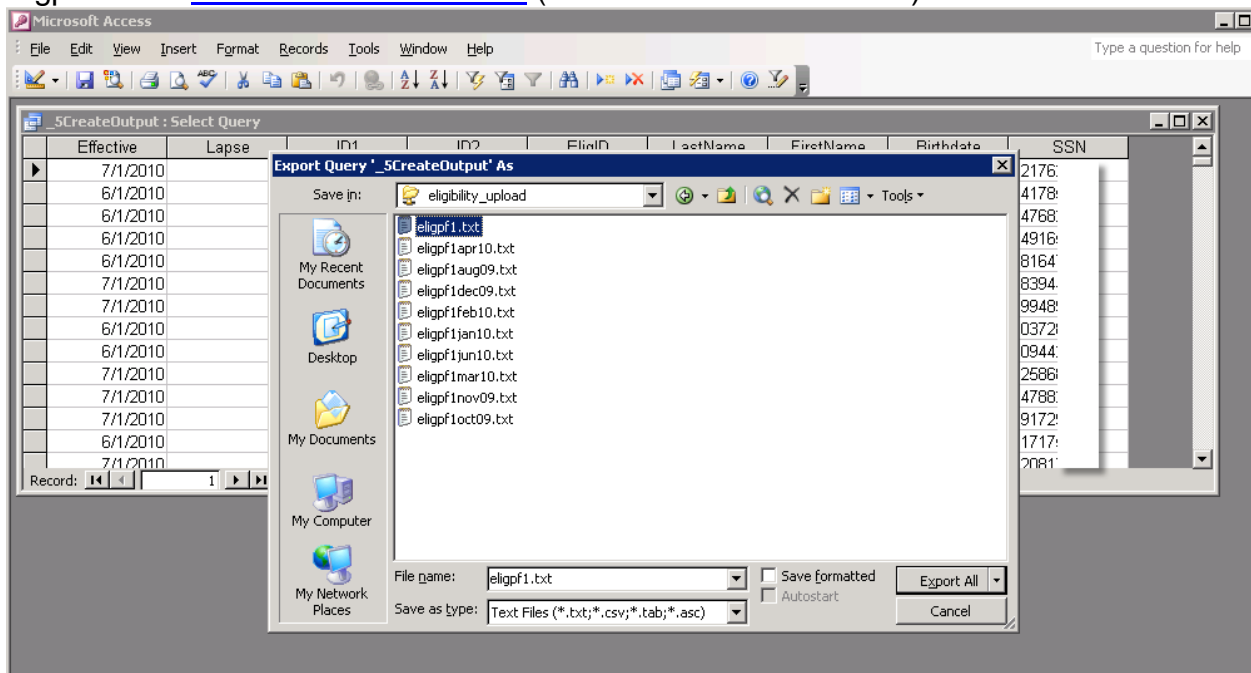
Again, you will get the messages (OK for both) and then close the query (this creates a new DB called CurrentPF)

For both Monthly and Weekly:

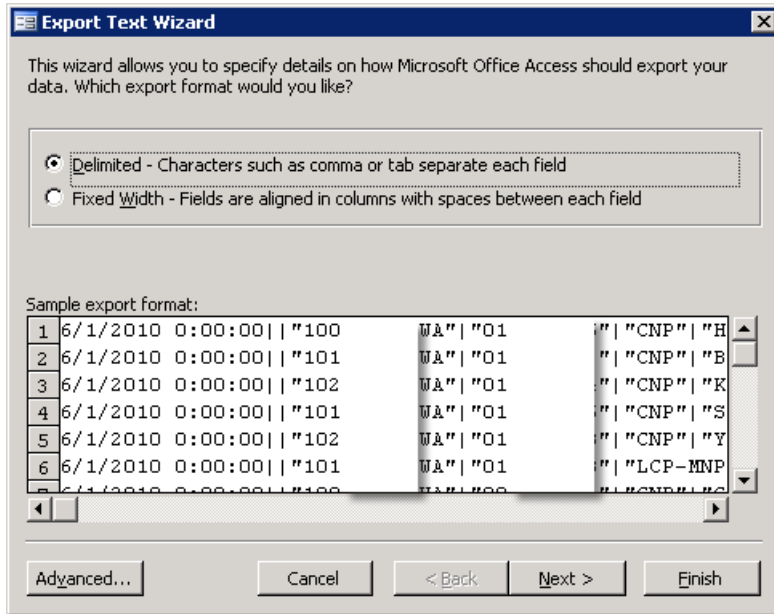
Select _4RvwPFFile (double-click). This opens the newly created file for review. Note the number of records on the bottom of the screen.

If all looks OK, select _5CreateOutput (double-click). This creates a view of the data in the file above – you now need to export the file.

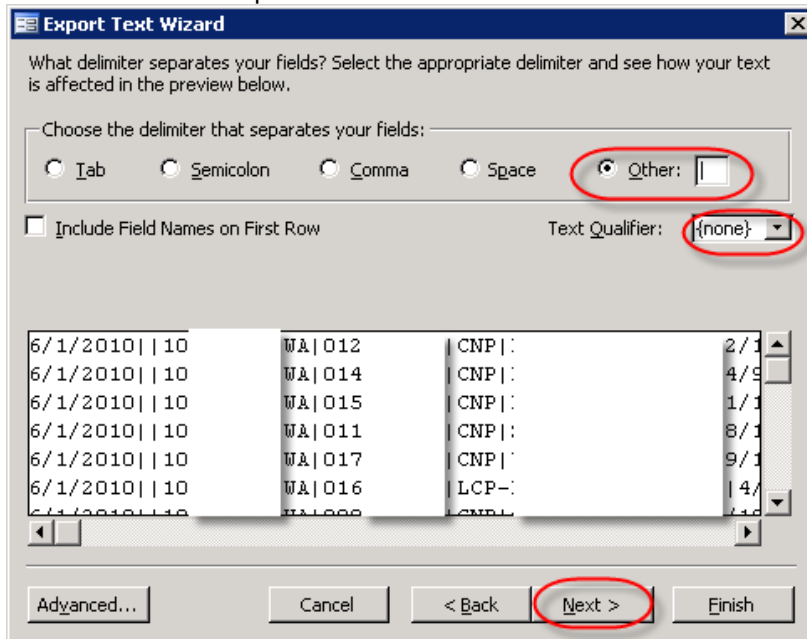
With the file open, select File – Export and export all (file type Text Files) to the filename eligpf1.txt in [\\NAS-1\IS-DOCS\ELIG](#) (You can overwrite this file)



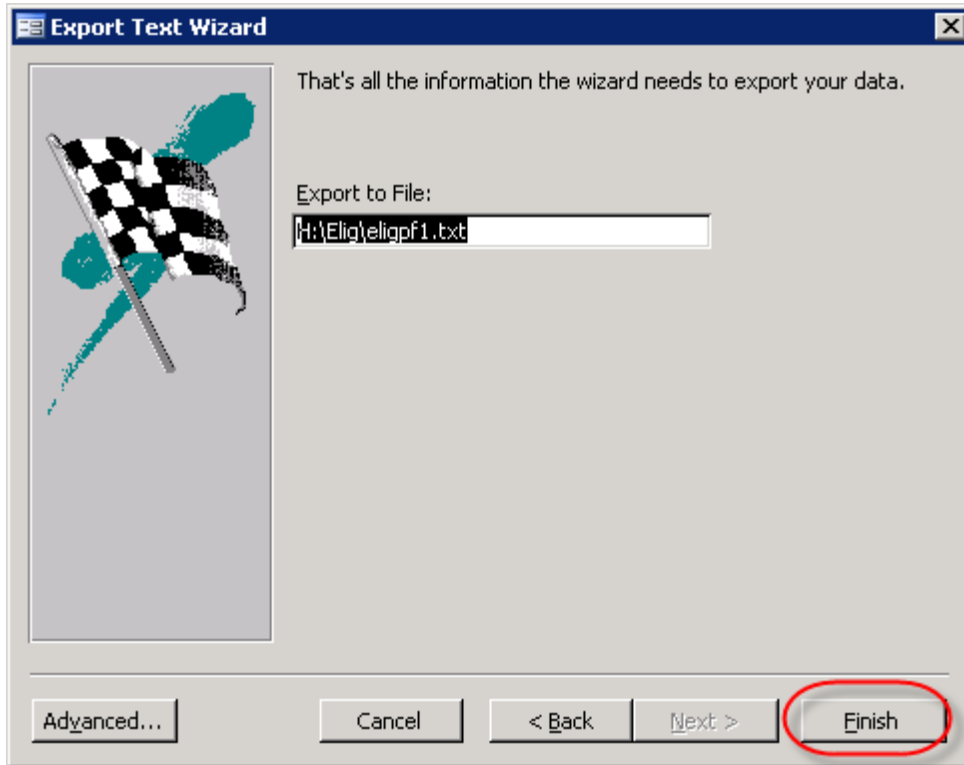
In the formatting – select as follows:
 Delimited – Next



Delimiter – Other | and Text Qualifier None



Finish



You will get a message that the export has finished.
 You can close this database and log off PFTEST.

Import the file into the ProFiler Eligibility database

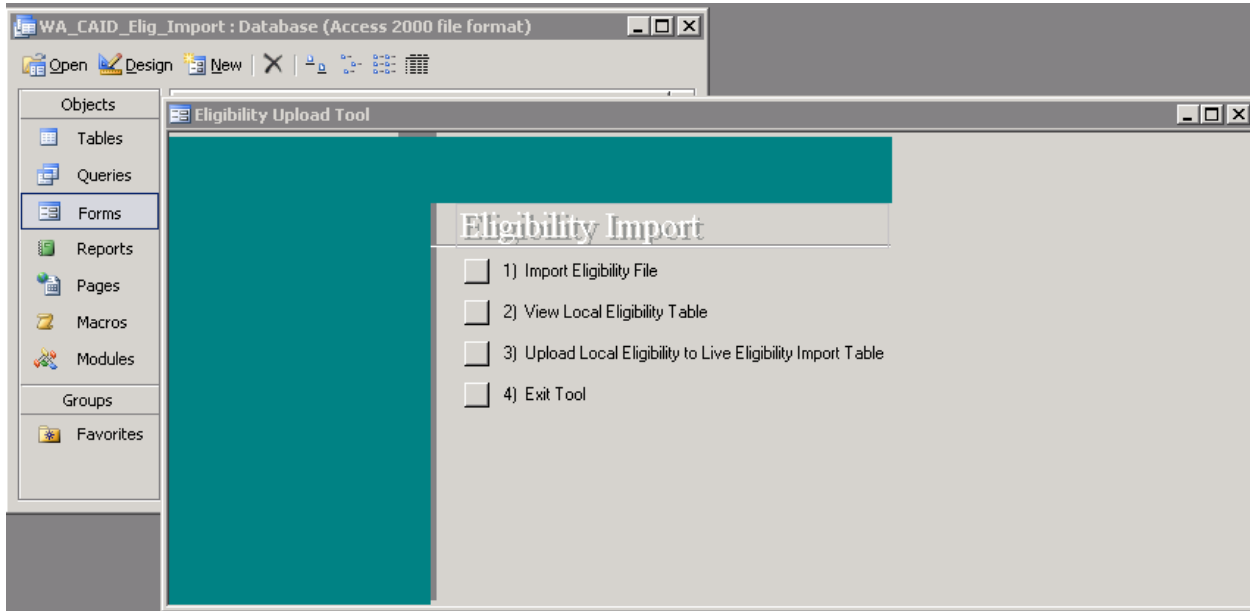
Log onto APPS1 server

Rename the current file called eligpf1.txt (the file name should be eligpfMMDDYYwkly or eligpfMMYYmo)

Move the eligpf1.txt from IS-DOCS\ELIG to APPS1 D:/Eligibility_Upload directory.

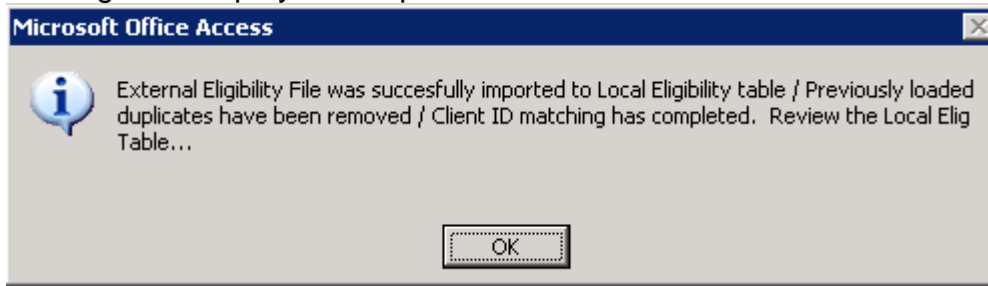
Open Access DB called “**WA_CAID_ELIG_Import.mdb**”

Open FORMS, Then Switchboard



Run item 1: Import Eligibility File (clears local DB, reads eligpf1.txt into local DB, reads Profiler DB, identifies/flags duplicates, marks new items for import by matching ID1+DOB, FN+LN+SSN or FN+LN+DOB)

SQL server login prompts for “sa” password partway thru
 Message will display when queries are done. Click OK



Run item 2: View Local Eligibility Table (make sure today’s date is in last_modified date field)

If ok, close table (NOTE: The record numbers may not match – this process looks for duplicate items and removes them)

Run item 3: Update Local Eligibility to Live Eligibility Import Table (reads local file, compares to Profiler client & payor tables to find matches; matches by name, DOB and/or SSN). Query takes about 1 hour. Message will display when complete. Click OK NOTE: Do NOT run this more than one time

Run item 4: exit tool. Close MS Access and log out of APPS1

Run SQL query to find additional possible matches

Log into UNICARE server as yourself

Find Eligibility.sql on the desktop (should be there for all users) and double-click to open

Connect to Unicare DB

Select database Unicare from the drop down and click Execute – this runs very quickly

Repeat this against the DW server Kitsap DW database.

(purpose is to run some additional queries/views to find matches)

When lower left side of window indicates query ran successfully, close SQL Server

Management Studio and log off Unicare server

Run Update in Unicare DB

Log into Profiler (Unicare live) DB

Open Automation Manager

Check Eligibility Import and click Start

There will be 1 record in the queue and 0 processed – when this changes to at least 1 processed and 0 in queue, click Stop and OK to close Automation Mgr

Run Payor/Episode Association Script in Unicare DB

Log onto the UNICARE server as yourself

Find NEWOther_Payor_Selfpay_Axis_080909.sql on the desktop (should be there for all users) and double-click to open

Connect to Unicare DB

Select database Unicare from the drop down and click Execute

When lower left side of window indicates query ran successfully, close SQL Server Management Studio and log off Unicare server

Repeat this against the DW server Kitsap DW database.

Run Rank90 Script in Unicare DB

While in the Studio Manager, find the Rank90.sql script

Run this against Unicare

Repeat this against the DW server Kitsap DW database.

Notify users Eligibility has completed for monthly processing

Send email to Rose Clemons and Tonya Ferguson (JMHS), Chris Marie Carter (KMHS), Michelle Johnson and Cheryl Miller (PCMHC) and Audrey Grafstrom and Sherrie Richards (WEOS) to notify them the eligibility data is completed.

Filename:

ACTION	INSTRUCTIONS	Date Complete
File Download	Go to the P1 SSH connection (ftp to ftp.waproviderone.org – mode is SFTP). Go to PROD directory, then HIPAA_Outbound directory Select current files and download the files – – you are looking for both 834.O.out and 820.O.out files - they need to end up in the PFTEST D:\Provider One Processing\Files directory. Log off the P1 SFTP	
Update file log spreadsheet	With Filename(s) and date – file is in the binder and blank copies in IS-DOCS/Elig/P1 Eligibility/FileLog.xls	
Add records to Access db	Connect to PFTEST and locate the shortcut for the Access DB P1ImportV6 (click OPEN at the message)	
Scan directory for files	Select first item on switchboard – Scan available 820 and 834 files to Import	
Review files	Select second item on switchboard – Review files prior to Processing – make sure the new files you imported are listed.	
Import 820 Payments	Select third item on switchboard – Import 820 Payment.	
Notify RSN	Notify Anders (337-4886 – aedgertn@co.kitsap.wa.us) the 820 Payment file has been imported.	
Import 834 Eligibility	Select fourth item on switchboard – Import 834 Eligibility – NOTE: Monthly files (determined by size) will take a few hours to import.	
Monthly 834 - Create export file for Profiler	In the PFTEST P1ImportV6 database, run the queries (_1AClearCurrentPF and _1MonthlyAdds and _1MonthlyInfoB. Once completed, run item _5CreateOutput (see instructions for formatting) and save the file in the \\NAS-1\IS-DOCS\ELIG directory called eligpf1.txt (OK to overwrite the file here)	
Monthly 834 Only	Create spreadsheet from the file in Step _1MonthlyInfoB from the table PRSN_Elig_LastMonthly (refer to detailed instructions for export and pivot table creation). Notify Anders Edgerton (aedgertn@co.kitsap.wa.us) that the file is in the PRSN Provider/RSN/P1 Elig directory.	
Weekly 834 - Create export file for Profiler	In the PFTEST P1ImportV6 database, run the queries (_1AClearCurrentPF and _1MonthlyAdds or _2WeeklyAdds and _3WeeklyExp. Once completed, run item _5CreateOutput (see instructions for formatting) and save the file in the \\NAS-1\IS-DOCS\ELIG directory called eligpf1.txt (OK to overwrite the file here)	

<p>Remaining for both Monthly and Weekly files. Rename last month's file on APPS1</p>	<p>Log onto the APPS1 server and go to directory D:\Eligibility_Upload Rename "eligpf1.txt" to "eligfp1mmddy.txt" with the mmddy from the file being processed.</p>	
<p>Copy TS1 Access output to APPS1</p>	<p>Use Filezilla or other transfer program to copy output file from TS1 to APPS1 D:\Eligibility_Upload directory and ensure it is called "eligpf1.txt"</p>	
<p>Import eligibility file to Access DB</p>	<p>Log onto APPS1 server Open Access DB called "WA_CAID_ELIG_Import.mdb" Open FORMS, Then Switchboard Run item 1: Import Eligibility File (clears local DB, reads eligpf1.txt into local DB, reads Profiler DB, identifies/flags duplicates, marks new items for import) SQL server login prompts for "sa" password partway thru Message will display when queries are done. Click OK Run item 2: View Local Eligibility Table (make sure today's date is in last_modified date field) If ok, close table. Run item 3: Update Local Eligibility to Live Eligibility Import Table (reads local file, compares to Profiler client & payor tables to find matches; matches by name, DOB and/or SSN). Query takes about 1 hour. Message will display when complete. Click OK Run item 4: exit tool. Close MS Access and log out of APPS1</p>	
<p>Run SQL query for further matching</p>	<p>Log into UNICARE server as yourself Find Eligibility.sql on the desktop (should be there for all users) and double-click to open Connect to Unicare DB Select database Unicare from the drop down and click Execute – this runs very quickly (purpose is to run some additional queries/views to find matches) When lower left side of window indicates query ran successfully, close SQL Server Management Studio and log off Unicare server and repeat this against the KitsapDW replicated database in DW server.</p>	
<p>Run Update in Profiler Unicare DB</p>	<p>Log into Profiler (Unicare live) DB Open Automation Manager Check Eligibility Import and click Start There will be 1 record in the queue and 0 processed – when this changes to at least 1 processed and 0 in queue, click Stop and OK to close Automation Mgr</p>	

<p>Run Payor to Episode Association and Rank 90 Scripts</p>	<p>Log onto the UNICARE server as yourself Find NEWOther_Payor_Selfpay_Axis_080909.sql on the desktop (should be there for all users) and double-click to open Connect to Unicare DB Select database Unicare from the drop down and click Execute When lower left side of window indicates query ran successfully, close SQL Server Management Studio and log off Unicare server and repeat this against the KitsapDW replicated database in DW server.</p>	
<p>For Monthly Files only: Send email regarding completion</p>	<p>Send email to Rose Clemons and Tonya Ferguson (JMHS), Chris Marie Carter (KMHS), Cheryl Miller (PCMHC) and Audrey Grafstrom and Sherrie Richards (WEOS), CC Anders Edgerton at the RSN to notify them the eligibility data is completed.</p>	

MONITORING

This policy is a mandate by contract.

1. This policy will be monitored through use of PRSN:
 - Annual PRSN Provider and Subcontractor Administrative Review.
 - PRSN will use reports generated by the Department to identify the list of total errors on data submissions.

2. If a provider performs below expected standards during any of the reviews listed above a correction action will be required for PRSN approval. Reference PRSN Corrective Action Plan Policy.



PENINSULA RSN

MANAGEMENT INFORMATION SERVICES POLICIES AND PROCEDURES

Policy Name: DATA TRANSFER TO THE DEPARTMENT **Policy Number:** 4.02

Reference: DSHS Contract

Effective Date: 4/2004

Revision Date(s): 1/2012

Approved by: PRSN Executive Board

CROSS REFERENCES

- Policy: Corrective Action Plan

PURPOSE

To ensure that the Peninsula Regional Support Network (PRSN) maintains a primary and backup system for the transfer of electronic data to the Department.

PROCEDURE

1. The Peninsula Regional Support Network contracts with Kitsap Mental Health Services (KMHS) to manage the Information Services (IS) system utilized by the PRSN.
2. KMHS, as contracted provider for PRSN Information Services, will use the SSH (Secure Shell) method of data encryption for all electronic data transfers to ensure confidentiality.
3. PRSN data is transferred (using the SSH software) to directories in the DSHS data system by connecting to the Virtual Private Network (VPN) via an Internet connection.
 - All data is submitted in accordance with the current Data Dictionary specifications.
 - Encounter data is submitted using HIPAA file formats.

4. In the event internet connectivity is unavailable over a period of 14 calendar days, data will be sent to DSHS using a password-protected CD, DVD or Flash Drive delivered directly to the Department.

MONITORING

This policy is mandated by contract.

1. This policy will be monitored by the PRSN by the following means:
 - Kitsap Mental Health Services will report to the PRSN any loss of VPN services.
 - KMHS and the PRSN will debrief any loss of connection and resolve problems identified.
2. If a provider performs below expected standards during any of the reviews listed above a correction action will be required for PRSN approval. Reference PRSN Corrective Action Plan Policy.



PENINSULA RSN

MANAGEMENT INFORMATION SERVICES POLICIES AND PROCEDURES

Policy Name: IS DATA SUBMISSION PROCEDURES

Policy Number: 4.03

Reference: WAC 388-865-0275

Effective Date: 4/2004

Revision Date(s): 1/2012

Approved by: PRSN Executive Board

CROSS REFERENCES

- Policy: Corrective Action Plan

PURPOSE

The Peninsula Regional Support Network (PRSN) contracts with Kitsap Mental Health Services (KMHS) to operate its Information Services (IS) in accordance with the PRSN's contract with DSHS and the state-issued Data Dictionary.

All providers within the PRSN are connected to KMHS via VPN tunnel connections via the Internet. All providers use the shared ProFiler® Electronic Health Record. RSN clients are distinguished at the Company level by presence of an RSN Payor record. These procedures describe the internal procedures run by specific agencies and KMHS to transfer data to the state.

PROCEDURE

PROVIDER Encounter Preparation Monthly Procedures. As part of normal monthly billing, run edits as defined in current agency billing checklist. Once all edits are completed, services have been posted and the RSN billing batches are created, notify Mary Anne Miller (mam@kmhs.org or 360-415-5859) of the batch name so the 837P files can be created and sent to the state. As stated in contract, each agency is responsible to have their encounters ready for receipt at the state by 60 days after the close of every month. To allow KMHS processing time, it is preferred these files are ready by 45 days after the close of every month.

Once files are sent, KMHS monitors and processes the ETRR files received from the state that acknowledges the receipt and cites any errors. Errors are reviewed and corrections submitted as indicated by KMHS with assistance/clarification from the provider agency as required. Errors must be corrected and resubmitted if indicated within 30 days of the notification from the state.

PROVIDER Weekly Client Data Preparation.

All data required by the current WA State DBHR CIS/Data Dictionary for RSNs must be entered and complete before any client is flagged for RSN services (client has the RSN Crisis or RSN Standard/PACT payors). The current version can be located at <http://www.dshs.wa.gov/dbhr/mhpublications.shtml>.

Once a client record is flagged with the RSN payor, the ProFiler® system checks to ensure all required data is present. If it is not, the state report transaction is held in error until data is corrected. The errors flagged by ProFiler® are sent to the specific agency for correction. Once the data is corrected, the next run in ProFiler® will recognize the correction and include the transaction in the next data send.

If a record clears the ProFiler® system and subsequently errors at the State level, KMH staff review the transactions to ensure there is not a problem with the file that was sent. These errors are corrected by Kitsap Mental Health Services staff (coordinating with the specific agency as needed) and resubmitted.

As specified in contract with WA State DBHR and each agency contract with the RSN, errors must be corrected within 30 days of notification.

MONITORING

This policy is mandated by contract.

1. This policy will be monitored through use of PRSN:
 - Annual PRSN Provider and Subcontractor Administrative Review.
 - PRSN will use a report generated by the Department to identify error statistics and total services received within 60 and 90 days of close of the month in which the service was provided to ensure timeliness is achieved.
2. If a provider performs below expected standards during any of the reviews listed above a Corrective Action will be required for PRSN approval. Reference PRSN Corrective Action Plan Policy



PENINSULA RSN

MANAGEMENT INFORMATION SERVICES POLICIES AND PROCEDURES

Policy Name: IS ENCOUNTER SUBMISSION AND EVALUATION

Policy Number: 4.04

Reference: DSHS Contract

Effective Date: 10/2005

Revision Date(s): 10/2006

Approved by: PRSN Executive Board

CROSS REFERENCES

- Policy: Corrective Action Plan
- Policy: Data Error Resolution

PURPOSE

Network providers within the Peninsula Regional support Network (PRSN) will be responsible for submitting encounter data into the PRSN Management Information System (MIS) according to Department Consumer Information System Data Dictionary by the 18th of each month. Late services will be accepted beyond this time, and must be flagged accordingly. The PRSN MIS contractor shall be responsible for reviewing all data, formatting it, and transmitting it to the state MHD within sixty (60) days of the close of the calendar month in which the encounter occurred.

PROCEDURE

1. Consumer encounters submitted from the Community mental Health Agencies (CMHAs) will be successfully submitted to the PRSN MIS subdelegated contracted by the 18th of the month following service.
2. The PRSN's subdelegated contracted Information Services provider conducts a series of procedures with the data to ensure that it is accurate and prepared to send to the Department of Social and Health Services (DSHS) on behalf of the PRSN.

3. The PRSN monitors submission of data to DSHS via the “RSN Weekly Status Report”, and compares key indicators on the report to statistics reported directly to the PRSN by KMHS off of the PRSN IS database.
 - a. Factors such as numbers served and hours of service per month are matched.
 - b. If specific inconsistencies are found, corrective action is required.

MONITORING

This policy is mandated by contract.

1. This policy will be monitored through use of PRSN:
 - Annual PRSN Provider and Subcontractor Administrative Review.
 - PRSN will use a DSHS report to identify the total services received by the Department within 60 and 90 days of encounter date to ensure timeliness is achieved.
 - PRSN will use a DSHS report to list total services received by the Department to match key indicators with statistical reports run off of the PRSN database.
2. If a provider performs below expected standards during any of the reviews listed above a Corrective Action will be required for PRSN approval. Reference PRSN Corrective Action Plan Policy



PENINSULA RSN

MANAGEMENT INFORMATION SERVICES POLICIES AND PROCEDURES

Policy Name: DATA ERROR RESOLUTION

Policy Number: 4.05

Reference: DSHS Contract

Effective Date: 4/2004

Revision Date(s): 4/2006

Approved by: PRSN Executive Board

CROSS REFERENCE

- Policy: Corrective Action Plan

PURPOSE

To ensure that any errors encountered through the processing of data from providers into the Peninsula Regional Support Network (PRSN) database are addressed and corrected in a timely manner.

PROCEDURE

Event Export / Import - Provider to RSN - Correcting Lattice Errors

This document addresses known errors that have occurred during event processing and explains how to correct them. It is possible at any time for new errors may occur that are not listed here. Contact the Systems Analyst whenever a new error occurs.

Errors are found by looking at the last line of the export or import report in the print queue. Lattice keeps track of errors and prints the message: ***ERRORS NOTED: X. When this message occurs, search the print out to find the specific client and error. Check the Lattice manual to see if the error is listed; the manual should describe the problem such that the reader can fix the problem. Many of the processing errors are not in the manual, however. Follow the instructions below to correct these errors.

Provider Event Export Errors

- No errors in last 4.5 years.

RSN Event Import Errors

*****INVALID SERVICE CODE: 152. EVENT NOT IMPORTED. Error occurs when service code does not exist in the receiving system.

Reason for error and solution:

- It is likely that a new service code was added to the provider database which also needed to be added to the RSNs but wasn't. Check the provider recode table "SACTORSN" for the SAC (Service Activity Code) which is recoding to the invalid RSN service code. Check the PRSN Code Change Form to see what is needed. Correct the provider recode and add event rule if needed. Add the code to the RSN if the form indicates. Reset the provider's events and export them again according to the Event Reset Procedure.

Adding A Service Into The RSN Database

Use this procedure to manually enter a service into the RSN event file. Services only need to be entered manually when an import error occurs. See "Resolving Event Import Errors" for details about why errors happen.

Before a service can be entered into the RSN you must look up the provider codes for the following items and convert them to the RSN codes:

- Staff ID and Reporting Unit
- Location Code
- Service Code

Refer to RSN Service Activity Master & Cross Reference and RSN Location Code Cross Reference to make the conversion.

Two methods are given to add the services to the RSN. The data base administrator may use either one. Both are listed so the DBA can pick whichever entry method they are most comfortable with.

Log on to the RSN system using either own user id. or "ru416".

Method 1: Service Entry Using Function 5.1 (Update Event Record Detail)

Select function 5.1 from the RSN CMHC/MIS main menu. At the functions window select "Add a New Event".

Enter the staff id. which is the provide 3-digit MHD number. See Attachment A.

Enter the client id. This is the RSN unique id., not the provider's client id.

There are two screens of information that need to be entered. The first screen is items 1 - 17. The second screen is items 18 - 31. When you have completed the first screen the system automatically continues to the second screen.

You must make an entry for these items on screen 1: items 1,2,3,4,10,14,15,16. Press <ENTER> through the other items and the system will place defaults in for you, if any.

There are no required items on screen 2. Press <ENTER> through all the items on screen 2 and the system will place defaults in for you.

When you have completed item 31 the prompt line changes to give you a chance to update an item if you made a mistake. Use the F1 and F2 keys to page between the two screens. If you complete the entry and still need to make a correction return to the functions window and select "Update Events".

Method 2: Service Entry Using Function 9.2 (Re-Enter Service/Activity Logs)

Select function 9.2 from the RSN CMHC/MIS main menu. Type in a SAL Control Number such as "999999" (the number isn't important, you just need to put in something to get to the next screen).

Enter the staff id. which is the provider 3-digit MHD number. See Attachment A.

Enter the date of service. Press <ENTER> at Total Time For Day. Continue to the next screen.

Here is a guideline to help make the correct entries:

Prompt	Meaning	What to Type
?	Status of Event	E
RU	Reporting Unit	See Attachment A
L	Location Code	See RSN X-REF
ACT	Service Activity Code	See RSN X-REF
PROJ	Project Code (not used)	Press <ENTER>
GROUP	Group ID (not used)	Press <ENTER>
DUR	Staff Duration	Hours/minutes of service
PREP	Prep. Time (not used)	Press <ENTER>
TIME	Appointment Time (not used)	Press <ENTER>
CLIENT	Client ID	RSN unique id. for client, not provider id.
R	Recipient Code	/ <ENTER>

The slash and <ENTER> signals the program to end the line and fill in the remaining items with defaults. If you have more than one service for a client for the same day you may continue making entries on lines 2 through 22. When all services for this date are entered type "/" and hit <ENTER>. At this point the prompt line changes to give you a chance to update an item if you make a mistake. Type the line number to update, make your changes and then keep hitting the <ENTER> key until you get to another screen showing items 23-44. Type "/" and hit <ENTER> twice and the entry is complete. If you complete the entry and still need to make a correction, use function 5.1 to update events.

NOTE: Service data may result in errors received from the MHD exception report. These errors seldom occur; therefore there is not a master correction instruction. The exception report must be reviewed and any errors must be researched and corrected within 3 business days. Usually these errors are due to client information not being recorded prior to the service data is submitted – before any service corrections, ensure all required client (daily) data is recorded at MHD.

E&T Inpatient Episode Correction Procedures (AIU/YIU)

Corrections to RTC/ATU episodes come to your attention by reading the RSN print out called "CLIENT DB E&T IMPORT".

Find and update the ISN for the episode discharge date: input the "force bill flag" value of "Y". The staff id is 036 and the service code is 500.

Screen print the ISN register. Highlight the ISN Claim Unique ID.

Remove client saved list "ETCOR" if it exists.

Create client saved list "ETCOR".

Update 837I parameter file "CORR837I" used for corrections: check the client saved list name. Make sure the ISA record is set for production. Change the line in the CLM record as follows:

- 7 = change/correct
- 8 = void

Refer to sample page for list of lines to change.

Check the parameter file called "ISASEQ" and update the last batch number sent if needed.

Display the E&T episode for the client and screen print.

Run parameter file with admit/discharge dates from above and prepare production file in /c1/transfers/hipaa.

Print the report called “837ICORR-ET REPORT”. Make sure the ISN Claim Unique ID is the same as the one you highlighted on the ISN screen print. If not the same, contact Mary Anne for help. Copy the report to /c9/cdata and call it ET837IC.xxx where “xxx” is the batch number.

Print the last page of the report called “ANSI 837I Event Rpt”. Delete from print queue after printing; don’t copy this one.

Use JSB file transfer or FTP to transfer batches to your workstation.

Follow instructions to transfer HIPAA batches to MHD and retrieve error reports.

Note: if there is a change to the discharge date after original submission, see Mary Anne. We may have to do some extra things if that happens. Episode change will occur but event will remain the same.

E&T Exception Report – Error Resubmission Procedure

The most common error is when discharge date is prior to admission date. This occurs when we are behind in submitting the inpatient services and the client has multiple layers of inpatient stays.

Log in to the RSN to process the resubmissions. You will need the exception report to tell you the client id’s in error.

- 3.17.2 Print each client’s episode history. Update the record effective date on the appropriate layer (the one that caused the error) to today’s date.
- 11.6 Remove saved list called “ETERRS” if it exists. Then create a new saved list of client id’s to be used in the resubmit process.
- 5.16.2 Search for the ISN for each client based on discharge date and service code 500. Update each ISN (item 25 on the screen) to “Y”. That forces the program to “bill” the service again.
- 2.11 Edit the parameter file called ETERRS and put in the client list name. Change the commands as shown in sample to prepare a test file. Make sure the “claim frequency type code” = 1.
- 15.4.10 Create test file, review, and submit to EDIFECS for error detection. Make sure all clients are included in the file and admit/discharge dates are correct.
- 2.11 Edit ETERRS parameter file to production status as shown in sample.
- 2.11 Display parameter file ISASEQ and make sure next batch number is correct and matches your HIPAA batch log. If not, update as needed.

- 15.4.10 Create production file and submit to MHD according to regular processing procedures. Archive files as usual.
- 3.17.2 Update episode layers back to chronological order (use your screen prints). Make sure this is done before the end of the day you changed them or the daily import of data to the RSN could be updated incorrectly!

MONITORING

This policy is a mandate by contract.

1. This policy will be monitored through use of PRSN:
 - Annual PRSN Provider and Subcontractor Administrative Review.
 - PRSN will use a DSHS report to identify total errors on data submissions.
2. If a provider performs below expected standards during any of the reviews listed above a correction action will be required for PRSN approval. Reference PRSN Corrective Action Plan Policy



PENINSULA RSN

MANAGEMENT INFORMATION SERVICES POLICIES AND PROCEDURES

Policy Name: ACCEPTANCE OF LATE MIS DATA

Policy Number: 4.06

Reference: EQRO Findings, FY 2007

Effective Date: 5/2005

Revision Date(s): 12/2007

Approved by: PRSN Executive Board

CROSS REFERENCES

- Policy: Data Transfer to the Department
- Policy: IS Encounter Submission
- Policy: IS Processing Procedures

PURPOSE

Contracted providers shall attempt to comply with data submission requirements outlined in the State Data Dictionary. If a provider needs to submit data after the cut off for the period in question, the Peninsula Regional Support Network (PRSN) Information Services (IS) contractor shall accept the late data.

PROCEDURE

If a contracted network provider needs to submit data after the data cut off timeframe outlined in the state Data Dictionary, the PRSN Information Services contractor will accept the data submission.

The PRSN IS contractor shall submit the late data to the Mental Health Division.

MONITORING

This policy is mandated by contract.

1. This policy will be monitored by the PRSN by the following means:
 - Kitsap Mental Health Services and the PRSN will identify trends of late MIS data submission from the provider network.
 - Annual EQRO audits and findings. The PRSN will follow-up with any assigned corrective action requirements.
 - Annual PRSN Subdelegation Review of the regional IS system
2. If KMHS performs below expected standards during any of the reviews listed above a Corrective Action will be required for PRSN approval. Reference PRSN Corrective Action Plan Policy
 - Because KMHS contractually provides the PIHP regional Information System, the PRSN has the ability to impose penalties, modify the subdelegation contract, or decide to not continue to contract.



PENINSULA RSN

MANAGEMENT INFORMATION SERVICES POLICIES AND PROCEDURES

Policy Name: DATA SYSTEM BACKUP AND RECOVERABILITY

Policy Number: 4.07

Reference: contract

Effective Date: 4/2004

Revision Date(s): 12/2010

Approved by: PRSN Executive Board

CROSS REFERENCES

- Plan: PRSN Disaster Response Plan
- Policy: Corrective Action Plans

PURPOSE

To ensure the Peninsula Regional Support Network (PRSN) data stored electronically is adequately backed up and plans in place to provide recoverability due to data corruption or a regional computer system failure.

Background

The Peninsula Regional Support Network contracts with Kitsap Mental Health Services (KMHS) to operate and maintain the data system used by all network contractors within the PRSN. The system uses ProFiler/UNICARE software. All PRSN network providers are connected to the data system through either a VPN or a secure Point to Point T1 data connection. KMHS is responsible for maintaining the network, and transmitting required data to the Department of Social and Health Services Mental Health Division.

PROCEDURE

Preparedness

Because of the potential risk and ongoing vulnerability to loss of data, the KMHS Information Services Department has in place a backup and storage policy and procedure that is practiced every working day. These backup procedures would allow KMHS and the other network providers within the PRSN to retrieve critical information

necessary for the conduct of business functions on an immediate basis, and ultimately allow a full restoration of the data system given a catastrophic failure.

Backups

Data backups will occur on a daily basis with tape verification and rotation as follows:

1. Bootable backup:

- Frequency: Each time any updates or changes are made to the system
- Copies: Two
- Storage: IS Lockbox (on-site), designated off-site location

2. Daily backup:

Database File

- Specifics: Production database and files (UNICARE) are backed up by SQL Server 2005 each night at 1:00 a.m. Two days are maintained on the SQL server to allow for fast recovery. These files are then backed up to the KMH tape and on-line backup device.
- Frequency: Daily 1:00 a.m.
- Copies: Two on the SQL Server, image of these sent to daily tape and on-line backup storage.
- Storage: IS Lockbox (tape - on-site), on-line digital backup in the Secure Server Room.

System files

- Specifics: Copies of at least one Application Server, Terminal Server and Automation Manager systems are contained within the nightly backup for quick restoration should it be needed.
- Frequency: Daily 1:00 a.m.
- Storage: Along with main KMH backup system.

3. Situational backup:

- Prior to any major version upgrade to the system(s). These are kept at the designated off-site location until the next major event.

Rotation of backups:

1. Bootable backup:

- 1 copy of current in IS Lockbox (Previous version moved to off-site storage in lockbox)
- 1 copy of current and previous 2 at designated off-site location

2. Daily backup:

- Non end-of period *(see below): IS Lockbox (re-using oldest tapes in rotation)
- Wednesday at designated off-site location
- End of month: Designated off-site location (keep a quarter's worth of monthly tapes – Jan-Mar, Apr-Jun, Jul-Sep, Oct-Dec – then place older tapes back into rotation).
- End of quarter: Designated off-site location (keep 4 quarter's worth – placing oldest tape back into daily rotation).
- End of year: Designated off-site location (keep all yearly tapes). This should be created when all processing is completed and books closed for the FY.

3. Situational backup:

- Keep current and one previous version at designated off-site location

Hard Copy Reports

- Should temporary manual operations be required, monthly reports (data as identified in the Disaster Recovery Plan) from the data system will be copied to a device (ZIP, Flash or CD).

System Restoration and Recovery

Critical Need

The following functions have been identified as critical:

1. Transfer of information to WA State. This includes new data as well as any researched and corrected data. Data is sent directly via the www.waproviderone.org site (logging into the PRSN domain – 1050210) or via the Provider One secure FTP site (sftp:waproviderone.org). Should the preferred secure VPN connection to MHD be unavailable for transfer (for more than 1 week), the following alternative methods shall be used (in order of preference):
 - Files (in approved format) will be transferred to an external device (such as flash or CD) and delivered to MHD in person.
2. Basic client information. This includes information such as scheduled appointments, client contact/ location information, caseload lists. Basic client data mentioned above will be downloaded monthly from ProFiler and written to a flash drive stored in an Excel format and stored at the off-site safe. This file can be loaded to any standard personal computer for access/printing.
3. PRSN eligibility data from the State on a weekly basis. The database (Access database) containing the eligibility information is backed up within the standard nightly backup at KMHS.
4. Payroll, Accounts Receivable, Protective Payee and Accounts Payable at any PRSN agency that uses these features within CMHC. The items described below

will be downloaded monthly in a text or delimited file and written to a flash drive stored in the off-site safe. This would require, at a minimum, the following to allow these crucial business functions to be manually processed:

- Payroll: Listing of staff pay scales, FTE, deductions.
- Accounts Receivable: Listing of client balances from each funding source.
- Protective Payee: Listing of current balances and check details for current FY.
- Accounts Payable: Listing of vendors and Journal Detail/General Ledger information for the current FY.

All other services could be deferred to the recovery stage.

Recovery

The main impacts of catastrophic loss of computer equipment or extended delays in resuming full processing capacity would be delays in financial and statistical procedures: reports and backlogs of client and activity information to be entered. This would not affect services to the public following an emergency, but could have effect to the provider financial stability and ability to determine impact.

1. The provider information systems would face difficulties in returning to full production in the face of backlogs, if the system were unavailable for more than one month, under normal circumstances. Staff shortage and unusual demand for services would make the need more critical. Business department needs would be given first priority if computer access were limited.
2. Finance could tolerate a 1-2 month delay, depending on the timing of checks to be processed.

Use of On-Line Terminals during and after a system failure or natural disaster

- Responsibilities

The most critical computer functions will be assigned to any terminals that remain on-line at KMHS.

- First Priority

1. Verify that the ProFiler and CMHC systems are still functioning safely, and will have a source of continuous power.
 - a. Physically inspect the computer room and status of UPS.
 - b. An Information Systems staff (usually the IS Director) at Kitsap Mental Health Services will determine if the computer must be shut down.
2. Verify that terminal locations function properly and the areas are safe to work in.

- Second Priority

1. After critical needs are met, allocate existing terminal access for emergency use by Jefferson Mental Health, West End Outreach and/or Peninsula Community Mental Health Services at Kitsap Mental Health Services locations.
2. Information Services staff from Kitsap Mental Health Services will be assigned to assist each site staff at KMH locations as needed.

Use of a Portable Computer as a Terminal during and after a system failure or natural disaster

- Responsibilities

A portable PC may be assigned to replace or supplement office terminals. The portable PC must be equipped with a modem for dial-up connectivity or, preferably, high speed Internet to connect to the PRSN VPN system.

- First Priority

1. If the Information Services offices are inaccessible, but the ProFiler, CMHC systems and phone lines are working, assign at least one laptop to serve as a terminal in a remote location.
 - a. Set up laptop in location with electricity and a phone jack.
 - b. Secure Internet connection with the KMHS VPN client installed (IP 66.81.199.165 or <https://secure.kmhs.org>)

- Second Priority

1. After critical needs are met, allocate existing access to Jefferson Mental Health, West End Outreach and Peninsula Community Mental Health staff for maintaining data processing.

Connection to and use of a CMHC “HOT SITE” during and after a system failure or natural disaster

- Responsibilities

Critical services for clients must be maintained by extracting or entering data in the system. If the CMHC system is not running, an emergency backup may be run at another location. Potential hot sites would include CMHC Systems in Dublin, Ohio; Jet Computers in Olympia, Washington; and Spokane Mental Health in Spokane, Washington. There would be costs associated with this hot site usage that would require negotiation at the time of the need.

- First Priority

1. Data necessary for direct client services.
 - a. Retrieve most recent CMHC backup tape from lock box in Room 508 (Note: If the hot site does not have BRU as a backup program, the weekly TAR

backup will have to be used – or the BRU could be provided to the remote site for installation).

- b. If Room 508 (located at KMHS main campus) is inaccessible, retrieve most recent backup tape (BRU or TAR format) from the safe located at 900 Sheridan, Bremerton, Washington.
- c. Load /c1/RSN, /c0/MIS, /c2/FKS, /c3/PT, /c4/IMAGEFILE and /c5/PA at hot site.
- d. Depending on location, dial in or have staff at hot site log on and print reports designated in the Critical Need section of this document.

- **Second Priority**

If KMHS staff may sustain access to the hot site, the following functions may be run, depending on time and equipment available.

1. Additional lists of staff or client, inventory, or financial/statistical reports for urgent needs.
2. Data lookups or updates for service to existing clients.
3. New client registers and services.

Information Services Evacuation Plan During a Natural Disaster

The following actions should be taken by KMHS IS staff upon evacuation and/or other assigned disaster prep staff upon assignment:

Upon initial evacuation:

IS Staff from room 508 (located on KMHS main campus) will take contents of the lock box. This lock box is located in room 508, by door. This lock box contains:

1. Nightly backup tapes from the IBM and Windows servers
2. Agency master key
3. Safe combination (for safe located at Sheridan facility)
4. Up-to-date IS, Agency, Cell Phone and vendor POC listing
5. Recovery procedures (data/programs, etc)
6. IS inventory listing
7. IS Recovery staff listing and responsibilities

Upon re-entrance/secure actions:

1. The main computer systems (room 508 computer room, labeled in orange) will be powered off and CPUs removed.
2. The computer designated for the DBA (room 508, labeled in orange) will be powered off and the CPU removed.

3. If power is on and water is present in room 508 or computer room, power should be secured via the circuit breakers. Any circuit breaker work must be coordinated with KMHS Facilities staff.
4. The telephone system computer (phone equipment room, labeled in orange) will be powered off and the CPU removed.
 - If power is on and water is present in phone equipment room, power should be secured via the circuit breakers. Any circuit breaker work must be coordinated with KMHS Facilities staff.
5. The IS companion telephones (assigned to the Help Desk and Computer/Telecommunication Technicians) will be removed and offered to command post for assistance (local on-campus communications only).
6. Additional charged batteries (as many as available) and charger units for companion phones.
7. If additional threat, the safe located at 900 Sheridan (Bremerton, WA) should be removed from area as soon as possible. This safe contains:
 - a. Master copies of software.
 - b. Master and scheduled backup tapes
 - c. Up-to-date IS POC listing
 - d. Disaster Plan (data/programs, etc)
 - e. IS inventory listing (quarterly run)
 - f. Critical printouts (identified in plan)

MONITORING

1. This policy is mandated by contract. This policy will be monitored by the PRSN by the following means:
 - Kitsap Mental Health Services and the PRSN will debrief any extended down-time and/or restoration action and resolve problems identified.
 - Annual EQRO audits and findings. The PRSN will follow-up with any assigned corrective action requirements.
 - Annual PRSN Subdelegation Review of the regional IS system
2. If KMHS performs below expected standards during any of the reviews listed above a Corrective Action will be required for PRSN approval. Because KMHS contractually provides the PIHP regional Information System, the PRSN has the ability to impose penalties, modify the Subdelegation contract, or decide to not continue to contract.

Addendum 1- KMHS IS Staff Contact Information

IS STAFFING AND RECOVERY RESPONSIBILITIES

1. All Staff have been instructed to contact Tracy Thompson for the following assigned duties:

- *If staff are unable to contact Tracy, they have been instructed to call their office phone numbers to communicate (pick-up and leave messages for her and other team members).*

Tracy Thompson, IS Director

Overall management and oversight of the recovery. This is the first staff to be contacted. She will direct all other staff with specific recovery actions.

Office – 360-415-5813

Home – 360-479-5476

Cell – 360-271-9879

Tracy maintains a list of personal contact information for all of the IS staff list- not available for distribution.

Network/Phones/Hardware

Jim Reichel, Telecommunications/Network Technician - Network and hardware recovery.

Office – 360-415-5811

Home –

Paul Benter, System Administrator/Technician – Network and hardware recovery.

Office – 360-415-5812

Cell –

Database for UNI/CARE (ProFiler) and CMHC – Note specialties:

Mary Anne Miller, Lead Systems Analyst – Billing, Payroll, Encounters, Eligibility

Office – 360-415-5859

Home -

Cell –

Beth Heinz, Systems Analyst – Clinical systems

Office – 360-415-5817

Cell –

Cynthia Wooten, Systems Analyst – Medical services, Transcription, InPatient data

Office – 360-415-5814

Home -

Cell -

Emily Pechia, Data Specialist - Data validation

Office -360-415-5818

Home -

Cell -

Adrienne Sablan, EMR Clinical Help Desk – Communication with users

Office - 360-415-5858

Home –

Cell –

Data System Back-up and Recovery Testing

PROCEDURE – This information is reviewed and tested annually in January.

Backups

Data backups will occur on a daily basis with tape verification and rotation as follows:

1. Bootable backup:

- Frequency: Each time any updates or changes are made to the system
- Copies: Two
- Storage: IS Lockbox (on-site), designated off-site location
- **Testing 1/2010: Verified backups on site and in the off-site location for all servers (system state backups).**

2. Daily backup:

Database File

- Specifics: Production database and files (UNICARE) are backed up by SQL Server 2005 each night at 1:00 a.m. Two days are maintained on the SQL server to allow for fast recovery. These files are then backed up to the KMH tape and on-line backup device.
- Frequency: Daily 1:00 a.m.
- Copies: Two on the SQL Server, image of these sent to daily tape and on-line backup storage.
- Storage: IS Lockbox (tape - on-site), on-line digital backup in the Secure Server Room.
- **Testing 1/2010: Restored test database from the backup file of the live database. Connected to the database and verified functionality. Verified system state backup from on-line storage and copies in the off-site safe.**

System files

- Specifics: Copies of at least one Application Server, Terminal Server and Automation Manager systems are contained within the nightly backup for quick restoration should it be needed.
- Frequency: Daily 1:00 a.m.
- Storage: Along with main KMH backup system.
- **Testing 1/2010: Verified system state backup from on-line storage and copies in off-site safe.**

3. Situational backup:

- Prior to any major version upgrade to the system(s). These are kept at the designated off-site location until the next major event.

- **Testing: Verified last copy of ProFiler system performed after the version upgrade to 2009 on 11/6/2009.**

Rotation of backups:

1. Bootable backup:

- 1 copy of current in IS Lockbox (Previous version moved to off-site storage in lockbox)
- 1 copy of current and previous 2 at designated off-site location
- **Testing 1/2010: Verified copy of current system state in IS lockbox. Verified storage at off-site location.**

2. Daily backup:

- Non end-of period *(see below): IS Lockbox (re-using oldest tapes in rotation)
- Wednesday at designated off-site location
- End of month: Designated off-site location (keep a quarter's worth of monthly tapes – Jan-Mar, Apr-Jun, Jul-Sep, Oct-Dec – then place older tapes back into rotation).
- End of quarter: Designated off-site location (keep 4 quarter's worth – placing oldest tape back into daily rotation).
- End of year: Designated off-site location (keep all yearly tapes). This should be created when all processing is completed and books closed for the FY.

3. Situational backup:

- Keep current and one previous version at designated off-site location

Hard Copy Reports

- Should temporary manual operations be required, monthly reports (data as identified in the Disaster Recovery Plan) from the data system will be copied to a device (ZIP, Flash or CD).

System Restoration and Recovery

Critical Need

The following functions have been identified as critical:

1. Transfer of information to WA State. This includes new data as well as any researched and corrected data. Data is sent directly via the www.waproviderone.org site (logging into the PRSN domain – 1050210) or via the Provider One secure FTP site (sftp:waproviderone.org). Should the preferred secure VPN connection to MHD be unavailable for transfer (for more than 1 week), the following alternative methods shall be used (in order of preference):
 - Files (in approved format) will be transferred to an external device (such as flash or CD) and delivered to MHD in person.

- **Testing 1/2010: Tested creating files as sent to the state on password protected Flash Drive. Verified data readability successfully.**
2. Basic client information. This includes information such as scheduled appointments, client contact/ location information, caseload lists. Basic client data mentioned above will be downloaded monthly from ProFiler and written to a flash drive stored in an Excel format and stored at the off-site safe. This file can be loaded to any standard personal computer for access/printing.
 - PRSN eligibility data from the State on a weekly basis. The database (Access database) containing the eligibility information is backed up within the standard nightly backup at KMHS.
 - **Testing 1/2010: Files downloaded from ProFiler (Excel and MS Word formats) opened for readability successfully. Data restored from system backup. Successful opening and operation of restored database (MS Access).**
 3. Payroll, Accounts Receivable, Protective Payee and Accounts Payable at any PRSN agency that uses these features within CMHC. The items described below will be downloaded monthly in a text or delimited file and written to a flash drive stored in the fire-proof disaster plan box in IS Tech office (room 508). This would require, at a minimum, the following to allow these crucial business functions to be manually processed:
 - Payroll: Listing of staff pay scales, FTE, deductions (CMHC Report ACSTFALL) – weekly reports, saved off monthly
 - Accounts Receivable: Listing of client balances from each funding source (AR Aging Report from ProFiler)
 - Protective Payee: Listing of current balances and check details for current FY.
 - Accounts Payable: Listing of vendors and Journal Detail/General Ledger information for the current FY.

All other services could be deferred to the recovery stage.

 - **Testing 1/2010: Files downloaded from ProFiler (Excel and MS Word formats) opened for readability successfully. Data restored from system backup. Successful opening and operation of documents.**

Recovery

The main impacts of catastrophic loss of computer equipment or extended delays in resuming full processing capacity would be delays in financial and statistical procedures: reports and backlogs of client and activity information to be entered. This would not affect services to the public following an emergency, but could have effect to the provider financial stability and ability to determine impact.

1. The provider information systems would face difficulties in returning to full production in the face of backlogs, if the system were unavailable for more than one month, under normal circumstances. Staff shortage and unusual demand for services would make the need more critical. Business department needs would be given first priority if computer access were limited.

2. Finance could tolerate a 1-2 month delay, depending on the timing of checks to be processed.

Use of On-Line Terminals during and after a system failure or natural disaster

- Responsibilities

The most critical computer functions will be assigned to any terminals that remain on-line at KMHS.

- First Priority

1. Verify that the ProFiler and CMHC systems are still functioning safely, and will have a source of continuous power.
 - a. Physically inspect the computer room and status of UPS.
 - b. An Information Systems staff (usually the IS Director) at Kitsap Mental Health Services will determine if the computer must be shut down.
2. Verify that terminal locations function properly and the areas are safe to work in.

- **Testing 1/2010: Weekly testing continues of access to all servers from systems contained within the IS Computer Room. On-going access verified via the external VPN connections.**

- Second Priority

1. After critical needs are met, allocate existing terminal access for emergency use by Jefferson Mental Health, West End Outreach and/or Peninsula Community Mental Health Services at Kitsap Mental Health Services locations.
2. Information Services staff from Kitsap Mental Health Services will be assigned to assist each site staff at KMH locations as needed.

Use of a Portable Computer as a Terminal during and after a system failure or natural disaster

- Responsibilities

A portable PC may be assigned to replace or supplement office terminals. The portable PC must be equipped with a modem for dial-up connectivity or, preferably, high speed Internet to connect to the PRSN VPN system.

- First Priority

1. If the Information Services offices are inaccessible, but the ProFiler, CMHC systems and phone lines are working, assign at least one laptop to serve as a terminal in a remote location.
 - a. Set up laptop in location with electricity and a phone jack.
 - b. Secure Internet connection with the KMHS VPN client installed (IP 66.81.199.165 or <https://secure.kmhs.org>)

- Second Priority

1. After critical needs are met, allocate existing access to Jefferson Mental Health, West End Outreach and Peninsula Community Mental Health staff for maintaining data processing.

Connection to and use of a CMHC “HOT SITE” during and after a system failure or natural disaster

- Responsibilities

Critical services for clients must be maintained by extracting or entering data in the system. If the CMHC system is not running, an emergency backup may be run at another location. Potential hot sites would include CMHC Systems in Dublin, Ohio; Jet Computers in Olympia, Washington; and Spokane Mental Health in Spokane, Washington. There would be costs associated with this hot site usage that would require negotiation at the time of the need.

- First Priority

1. Data necessary for direct client services.

- a. Retrieve most recent CMHC backup tape from lock box in Room 508 (Note: If the hot site does not have BRU as a backup program, the weekly TAR backup will have to be used – or the BRU could be provided to the remote site for installation).
- b. If Room 508 (located at KMHS main campus) is inaccessible, retrieve most recent backup tape (BRU or TAR format) from the safe located at 900 Sheridan, Bremerton, Washington.
- c. Load /c1/RSN, /c0/MIS, /c2/FKS, /c3/PT, /c4/IMAGEFILE and /c5/PA at hot site.
- d. Depending on location, dial in or have staff at hot site log on and print reports designated in the Critical Need section of this document.

- Second Priority

If staff may sustain access to the hot site, the following functions may be run, depending on time and equipment available.

1. Additional lists of staff or client, inventory, or financial/statistical reports for urgent needs.
2. Data lookups or updates for service to existing clients.
3. New client registers and services.

Information Services Evacuation Plan During a Natural Disaster

The following actions should be taken by KMHS IS staff upon evacuation and/or other assigned disaster prep staff upon assignment:

Upon initial evacuation:

IS Staff from room 508 (located on KMHS main campus) will take contents of the lock box. This lock box is located in room 508, by door. This lock box contains:

1. Nightly backup tapes from the IBM and Windows servers

2. Agency master key
3. Safe combination (for safe located at Sheridan facility)
4. Up-to-date IS, Agency, Cell Phone and vendor POC listing
5. Recovery procedures (data/programs, etc)
6. IS inventory listing
 - **Testing 1/2010: Verified contents of the IS Lock Box.**

Upon re-entrance/secure actions:

1. The main computer systems (room 508 computer room, labeled in orange) will be powered off and CPUs removed.
2. The computer designated for the DBA (room 508, labeled in orange) will be powered off and the CPU removed.
3. If power is on and water is present in room 508 or computer room, power should be secured via the circuit breakers. Any circuit breaker work must be coordinated with KMHS Facilities staff.
4. The telephone system computer (phone equipment room, labeled in orange) will be powered off and the CPU removed.
 - If power is on and water is present in phone equipment room, power should be secured via the circuit breakers. Any circuit breaker work must be coordinated with KMHS Facilities staff.
5. The IS companion telephones (assigned to the Help Desk and Computer/Telecommunication Technicians) will be removed and offered to command post for assistance (local on-campus communications only).
6. Additional charged batteries (as many as available) and charger units for companion phones.
7. If additional threat, the safe located at 900 Sheridan (Bremerton, WA) should be removed from area as soon as possible. This safe contains:
 - a. Master copies of software.
 - b. Master and scheduled backup tapes
 - c. Up-to-date IS POC listing
 - d. Disaster Plan (data/programs, etc)
 - e. IS inventory listing (quarterly run)
 - f. Critical printouts (identified in plan)



PENINSULA RSN

ADMINISTRATION POLICIES AND PROCEDURES

Policy Name: MANAGEMENT ATTESTATION OF ACCURACY OF DATA

Policy Number: 4.08

Reference: DSHS Contract , 42 CFR 438

Effective Date: 8/2004

Revision Date(s): 12/2007

Approved by: PRSN Executive Board

CROSS REFERENCES

- Policy: Corrective Action Plan

PURPOSE

To ensure that required data submitted to Department of Social and Health Services (DSHS) is complete and accurate.

DEFINITIONS

Management Certification: Federal regulations require that utilization data be certified by management prior to submission to the Department.

PROCEDURE

1. The Peninsula Regional Support Network (PRSN) Administrator certifies the accuracy of all data submitted to DSHS.
2. Data is certified at the time of batch transmission to the Department.
3. The PRSN has authorized all edits and audits used by the PRSN Information Services contractor Kitsap Mental Health Services (KMHS) and providers to ensure data is managed in accordance with the Data Dictionary and Trading Partner Agreement as described below.

- These processes provide PRSN Administration staff with the ability to ensure accuracy of data prior to submission to DSHS.
4. Data entry screens used by providers to enter all information is controlled, utilizing tables that allow entry of only authorized values in client records. The authorized tables are as specified in the Data Dictionary.
 5. Clients identified as RSN clients are not allowed to be sent to the RSN database until all required elements are completed.
 6. Prior to any service/encounter information generation, all PRSN providers review miscellaneous audit reports and correct data within prescribed timelines.
 7. PRSN Administrator is notified by email of any encounter data as it is being transmitted to DSHS to provide for the HIPAA Encounter Certification.
 - This form is completed by the PRSN Administrator for each encounter (HIPAA) claim submitted.

MONITORING

This policy is a mandate by contract and statute.

1. This policy will be monitored through use of PRSN:
 - Monthly Provider Chart Reviews
Data integrity is assessed on a random sample of charts to ensure that encounter data submitted to the PRSN is documented in the clinical file and that all documented encounters are submitted to the IS system.
 - PRSN IS Attestation document transmitted via email, daily- with a monthly letter signed.
2. If a provider performs below expected standards a Corrective Action Plan will be required for PRSN approval. Reference PRSN Corrective Action Plan Policy