Introduction and System Administrator's Guide to

RW CAREWare 5.0

Document Date: August 2011

Draft 4

From stand-alone to wide area network to the Internet:
A scalable software application for managing and monitoring HIV Care

SECTION ONE: Overview

Sharing Data and Granting Access Rights

First, let's review how data are shared in CAREWare and how access rights to the system and to specific data will be granted and administered. As an example, we'll consider an imaginary Part B grantee that funds 30 providers across the state; these providers offer the full range of services funded by the CARE Act. In the part of the state with a higher prevalence of people living with HIV, there are multiple primary care providers, substance abuse and mental health agencies funded by the CARE Act. There are also likely a handful of providers in this state that do not want to join the network, perhaps because they already have a well-established health information system in their hospital or clinic, or they simply elect not to be connected to the network in real-time; these latter providers would be set up as PDI providers (see below).

NEED-TO-KNOW: CAREWare has a great deal of flexibility with regard to granting and denying access to which users can view and/or edit data. Users on the network access client data on a "need-to-know basis"- that is, they can see and share client data when it is necessary, and be denied access to client data when it is unnecessary. This arrangement is obviously a critical data privacy feature of CAREWare.

Grantee and Provider Domains: Who does what

In this section we refer to two domains: the central domain, typically the grantee — and the provider domain. In conjunction with providers, the grantee administrator creates users IDs and passwords at the provider level, but it is the grantee administrator who ultimately has the authority to create (and revoke) user IDs and expand or limit how an individual user at a provider may access data.

Providers can designate their own administrator. The provider administrator has full read/write access to the data and can even manage users at their agency, while the grantee administrator manages the full central database contributed to by all providers on the network. The provider administrator, in turn, assigns users and determines access rights at his or her own agency, but all rights at the provider level are ultimately controlled by the grantee administrator.

In CAREWare there is a great deal of flexibility in creating user accounts. Certain users may have full read/write access to their agency's data, while access rights of other users may be more restricted to entering or viewing only certain parts of the data such as demographic and service screens or case notes. (Note that read access means that you can only view the data and cannot edit it; write access means that you can change or edit the data.) Other users may only be granted the rights to run reports.

USER Groups: Grantees and provider administrators can create Groups for specific user types. For example, you may want to establish an account for users who can enter service data only and who can run reports, or perhaps another group that has the rights to view clinical information including labs and medications, but not edit that data. Once a user group is created, those groups can be readily assigned to other users, thus eliminating the need to create entire users from scratch. CAREWare is flexible—very specific user types and rights can be established.

Grantees obviously play a number of important roles overseeing the daily technical functioning of the network; they are also charged with overseeing the proper use of the system, *examining audit trails* of how the system is being used (or misued) and who is using it. Provider administrators also play a critical role in overseeing the daily functioning of their agency's database operations and use of the system.

In addition to Central Users and Provider users, CAREWare allows the establishment of Regional Users. Regional Users are a special type of central user that can only access data at specific providers to which they have been assigned. These data access rights limit which providers can be accessed, and what providers are included in cross provider

central reports they may run. A detailed description of how to set up Regional Users can be found in the CAREWare user manual.

Important Data sharing rules and security issues

Note: Users running CAREWare simply as a standalone application on one PC, or forwarding data in batch (e.g. monthly) to the central administrator via the PDI, will not share data with other providers and therefore DO NOT need to concern themselves with data-sharing issues across a network! However, if you are established as a standalone or PDI provider, you can still join a real-time network down the road.

Data-Sharing Across Providers: It is important to clarify some important features of data-sharing in CAREWare.

- If you elect to share data with another provider, you share data ONLY on the clients that you have in common with that other provider; in short, *I can never see information on clients served at your agency that I don't also serve.* That access would clearly not meet the need to know criteria.

- **Demographic and Annual Review Data**: For years CAREWare always shared this common data across providers if they share the same Client. Demographic sharing is still the default configuration, but as of build XXX, CAREWare also has the option to turn common data completely off. When common data is turned off, even if two providers serve the same client, changes to a demographic field will not be reflected when another provider looks up the same client. This setting only affects common fields across real-time providers on the network, including demographics, data entered on the Annual Review tab—HIV Status, Primary insurance, source of primary care, poverty level, Housing Arrangement—and certain custom fields. So, for example, if common data is turned on, if one provider edits the address, changes the ethnicity of a client, or updates his or her HIV/AIDS status, those changes will be seen by and also can be edited by any other provider who has view and edit rights to that client's demographic data. Grantees can use audit trails to determine if important client identifying information (or any other data, for that matter) is being modified improperly.
- ***Remember that a provider can never edit another provider's service, clinical, and other data even though they may have been granted the right to view that data (this is called "read only access")***.

  In these cases, information is owned by the provider that rendered the service. Again, demographic and annual review data are common managed under a separate setting.
- In network configurations, all data, including personal identifying information such as *client names, dates of birth, addresses, etc. are stored centrally on the grantee administrator's database server (the data tier).* Of course, as outlined below, all data transmitted between the client tier (the user) and the business tier on the server in version 5.0 are encrypted and will require a public/private key to decrypt (see technical section below for details). Client-identifying data, including client's name, date of birth, and address can also be encrypted before being stored on the central data tier, thus further restricting the ability to decipher this sensitive data at the cost of slower reports (because the data is always being decrypted and passed around in algorithms). Again, please refer to the accompanying system-administrator section for technical information on encryption of data in CAREWare.

- **TO SHARE OR NOT TO SHARE:** Each provider must determine which (and whether) other providers, or provider types, can view service data when they share a client.

Data Sharing Configurations: Services, Clinical Information, and Case Notes

For service records, there are three levels or data-sharing configurations available to the individual provider:

- ***Level I:*** All other providers can view your agency's service records. This is obviously the most open setting, and will allow other agencies, regardless of the type of services they

provide, to view service records for clients that you both serve.

- ***Level II**:* A provider shares service records ***only** with other providers that offer the same service type.* For example, a primary medical care provider would share service records with other medical providers (a service "need to know" basis) on the network. However, if a primary care clinic also offers mental health services, a second primary care provider that does not offer mental health services would only be able to view medical care services and **not** the mental health service records from the other agency for the clients they share.

- ***Level III:*** Do not share service records with any other providers. This is the most restrictive level.

Client-by-client option

To accommodate special client requests, providers using either Level I or II may also share service records on a client-by-client basis. Providers who choose this option will grant specific providers permission to see specific clients' service records. Other providers may request to view a particular client's service records, and the original provider, in conjunction with the client, may grant or deny permission.

- Requests made of other providers on the network - for example to view data or make a referral - can be made through a convenient internal messaging system.

How Demographic Data Are Handled with common data turned on

As noted, when common data is on, unlike almost all other data, which are owned by each provider that renders services to a given client, demographic and annual review data have common ownership. It is in this sense that centralized data storage is, by definition, unduplicated; individuals appear only once in the database, even if they are served by multiple providers.

If your agency enrolls a new client whose URN is identical to a client already in the database (and they are genuinely different people), CAREWare will require you to enter an additional letter to the end of the URN in order to distinguish the two clients. For example, if Jane Doe, born on January 15, 1960, is in the database, her URN will (by default) have the letter 'U' (for unique) appended: JNDE01151960U. If a client named Janice Doebay, born on the same date, enrolled in the same clinic, her URN would be 'JNDE01151960A', the only distinction being the last letter. (If you enroll more clients with the same base URN, the last letter would be B, and then C, and so forth.) The CAREWare screen on which users unduplicate clients shows other identifying features of the clients, including their addresses and racial/ethnic designation, so that users can clearly distinguish them.

How Demographic Data Are Handled with Common Data turned off

If you turn off common data, providers will have completely separate demographic data for each client, even when a client is also served by another provider on the network. To the user, CAREWare will act as if their data were on completely different servers from all other providers. CAREWare will still maintain a silent unduplicated list of clients for central analysis and reporting, but the user at the provider will see no visual cue that this is happening.

With common data turned on, when one provider adds a client to its domain, and the URN matches an existing record at another provider, the user is asked for confirmation to make the link. With common data turned off, CAREWare will still notice the link (based on URN), but the user will not be made aware of it and he or she will enter all demographics from scratch for their domain.

Restricting PII for reports for certain users

Some providers and grantees may want to grant certain users the right to run reports for quality

control and reporting, but not allow them to see PII. This can be accomplished by restricting the user's ability to lookup an individual client, and then disabling the PII fields in the CAREWare report engine. This can be done for Central, Provider and Regional users. Please refer to the CAREWare user manual for a detailed description of how to accomplish this.

Client ID Field: exception to shared Demographic Data

Although it appears on the demographic screen, the client ID field is provider-owned, not a common field; hence clinics can store their own identifier, such as a clinic chart number.

The example of John Doe with Common Data

Let's say Provider #1 in the network first sees a client named John Doe in 2002. Provider #1 offers primary care and mental health services. In the next year, Mr. Doe enrolls at primary care Provider #2 across town, but also in the network. Let's also say that these 2 providers were already set up to share service information (Level II described above). (If they hadn't been, provider #2 may have requested from provider #1 the right to view but not edit this data—you can never edit another provider's service and other data!)

Now, when the data administrator at provider #2 with read/write access to John Doe's record finds his record following a database search, a couple of things occur. First, Mr. Doe's demographic data are completed, but could be changed if this were deemed necessary. For example, maybe his address had changed, or his race was entered incorrectly. Remember, these edits are possible at provider #2 because a) demographic data (except for the Client ID field) are common fields and 2) *the user accessing the system has been granted the appropriate rights to edit these fields.* There are also likely other users of the system who were not granted the right to either view or edit demographic data. Note that through an audit trail, the central administrator can track how often specific fields are modified; this is an important way of overseeing the integrity of the database *and ensuring that records are not being unnecessarily changed or modified.*

Now say that provider #2 goes to the service tab. Because service records are not common, but owned by the provider, provider #2 may add services and view the services Mr. Doe received at the Provider #1, but cannot edit any of the services *entered* by another provider. Similarly, because these two agencies provide primary outpatient care, provider 2 could view—but not edit—the medications and other clinical information collected at provider 1 on that client. Again, it is quite likely that only select users at each site are granted the right to view (let alone edit) clinical information in the first place.

Case Notes

Because of the additional sensitive nature of case notes, the network version of CAREWare allows the following sharing arrangements:

- **Rule-based sharing**: users at other providers will be able to view case notes if they are granted sufficient permissions
- **No sharing**: no other providers can view the case notes entered by a specific provider

Provider Data Import (PDI)

For agencies electing not to join the real-time network, CAREWare can import their data using the PDI. The PDI simply means that the agency will export all or part of their database to the central domain on a regular basis. This feature will ensure that the main database stored on the grantee's server will contain the client level data from all providers, whether or not they are joined to the network in real-time. However, the provider electing to export their data will *not*, of course, have access to other providers' data in real time, as they are not connected to the central CAREWare database stored on the network. Grantee administrators will be able to establish read only access accounts for PDI providers.

Getting Started: Data Conversion and Centralization

Providers joining a real-time network will have to export their data to the central database administrator using the PDI or Store and Forward (see PDI and S&F documentation for more details). For real-time providers, this is a one-time process; once your data have been successfully exported and then imported by the grantee, you are set to enter

data on the network. From this point on, your CAREWare data will no longer be stored locally on your own computer but on the central database server. Providers electing not to join the real-time network will of course have to export their data on a regular basis, as worked out with the grantee.

When doing a one-time data upload to join a real-time network after having used CAREWare as a standalone application, S&F is often the better choice because it requires less time for preparing the server. However, providers who export data regularly usually find the PDI easier to work with.

PDI Export Rules: The Important Case of the Provider Receiving Funds from Multiple Grantees

CAREWare is designed to allow you to export, using the Provider Data Export (PDE), only specific clients or only specific types of data. This is especially important for providers that are funded by multiple CARE Act parts. The PDE has export rules that allow you to export only clients who receive services with certain types of funding. Please see the PDE documentation for all of the available options.

IMPORTING PDI Files: What happens when a client is in multiple provider databases?

In the central database, the PDI gets tricky when a client with the same URN appears in multiple provider databases because he or she receives services from more than one agency in the network. Obviously, the problem only pertains to common demographic or annual review data (all other data are provider specific, as discussed above), and if common data is disabled, then it is not an issue for demographic or annual data either.

Let's say that John Doe, with an address of 100 HRSA Lane, is in Provider #1's database and that his record was imported by the grantee, and then the grantee receives a PDI export from Provider #2. John Doe is also in the Provider #2 database, but the address here is 123 DHH Ave. If the central administrator imported Provider #2 without any questions, and demographic sharing is turned on, the 100 HRSA Lane address would get written over with the 123 DHH Ave address imported last. This would be the case with any common fields that had different values in the last database imported.

If the Central Administrator ***does not*** want the PDI to simply use the last value demographic value, he or she can set a filter that simply bypasses the latest value and keeps the non-missing value found in the first import. (Of course, if Provider #1 had no address at all, and the Provider #2 database contained a non-missing value, the latter would get written to the database.)

Table 1. Summary of version 4.0 Roles, User types, Rights and Permissions

Role in RW CAREWare 5.0	User Types	Possible Rights and Permissions
Real-Time Central Administrator	Grantees, Data Directors, Computer Administrators	▪ Read/Write access to all domain contact information in system ▪ Create/Edit central and provider domain user accounts
PDI Central Administrator	Grantees, Data Directors, Computer Administrators	▪ Read/Write access to current Grantee contact information
Regional User	Data Directors	▪ Read access to provider data, possibly without access to PII.
Real-Time Provider Administrator	Provider, Data Directors, Computer Administrators	▪ Read/Write access to provider domain contact information ▪ Create/Edit provider domain user accounts
PDI Provider Administrator	Provider, Data Directors, Computer Administrators	▪ Read/Write access to current provider contact information ▪ Create/Edit provider domain user accounts
Central User	Data Entry, Data Monitor, Care Givers	▪ Read/Write access to certain client data modules of assigned domain(s) client data
Provider User	Data Entry, Data Monitor, Care Givers	▪ Read/Write access to certain client data modules of current domain client data
Installation/Maintenance personnel	System Administrators, Network Administrators, Applications Administrators.	▪ No CAREWare access.

Major Features in CAREWare

- Scales to the very small (a rural nurse with a laptop) to quite large, 80+ providers on one server.
- Extensive reporting engine and export capabilities if you use 3rd party tools like SAS.
- A flexible performance measure engine with optional email alerts and the ability to drill down to the individual clients that make up the numbers.
- Extensive data export and import capabilities.
- Automated HL7 imports for lab data and ADT feeds.
- An internal network messaging system that enables providers to send referrals and other messages such as system updates to contributing network members. A bulletin board also allows the grantee administrator to send messages across the network.
- Controlling Contract expenditures for each service: Grantees have the ability (from the central domain) to create contracts that limit spending by service type. The following options will be available:

  Subservice cut-off: Grantees can decide that providers who reach the annual expenditure limit for a subservice will no longer be able to enter data for that subservice.

  Nag screen: Some grantees may not want to prevent data entry. They will, though, be able to implement a warning message that appears every time the provider enters a record for a service whose annual limit has been reached.

HIPAA Compliance

The network version of CAREWare has a number of features that will ensure compliance with HIPAA in a variety of ways. But it is important to remember that the data privacy and security requirements of HIPAA require the trust of the individuals running and managing and using the system at the provider and grantee level; it's not ONLY the responsibility of the computer hardware and software!

Nevertheless, there are many features of version 5.0 that are critical to maintain the security of the data, and ensure that only authorized individuals see only the information they need to see to provide services.

- Passwords which limit access to view or edit data
- No access after three failed logon attempts
- Grantee can set a number of days after which passwords must be changed
- Role-based and need-to-know access: Very flexible data sharing system to restrict user access to and ability to view only specific parts of the database
- Full data encryption over the network through the .NET system

- Client identifying information-name, date of birth, address- is encrypted in a string when it is stored in the database

- Audit trails that enable the grantee administrator to oversee who was logged in and made specific changes to the database

Section 2
System Administrators

Background

This section is designed to provide System Administrators the information they will need to design and manage a computer system on which to run RW CAREWare 5.0. It will:

- Give system requirements, both hardware and software.
- Provide and overview of the three-tier architecture used in RW CAREWare.
- Discuss security of client information, including encryption techniques used in storing and transmitting data.
- Give example configurations for a variety of systems — from a simple standalone workstation to large-scale WAN installations.
- Give estimates of storage requirements. This will be important in deciding whether to use the included MSDE data engine or to upgrade to MS SQL Server, as well as deciding what types of connections will be needed between computers.
- Provide considerations for firewall configurations.
- Discuss deployment of CAREWare, and the automatic update system.
- Detail what needs to be backed up in order to be able to recover CAREWare from a catastrophic failure.

There are a couple topics that are outside the scope of this document, and so are NOT covered:

- Specific back up *systems* are not discussed. While this document details what to back up, it does not discuss how to back it up.
- System redundancy – this is highly contingent on how mission critical an installation of CAREWare is, and will not be a consideration in most cases. Network Administrators will need to assess the necessity of redundancy, and how to set that up should they deem it necessary.

System requirements

Since new technology tends to expand at a very rapid rate and CAREWare continues to evolve in this environment, we feel that publishing specific minimum processors is of little value, if not misleading. Another reason for not publishing minimum processor and memory requirements is that most manufactures tolerate a much slower response than you may find users will tolerate. Rather than do that, we will try to lay out general factors that should be considered.

The scale of your CAREWare installation is the primary factor determining the system requirements. For instance, if you are going to be running a central server with 80 real-time providers you will want a beefy 64-bit server and another for the SQL Server. On the other hand, if you are a single standalone or small network operation with 100 clients, you can probably install CAREWare on existing (at the time of this writing) 32-bit equipment you currently use for word processing and so forth.

If you are required to check minimum requirements anyway, we suggest you check the current minimum requirements for the technologies CAREWare uses.

- The Client Tier runs in the Microsoft .NET 2.0 framework.
- The Business Tier runs in the Microsoft .NET 2.0 framework.
- We currently recommend Microsoft SQL Server 2008, but CAREWare will run on SQL Server 2005.

A quick search of the Microsoft site will show their purported minimum specifications. We recommend you treat these as an absolute minimum in a worst-case for existing equipment at small sites, not as specs for buying new equipment or running medium to large installations.

Data Tier

The data tier is the database where the actual information is stored. This is a storage facility that holds all the data and fills requests for retrieving and modifying program data. It is composed of tables of data managed by a Microsoft SQL Express (formerly know as MSDE) database engine, which is based on core SQL Server technology. SQL Express is freely distributed with CAREWare though a developer license. Providers and grantees will not have to incur expense when setting up their data tiers if they use SQL Express.

SQL Express does have limitations: a SQL Express database is restricted to 4GB in size, and according to online sources, it is restricted to 1 processor and RAM limitations. This should be fine if you are a reasonably sized single clinic, but if you are a large volume clinic or setting up a multi-provider server, you will likely want to purchase the full version or Microsoft SQL Server 2008 (or the highest supported version).

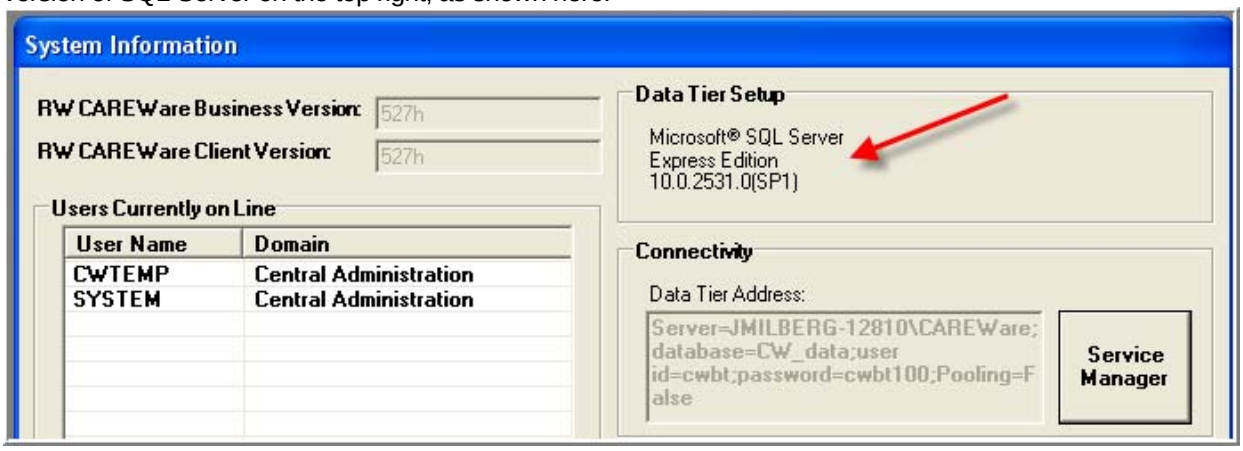
What CAREWare configuration do I need for good performance?

Use the table below to determine which scenario best describes your current configuration, and the actions to take.

If your CAREWare configuration is this…	And You're your Version of SQL Server is…	And your computer is...	Consider this software upgrade …	And these possible improvements…
Small use with one to 20 concurrent users	SQL Express 2000 (MSDE) or SQL Express 2005	32-bit	SQL Express 2008 using conversion utility.	See small use checklist.
Medium use on a LAN or WAN with 20 to 50 users and 1-10 or real-time providers	SQL Express 2000 (MSDE) or SQL Express 2005	32-bit	SQL Express 2008 using conversion utility.	See medium use checklist.
30+ concurrent user and 10+ real-time providers on a wide area network or Internet	SQL Server 2000 or SQL Server 2005	32-bit or 64-bit	Full SQL Express 2008 64bit Standard or Enterprise Edition.	See heavy use checklist.

How do I know what version of SQL Server I have?

Press Control + I to obtain system information while logged in centrally. The screen will show your version of SQL Server on the top right, as shown here:



- Any number that begins with 8 is SQL Server 2000.
- Any Number that begins with 9 is SQL Server 2005.
- Any number that begins with 10 (as the example above does) is SQL Server 2008.

- If you have SQL Server 2000 and it says “Desktop Edition,” then you have the “MSDE” free version that was distributed with CAREWare and you should upgrade to the free version of SQL Server 2008 which is now called “Express Edition.”

- If you have SQL Server 2005 and it says “Express Edition,” then you have the free version that was distributed with CAREWare and you should upgrade to the free version of SQL Server 2008 which is also called “Express Edition”.

- If you have SQL Server 2008 and it says “Express Edition,” then you have the free version that was distributed with CAREWare and that should be OK unless you are experiencing slowness because of heavy traffic or if your CW_Data.mdf file has exceeded or is pushing the maximum size of 4GB, in which case you should get the full version of SQL Server 2008.

Small Use Checklist (1 to 20 concurrent users and 1 Real-time provider)

- 1 preferably 2GB of memory and a reasonably new machine with 32bit OS should be fine

- Upgrade to SQL Server 2008 Express Edition

- Check your .Net Framework Service Packs and SQL Server Service Packs

- Make sure virus protection is in place

Medium Use Checklist (20 to 50 concurrent users 1 to 10 real-time providers)

- If you have a 32bit operating system make sure you have at least 4GB of memory. Try to work getting a 64bit server into your future plans if you are still too slow after doing the things on this checklist.

- If you have a 64bit operating system you will benefit from adding more RAM if your SQL Server is 64bit. Remember you can install a 32bit version of SQL Server on a 64bit operating system but it is not recommended because the SQL Server can’t access more than 2GB of ram if it is 32bit.

- Upgrade to SQL Server 2008 (64bit if possible) Standard or Enterprise edition or SQL Server 2008 Express (64bit if possible). Note that is possible to use the Express edition if your CW_Data.mdf is below 4GB in size and is not growing at too fast of a rate.

- Check your .Net Framework Service Packs and SQL Server Service Packs

- Make sure virus protection is in place

- If users are connected to the internet test their connection speed at a site like dslreports.com and make sure they have a reasonably fast connection like 1000kbs or more up and down and make sure the server they connect to have a reasonably fast connection like 3000kbs or more up and down.

Heavy Use Checklist (30+ concurrent users and 10+ real-time providers)

- If you have a 32bit operating system make plans to get a 64 bit operating system.

- If you have a 32bit SQL Server or a SQL Server 2000, make plans to get SQL Server 2008 64bit Standard Edition or Enterprise Edition.

- Check your .Net Framework Service Packs and SQL Server Service Packs

- Make sure virus protection is in place
- If users are connected through the internet test their connection speed at a site like dslreports.com and make sure they have a reasonably fast connection like at least 1000kbs up and down and make sure the server is connected to an appropriately fast connection.
- Consider the appropriateness of VPN connections or Citrix type session management.

How do I know if my computer is 32 or 64-bit?

Check the properties under My Computer. Please note that CAREWare plans to release a 64-bit version of the CAREWare business tier to be available along side the current 32-bit version.

3-Tier Architecture

CAREWare utilizes a 3-tier architecture composed of 3 parts: the Data Tier, the Business Tier, and the Client Tier. In some cases, grantees will host the back-end database and business tier components while providers run front-end client components that will allow them to enter data and run reports. In other cases, all three components of the software will run on a single PC.

Data Tier

The data tier is the database where the actual information is stored. This is a storage facility that holds all the data and fills requests for storing, retrieving, and modifying program data. It is composed of tables of data managed by a Microsoft SQL Express database engine, which is based on core SQL Server technology. SQL Express is freely distributed with CAREWare though a developers license.

Providers and grantees will not have to incur expense when setting up their data tiers if they use the SQL Express.

SQL Express does have limitations: an SQL Express database cannot be larger than four gigabytes, and according to online sources, and is limited to 1 processor and memory size. See the Microsoft site for more information.

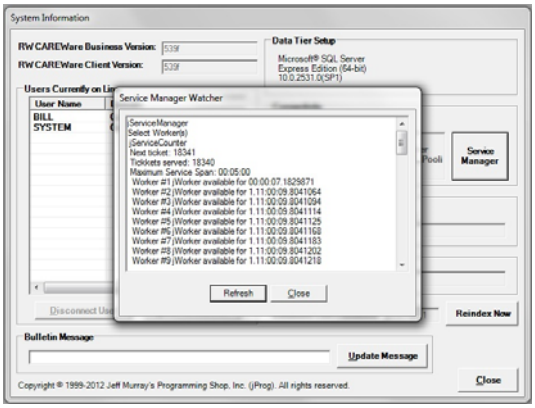
These limitations will affect only medium to large RW CAREWare installations, however. Most RW CAREWare are between one to two GB

Those planning on hosting a data tier with data from multiple providers are more likely to need more capacity than the four GB allowed by SQL Express.

Organizations with sufficient resources will be able to upgrade SQL Express to MS SQL Server, which is not limited in the way that SQL Express is.

If you do upgrade to the full version of SQL Server, the Standard Version less expensive all CAREWare will need, although your IT department may have other reasons to want the Enterprise Edition.

If you get the full version, another important consideration will be user licenses. It is important to remember that you do not need to buy a new SQL Server User License" for every CAREWare user. With CAREWare's 3-tier architecture the Business Tier is what manages SQL Server connections, and CAREWare is very efficient in pooling its connections so that even if you have 30 or 40 users, they will only be using a few SQL Server connections. The standard 5 pack should be should be fine for all but the largest CAREWare installations. If you want to check if you are exceeding you Licenses, you can check how many the business tier has used since the last time the server started by logging in to CAREWare as a central administrator and pressing Cntrl+I to see the System Information screen and then clicking Service Manager.



In the business tier, CAREWare has an internal entity called a 'Worker" that the SQL Commands are sent through. If you scan the list you will see that there are Select Workers, Update Workers and Report Workers. Each one says available for [days].[hours].[minutes].[seconds].[fraction of second] Looking at this example, only the first select worker was used, the others have not been used since 1 day and 11 hours ago when the computer was turned on. The slight difference in the fraction of a second is not important. If you scan down you can easily see if and when the last worker was used, count them up, and that is how many SQL Server connections CAREWare is using.

Business Tier

The business Tier acts as the communication manager for CAREWare. It is run as a Windows service, and is built on the .NET 2.x framework.

This tier provides secure communication to and from the Client Tier, and reliable transportation of data to and from the database. This tier also manages data encryption, as well as the checking of the credentials of the user attempting to use CAREWare and enforces the business rules.

Business tier <-> Client Tier Communication

The Business Tier utilizes .NET Remoting as its means of communication with the Client Tier. When shipped, RW CAREWare uses HTTP for Remoting because this protocol is more robust, particularly in regards to firewalls, which will commonly be encountered between the Business and Client Tiers.

When the Business Tier is started as a service, it sets up a listener that awaits requests from a client. Whenever it receives a request, if the request has the proper credentials (see Permission Management), then the Business Tier fills the request and sends an appropriate response to the client. Note that all data sent to and from the client is encrypted (see Client tier < - > business tier communication channel on page 18).

The file RWCAREWareRemoting.config, which is located in the installation directory of the Business Tier holds the connection information to the Client, including the port number that the business tier will listen on.

Business tier <-> Data Tier Communication

The business tier ships using five standard SQL Server connections to communicate to the data tier of the program. These connections are created under the authority of the CWBT (Care Ware Business Tier) SQL Server user. These two tiers are intended to reside behind the same firewall, whether on a single machine or separate.

The settings for the SQL connection information are in the file **BusinessTierSettings.xml** under the **DataTierAddress** setting. This file will be installed (and must remain) in the installation directory for the Business Tier.

RW CAREWare's query throttling technology insures that the business tier administrator can specify the maximum concurrent queries that will be submitted to the MSDE/SQL Server during peak periods. It also allocates the queries by purpose. In the default configuration, one query is allocated for updates, two are allocated for select queries related to data entry screens and program operation, and two are allocated for reports. Under this default setup, if there are three users are trying to run reports at the same time, the third report request will experience a pause until one of the preceding report queries finishes, but the data entry related activities will continue like normal, and the MSDE will not purposefully slow down. If you are using the MSDE as your data tier, it is recommended that you do not change these default settings, but if you are using the full version of SQL Server, you will most likely want to allow the business tier to use more connections and submit more simultaneous queries during peak periods. You can do this by adjusting the NumReportConnections, NumSelectConnections, and NumUpdateConnections values in BusinessTierSettings.xml.

NOTE: The default ports that are used can be changed by modifying these files, but you must be sure to change the port on the client config file as well (or the setup of the MSDE database connection on the database if it is changed); Otherwise the program will not work, since there will be no communication through the business tier.

NOTE: The business tier and data tier have a one to one relationship. For a number of reasons, the business tier keeps data cached in memory, and assumes that it is the only entity changing data in the CW tables on the data tier. For this reason you should never configure two CW business tiers to point to the same data tier. If you are contemplating inserting data into the data tier directly from a third party application, you should first contact CW technical support to discuss required techniques to insure the integrity of the business and data tiers.

Permissions Management

RW CAREWare employs an extensive custom permissions module to exercise control over access to features. Users need to have different permissions to view, or edit, or add, or delete data, and different permissions based on which data they would access (See the System Administrator's section of this Guide for detailed information on these permissions).

The Business Tier acts as the manager for this permission system. Any time a user makes a request to access the database, the Business tier verifies that the user is a valid user, that they are logged into the system, and that they have the necessary permissions for the requested data access. If all these criteria are met, then the Business Tier fulfills the request. Otherwise, an appropriate error message is sent to the client describing why the request was denied.

The business tier also manages data encryption for the program, including encrypting data streams to and from the client, and the encryption of identifying information on the data tier. This encryption is covered more in Encryption Technology on page 167.

Client Tier

The Client Tier is the user interface for CAREWare. It is composed of all the forms and the code that is used for requesting, submitting, and presenting data in the program. The interface uses Windows Forms technology, written in Visual Basic .NET. This allows us to deploy and use secure and user-friendly client systems that users will be able to setup and use with ease.

For information about installing and updating these 3 components, see Deploying and Maintenance.

Security

The information captured by RW CAREWare is very private in nature, and so security is a very high priority. The program uses multiple layers of security to help protect client data; this section will talk about those.

Secure User Manager

RW CAREWare employs a custom designed user manager with a very sophisticated permissions system (which is managed by the Business Tier). Through this system, administrators can give very specific privileges to users, deciding what data users are allowed access to and what type of access they have to that data (Viewing, Adding, Editing, Deleting, etc.). This user manager is entirely separate from any Operating System user management system, and so does not depend on the version of Windows installed, whether Active Directory is used, etc. More information on managing users can be found in the RW CAREWare User Manual.

In addition to the permission system, RW CAREWare also uses an extensive logging system. There are 3 types of logging in RW CAREWare:

Event Log – These entries can be viewed in XML files named cw_log*.XML that reside in the installation directory. The log file contains rendering information and points to a companion file named cw_events*.txt that holds the raw, unformatted xml containing the events.

The business tier creates a new log file for each day's events and limits the number of log files in the directory to five pair by deleting older files. The business tier logs any exceptions that are encountered by the program. These entries will generally be used by IT staff and RW CAREWare support personnel to help correct problems with the operation of the program. In addition to errors, if CW makes any changes to the data tier while upgrading to a new version, each step will be logged in the log file.

Security Violations – This log can be viewed in the administrative section of RW CAREWare. They are also presented to RW CAREWare administrators in the system messages section of the main menu. It shows a history of any security violations in the program, which includes unsuccessful login attempts, any client trying to access data without the proper credentials, etc. These types of violations are also written to the event log.

Change Log – This is also viewed under the

administrative section of RW CAREWare and shows a history of all changes made to client data and services. It records information such as the user making the change, the time of the change, old value, new value, etc. Entries are made for *each field* on any record that is added, updated, or deleted.

Encryption Technology

.NET's cryptology library provides native encryption capabilities that can be used to secure communication streams used in n-tier applications. RW CAREWare 4.0 (CW) will use these capabilities to enable Providers or Grantees (PG) to store, retrieve and transport the highly confidential Personal Identifying Information (PII) they may possess. All remoting streams that will be used in RW CAREWare 4.0 will be encrypted using the RSA and DES encryption algorithms available in the .Net cryptology library. The following encryption plan addresses three key areas where CW may store or transport PII.

Database storage of PII

In some larger implementations of CW, it is likely that the PG will house the CW data in large SQL Servers that are administrated and backed-up by network personnel who are not directly controlled by the PG. PGs may also choose to store backups of their data offsite in case of fire. To ensure confidentiality in these types of scenarios, the business tier will encrypt name, birth date, URN, and soundex information prior to storing it in the database. This encrypted information will be concatenated and stored in a single binary field in the client's record. The data can only be decrypted with the private key that will be kept on the business tier. This enables a PG to install the CW business tier on a computer that is secured by personnel they monitor closely.

The encryption will is accomplished using the .NET TripleDESCrypto-ServiceProvider functionality. TripleDESCryptoServiceProviders GenerateIV() and GenerateKey() methods will be used to randomly create strong private keys during the CW installation process. These keys will be stored on the business tier computer in an encrypted file (see Key Protection on page 14). With the use of these keys, the business tier will encrypt PII prior to saving to a database and decrypt it after retrieval. The encrypted data (encompassing several fields, as is explained above) will be packaged together and stored in one MS SQL Server VARBINARY field.

Turning Database PII Encryption off

If you feel your internal procedures are sufficient to protect your backups and so forth. You may prefer to turn the PII database encryption off. This can be accomplished through Administrative Options / Advanced Encryption Options. There is a fairly substantial performance gain for turning PII database encryption off because CAREWare can skip having to decrypt the information and does not need to hold it in memory or pass it back to the SQL server using its in memory XML table features.

Encryption and Store and Forward

A solid understanding of CW Store and Forward (S&F) is required to understand its encryption scheme. More importantly, the PDI is much simpler to use so we recommend you using that instead of S&F is at all possible.

CW allows disconnected providers to enter data and then periodically create export files that are then transported to the grantee for importing. CW implements an RSA public/private key scheme help ensure confidentiality of data during transport. Each installation of CW will have its own randomly generated public/private key pair that will be stored in an encrypted file on the data tier (see Key Protection on page 19 for details). When a provider first wishes to transport data to a grantee, the provider will need to import a grantee-created setup file that contains the grantee's RSA public key. From then on, data sent to that grantee will be encrypted using that public key. Once the data has been transported to the grantee, the grantee's business tier will use its RSA private key to decrypt the data.

The .NET **RSACryptoServiceProvider** functionality will be used to generate the public and private keys during the CW installation process and to encrypt export data and decrypt for import.

S&F Import Adapter

Before data can be imported, a CW administrator will setup an S&F import adapter. From that adapter they can create a small configuration file that among other things will have the public key for

their CW installation.

S&F Export Adapter

When the provider wishes to export to a grantee (or any other CW installation) they can create an S&F Export Adapter from the configuration file sent to them by the grantee. At that time they will read the grantee's public key and store it in their database with other export adapter information. Any export files sent to the grantee will be encrypted with the grantees public key.

Client tier <-> Business tier communication channel

CAREWare uses .NET remoting for all communication between the client and business tier. When a new channel is first established, the client generates a random RSA public/private key pair and sends the public key to the business tier. The business tier then responds by generating a new random private key that is encrypted with the public key and sent to the client. From then on, both the client and the business tier use the same private key to encrypt and decrypt the data that is communicated across the channel. These random keys are unique to each channel and are discarded once the communication channel is terminated. This method is commonly referred to as Secure Socket Layer (SSL).

The strength of the key that is exchanged and the method used to encrypt data on the channel depend on the setting you choose in the **RWCAREWareRemoting.config** file. There is a copy of this file on the business tier and the client tier in the same location as their EXE files. These are small XML files that CW remoting uses to configure itself. When you first install CW you will find the entry algorithm = "DES" in these files that causes remoting to use standard DES. Your other choices are "3DES" for Triple DES, "RIJINDAEL" for Rijindael, and "RC2" for RC2. If the client does not use the same encryption method as the business tier, it will not be able to connect.

Mark Strawmyer has published a good introductory article on the DotNet implementation of these algorithms:
http://www.developer.com/net/net/article.php/1548761

Below is an excerpt from the article:

- *Data Encryption Standard (DES) algorithm encrypts and decrypts data in 64-bit blocks, using a 64-bit key. Even though the key is 64-bit, the effective key strength is only 56-bits. There are hardware devices advanced enough that they can search all possible DES keys in a reasonable amount of time. This makes the DES algorithm breakable, and the algorithm is considered somewhat obsolete.*
- *RC2 is a variable key-size block cipher. The key size can vary from 8-bit up to 64-bits for the key. It was specifically designed as a more secure replacement to DES. The processing speed is two to three times faster than DES. However, the RC2CryptoServiceProvider available in the .NET Framework is limited to 8 characters, or a 64-bit key. The 8-character limitation makes it susceptible to the same brute force attack as DES.*
- *TripleDES algorithm uses three successive iterations of the DES algorithm. The algorithm uses either two or three keys. Just as the DES algorithm, the key size is 64-bit per key with an effective key strength of 56-bit per key. The TripleDES algorithm was designed to fix the shortcomings of the DES algorithm, but the three iterations result in a processing speed three times slower than DES alone.*
- *Rijndael algorithm, one of the Advanced Encryption Standard (AES) algorithms, was designed as a replacement for the DES algorithms. The key strength is stronger than DES, and was designed to out perform DES. The key can vary in length from 128, 192, to 256 bits in length. This is the algorithm I personally trust the most and that I'll use for the examples contained in the column.*

Note that this SSL connection only encrypts the channel -- it does NOT restrict communication to certain computers or locations. If this is something you need to do then you will have to implement you own solution. Many VPN products can restrict access (to the CW business tier server) to specific selected sites or computer(s).

Business tier <-> Data tier communication channel

CW does NOT encrypt channels between the business tier and the data tier because in most installations they both will be located *behind the same firewall* and possibly on the same server or same rack. If you are installing CW in an environment where you have determined these channels should be encrypted, it will be up to you to

implement the solution.

If your business and data tier are both running on Windows 2000 Server or above, and you must have encryption of this channel, you may want to consider using IPSec to secure it. Information on how to configure Windows 2000 Servers to communicate using IPSec can be found at:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/SecNetHT18.asp

If you have the data tier using MS SQL Server 2000 or above, you may want to consider using its SSL capabilities to encrypt the communication channels.

Key protection

All private keys will be stored in a password-protected configuration file in the directory where the business tier resides. This configuration file will be encrypted using .NET **TripleDESCrypto-ServiceProvider** functionality. A key that will be used to decrypt the private keys will be generated from a GP-provided password.

Automatic vs. Manual GP password retrieval

Given that the private keys are required for the business tier to operate and that they are protected by a GP-supplied password, the business tier will require that the password be retrieved before it services client requests. 'cw_temp'. GPs will need to decide whether or not to change the default keys, and whether or not to keep those keys in the business tier directory.

Manual GP Password Retrieval

You can perform manual password retrieval by removing the DataTierEncryptionKeyPassword.xml and DataTierEncryptionKey.xml files from the install directory once the business tier is initialized, and restoring them to the directory prior to starting or re-starting the business tier. After being started, or re-started, the business tier will automatically read the files within 3 minutes, or at the first client login attempt, whichever comes first, they will not be needed again unless the business tier is restarted, or Advanced Encryption features in the CW client are used to change them.

The benefit of this system is that it avoids having to store passwords on the disk of the business-tier and hence provides some additional protection if the operating system security of the business tier computer is breached.

The drawback of this system is that it requires human intervention when the system is started or rebooted, and it may cause more people to need to know the password. It also carries the possibility that the password may be forgotten and/or lost.

Automatic GP Password Retrieval

With automatic key retrieval the GP-supplied password and other keys are kept in the business tier directory. Although the keys in the XML files are encrypted using another key stored in programming code, storing a key in software is a weak form of key protection. Therefore, under this method, the GP would need to take steps ensure that their operating system security prevents unwanted access to the configuration file. The GP would also need to ensure that they changed the CW-supplied default password to a password that contains a sufficient number of mixed letters and numbers that cannot be guessed. These are things you should be ensuring anyway.

The benefit of this system is that it allows the business tier to be started and rebooted without human intervention, which can be efficient after system failure. It also may be desirable in single user installations where the user doesn't have the technical skill necessary to use manual key retrieval. It most likely would require fewer people to know the GP password as well.

The drawback of this system is that if a hacker gains unwanted operating-system-level access to the business tier computer, he or she might find the password and key files and then hack the programming code and decrypt the password, which he or she could use to get the key. But arguably if the PG's security is lax enough to allow this, the revealing of this password may be the least of their worries.

Sample RW CAREWare Network Configurations

The following illustrations depict a sample of possible configurations that RW CAREWare will support.

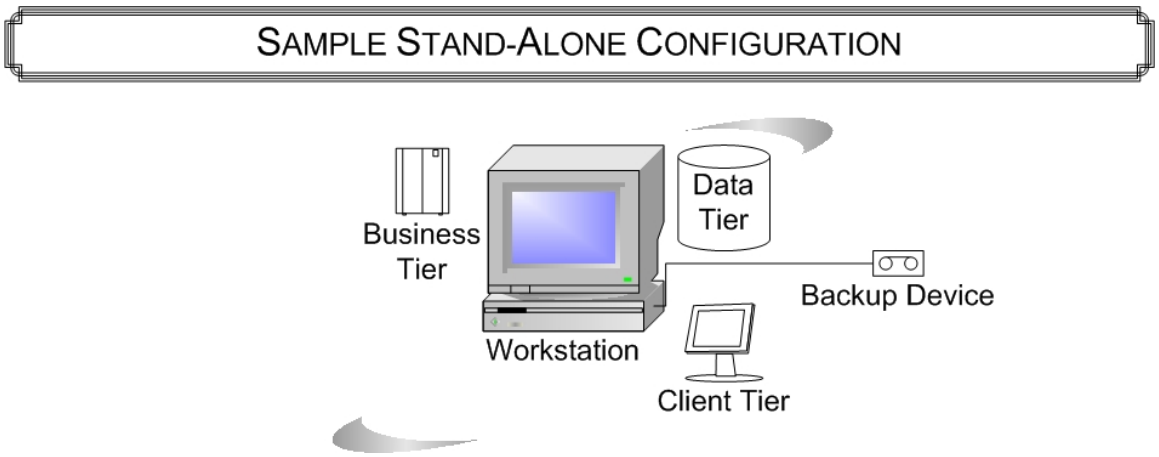


Figure 2.1 Sample Stand-Alone Configuration
In this illustration, all three tiers are installed onto one workstation.

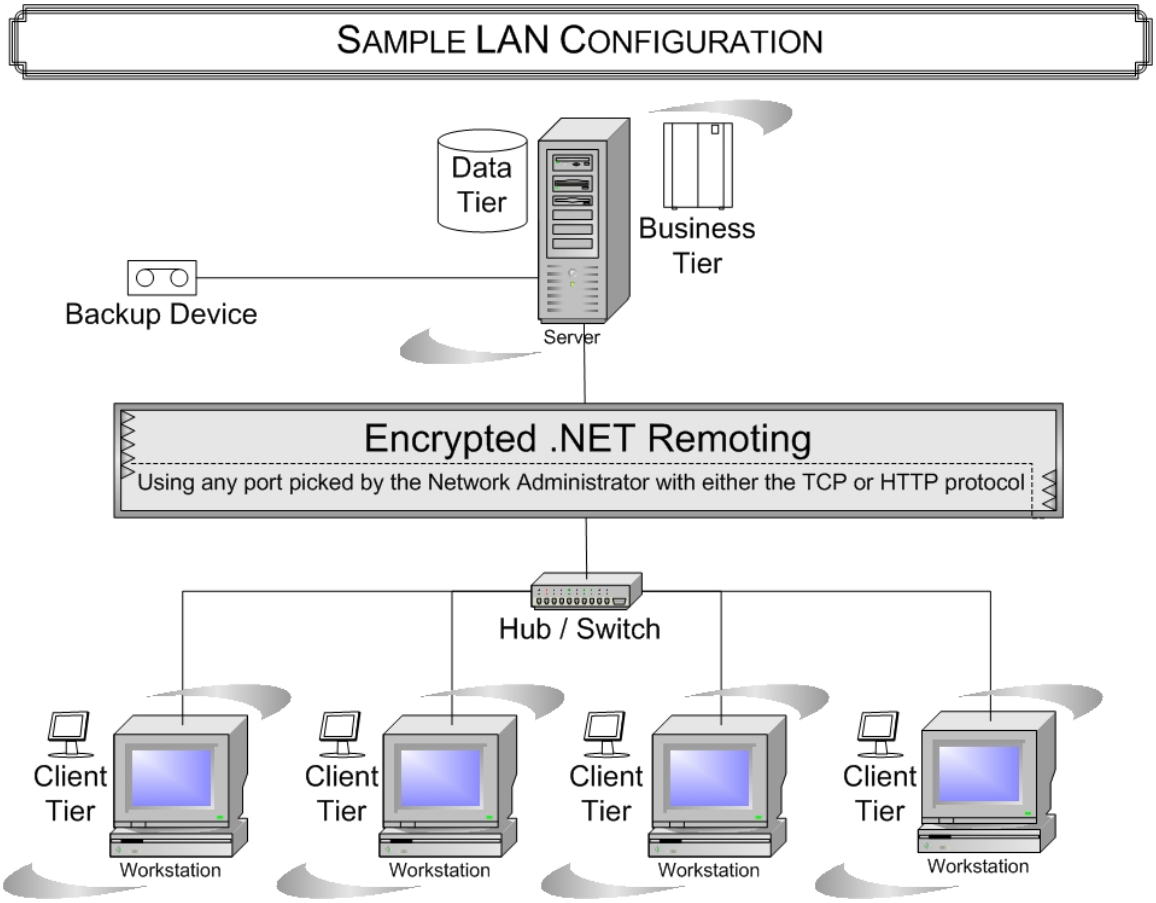


Figure 2.2 Sample LAN Configuration

In this sample configuration, four workstations, using client tier software, are connecting to a server computer using encrypted .NET Remoting. This server has both the data and business tier installed.

Note that the Data Tier and the Business Tier could be installed on separate servers if it better fits the specific network architecture.

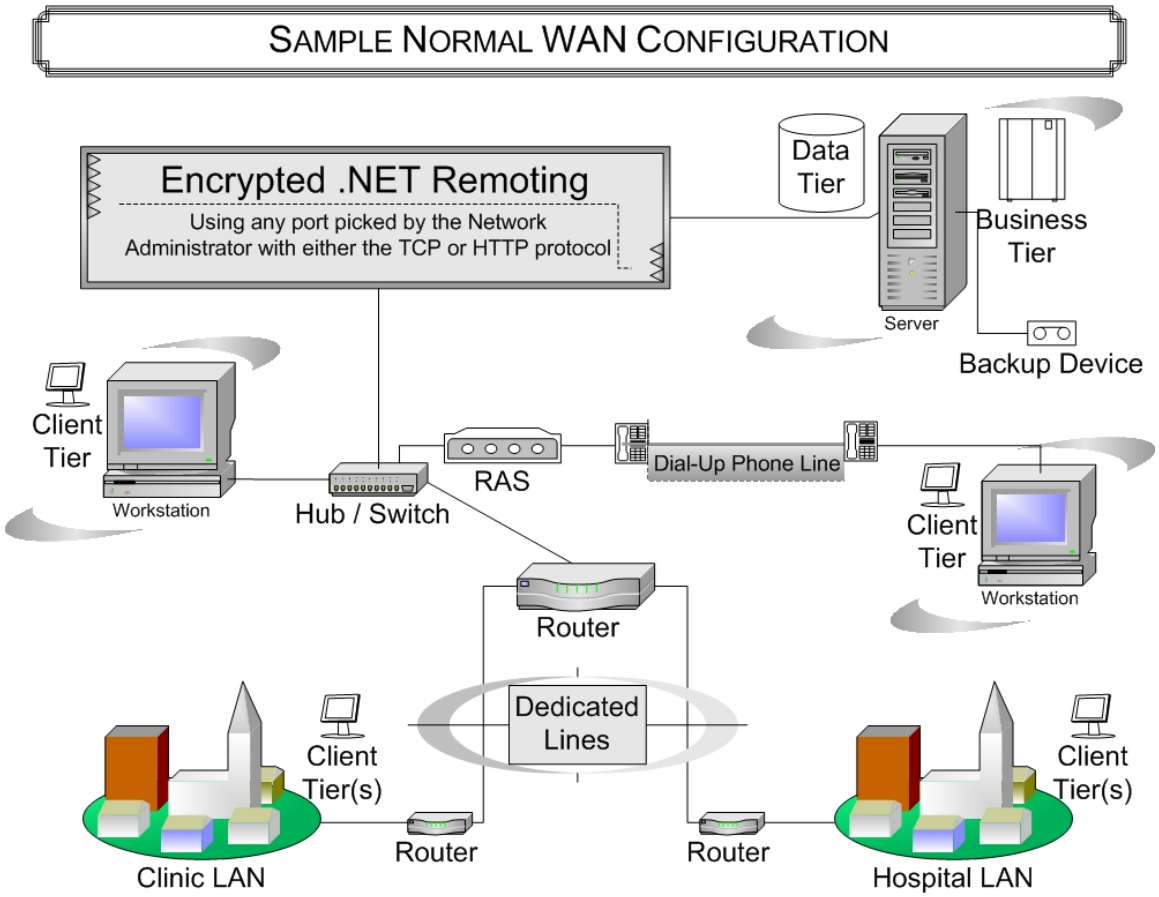


Figure 2.3 Sample Normal WAN Configuration

In this sample configuration, two LANs from a clinic and a hospital are using .NET Remoting to connect to the server. Each LAN site has dedicated lines that are directly connected to the server site. At the server site, there is one workstation running the client tier software connecting locally to the network and another connecting to the network using dial-up. The server at this site has both the data and business tier installed.

Note that the Data Tier and the Business Tier could be installed on separate servers if it better fits the specific network architecture.

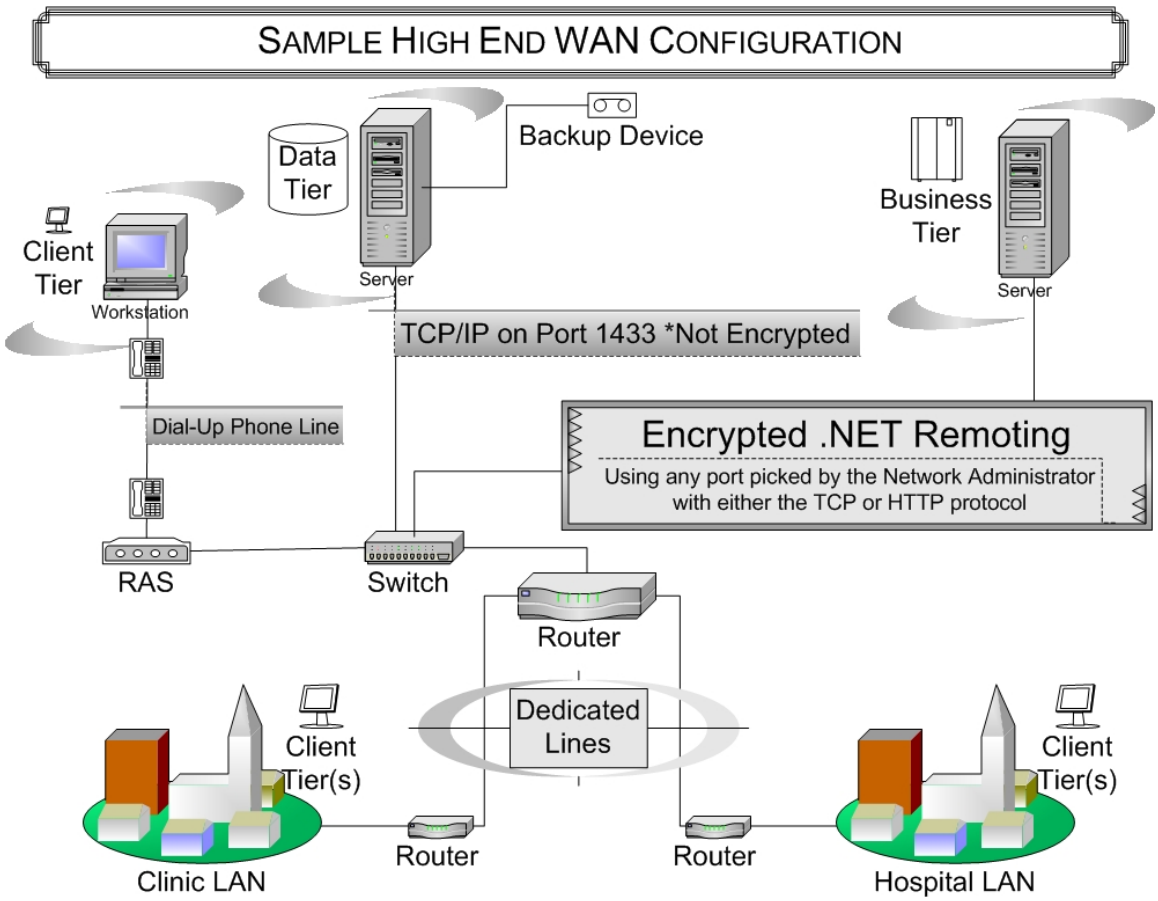


Figure 2.4 Sample High End WAN Configuration

This configuration is identical to figure 2.3 except that the data and business tier are separated into two server computers on the server site.

- We are designing the business and data tier to reside behind the same firewall. Therefore, the RW CAREWare 4.0 system will not encrypt the communication channel between these two tiers.

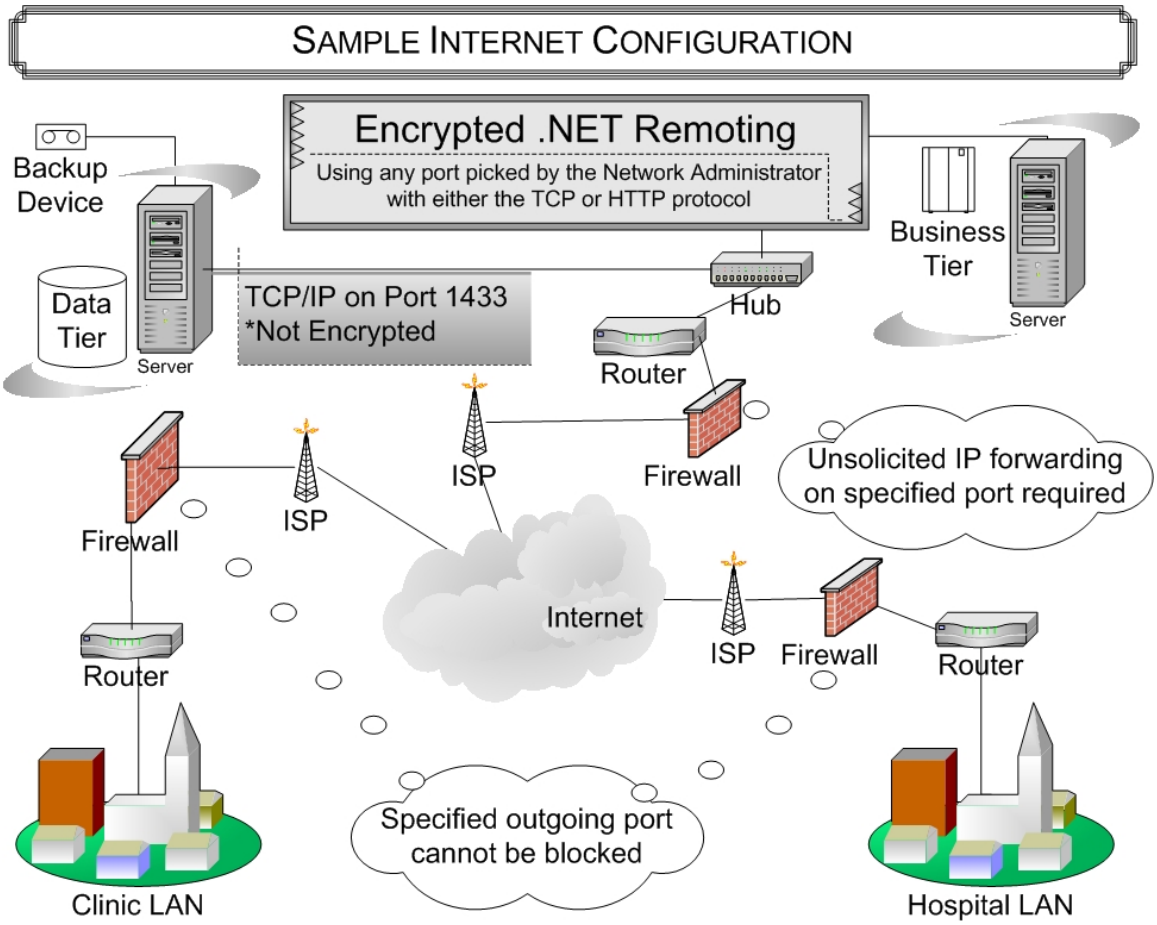


Figure 2.5 Sample Internet Configuration

This configuration details the transfer of data through the Internet. LAN sites from a clinic and hospital are connecting to the server by making unsolicited requests for connections and transferring encrypted data using .NET Remoting through the Internet. Firewalls are placed at each site to symbolize possible security measures taken by each site.

- The business and data tier are designed to reside behind the same firewall. Therefore, the CAREWare system will not encrypt the communication channel between these two tiers.
- In normal operating conditions, it is ok to put the data tier and the business tier on the same server

Firewalls and Port Forwarding

As can be seen from the sample Network Configurations, firewalls are an expected component of the systems that RW CAREWare will run on. The business tier acts as a communications hub of sorts, since all client requests go through the Business tier to and only the business tier accesses the data tier, and all responses go back through the business tier to get to the client (See 3-Tier Architecture for an overview of these components).

Business Tier < - - > Data Tier

The SQL Server database sets up a listener to handle requests, and the Business Tier makes its requests over the standard SQL Server port(s). The connection string information is located in the file **BusinessTierSettings.xml** under the **DataTierAddress** setting.

Business Tier < - - > Client Tier

The Business Tier and Client Tier use .NET Remoting to communicate. CAREWare ships with Remoting wrapped in HTTP protocol. The Business tier sets up a listener for Client requests, and sends replies to these requests over a single port. This port information is stored in the file **RWCAREWareRemoting.config.** The Client has a similar file, called **ClientTierSettings.xml** that has its connection information (this file is always located in the same folder client.exe is located). In both of these files, the communication port is specified, and this is the port that is used for all communications (the default port is 8124). If the Business tier is located behind a firewall, then this port must be opened on the firewall and forwarded to the computer hosting the business tier.

Changing the default port (8124) on the Business Tier

The only way to change the port that the Business tier listens on is to manually open the RWCAREWareRemoting.config file and change the port setting. Note that once this is changed, any client that wishes to communicate with that Business tier MUST use the new port. Changes to the configuration file will not take effect until the business tier service is restarted.

Changing the default port (8124) on the Client Tier

The port that the client file uses can be changed in two ways – either by manually editing the ClientTierSettings.xml file, or from inside RW CAREWare. The client keeps a separate entry in its config file for each server that it wants to connect to, along with the port information. Thus, a client can make connections to any number of servers over any number of ports (of course it can only use one connection at a time). The connection port is specified when the server connection is initially set up (the default value is still 8124).

Backing Up Data

Microsoft's SQL Express database has built in procedures for backing up and recovering the data. RW CAREWare provides functionality that will invoke the Transact SQL that creates the backup files from inside the program itself (Advanced users that still desire to back up the database manually using Transact SQL or SQL Server's Enterprise Manager will still be able to do so, of course, but these tools will not be required). Using this functionality, a user will be able to specify where the backup will be placed. Then when the backup utility is run, it will save the backup files to the specified location, where they can be stored, archived, etc.

If an installation is using SQL Server, the backup procedure is the same is it is for SQL Express. SQL Server will provide more tools, including the Enterprise Manager. This provides administrators with many tools for managing the database that are not covered in this document.

Keeping RW CAREWare Up To Date

The CAREWare client tier helps with keeping itself up to date by using its self-updating smart-client technology. Using this, the Client automatically checks for updates from the Business Tier every time the program starts. If there is a new version, it is automatically downloaded from the Business Tier and installed. This ensures that the three tiers of the program will always be on the same version. This means that clients only have to be installed on a computer once, and from then on they will update themselves.

Any updates to RW CAREWare will come in the form of an *.msi installation package. This package will update all files that require updating on the Business Tier. The Business Tier will then automatically update the Data Tier as necessary, and have updates ready for download to clients that require them. Thus, whenever an update or new version of RW CAREWare is released, a user will simply run the setup file, and this will update the business tier, which will take care of everything else.

Setting up the Data Tier

Overview

Deploying the CAREWare data tier involves three steps:

Installing and Configuring SQL Server or MSDE

Two parts of this process are worth noting here. First, when installing SQL Server, there are options for allowing *only* Windows Authentication and for allowing Windows *and* SQL Server Authentication. CAREWare uses SQL Server Authentication, so this security mode must be enabled.

Second, you must decide whether or not there should be a password for the default administrator login, "sa." If the user configuring SQL Server decides to create an sa password, then whoever manages the data tier for RW CAREWare will need to know that password.

Configuring the CAREWare Business Tier Login Account (cwbt)

You will need to create the cwbt login account and assign a password to that account. If the password is different from the default cwbt password, then you will need to modify the business tier settings.

Copying and Attaching the Database Files and Making cwbt the owner of CW_Data.

The CAREWare data files are CW_Data.mdf and CW_Log.ldf. These need to be copied to a location that can be accessed by SQL Server.

SQL Server needs to be made aware of the existence of the data files before any further actions can be taken. Attaching the RW CAREWare data files to SQL Server adds a reference ("CW_Data") to SQL Server's list of known databases.

Finally, the user needs to make the cwbt account the owner of the CW_Data database.

Automated Installation

CAREWare is used in a broad range of situations. Statewide Part B grantees with many real-time providers likely will have more complicated configuration demands and likely will have experienced staff who will want to configure the data tier manually. However, smaller providers using a standalone configuration might have no staff with expertise in this area.

To ease installations at providers with less knowledgeable users CAREWare provides an installation wizard that helps walk you through the three steps described above.

Manual Installation

The following technical information might be helpful for users installing the data tier manually.

Installing and Configuring SQL Server or MSDE

SQL Server

Using the SQL Server Enterprise Manager, you can change the Security Mode and sa password after installation. To change the security mode through the Enterprise Manager, right-click the server that will run the data tier, go to Properties, go to the Security tab, and select Mixed Mode. Advanced users can also change the Security Mode by editing the registry key

"HKLM\Software\Microsoft\MicrosoftSQLServer\ Instance Name\MSSQLServer\LoginMode."

Similarly, the sa password can be changed after installation through the SQL Server Enterprise Manager. To do so, expand the relevant server, expand Security, select Logins, right click the sa account (visible on the right-hand side of the screen), choose properties, and then change the password.

SQL Express

The SQL Express Security Mode is established at installation. The default is Windows Authentication, so users need to specify Mixed Mode by using the SECURITYMODE=SQL switch.

The sa password is also established at installation. To set a specific password, use the SAPWD="*sa_password*" switch; if you want the sa password to be blank, use the BLANKSAPWD=1 switch.

Here's a sample MSDE installation script that specifies Mixed Mode and a blank sa password. This kind of installation can be run from a DOS prompt or by clicking Start and then Run.

```
C:\[PathToSetupFolder]\setup.exe

BLANKSAPWD=1 SECURITYMODE=SQL
```

Once SQL Express is installed, it will be started the next time the computer is restarted. To restart it manually, click Start → Settings → Contral Panel, double-click Administrative Tools, double-click Services, right-click the MSSQL$VSdotNET service, and choose Start.

Configuring the CAREWare Business Tier Login Account (cwbt)

In this step you will create the SQL Server account that the RW CAREWare business tier uses to connect to the data tier. As a default, the business tier is configured to use 'cwbt100' as a password. If you wish to use a different password, you will need to modify the BusinessTierSettings.xml file that resides in the 'Server Application/bin' folder on the computer running the business tier; look for "password" under "DataTierAddress" in the XML structure.

If things go wrong

CAREWare has a handy tool calles cwadmin.exe

Copying and Attaching the Database Files and Making cwbt the owner of CW_Data.

Save the CW_Data.mdf and DW_Log.ldf files to a convenient location on the server. The default location for SQL Server data files is the C:\Program Files\Microsoft SQL Server\MSSQL$VSdotNET\Data folder, but SQL Server does not require that its data files be in any specific folder. Then, to attach the database:

SQL Server

Expand the relevant server, right-click on Databases, choose All Tasks, and choose Attach Database. On the screen that pops up, indicate the path to the CW_Data.mdf file, and in the Attach As box type "CW_Data". Next to Specify Database Owner, choose the cwbt account.

MSDE

To attach the RW CAREWare database using OSQL, use the sp_attach_db stored procedure. For example, the following script would work for the default path to the data files:

```
osql –S [servername]\VSdotNET –U
```

```
sa –P –Q “EXEC sp_attach_db
‘cw_data’, ‘C:\Program
Files\Microsoft SQL
Server\MSSQL$VSdotNET\Data\CW_Dat
a.mdf’,

‘C:\Program Files\Microsoft SQL
Server\MSSQL$VSdotNET\Data\CW_Log
.ldf’”
```

To make the cwbt account the owner of CW_Data, use the sp_changedbowner stored procedure. Here’s how it might look:

```
osql –S [servername]\VSdotNET –U
sa –P -d cw_data –Q “EXEC
sp_changedbowner ‘cwbt’”
```