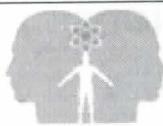


APPROVALS:

Department	Name	Signature	Date
QA	Scott Pletzer		25Oct12
OPS	Michael Stowell		25Oct12
Exec	Nancy Rizzo		10/25/12
IS	Andrew Mason		10/25/12



1.0 Purpose

The purpose of this document is to describe the specifications and design that will be implemented for the Application Functions in the ClearView system.

2.0 General Requirements

Where appropriate, logic should be contained in try/catch blocks and any exceptions should be logged using the standard logging mechanisms.

3.0 Definitions

SaaS	Software as a Service
------	-----------------------

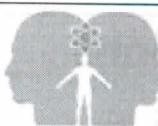
4.0 Specifications

Requirement #4.1: The system must close after a specific amount of time of inactivity per HIPPA regulations. The initial amount of time should be 15 minutes. Inactivity is defined as no keyboard input or mouse clicks within the time frame.

Specification: A monitoring object will be created that will watch the windows message queue for messages related to either keyboard input or mouse clicks. If none of these messages are seen, a counter will be started to record how much time passes before one of these events is seen again. If the amount of time exceeds the defined amount of time that the application can be idle, the application will be automatically closed. This check will be temporarily suspended when performing a calculation or analysis as there is no possibility of a keystroke or mouse click during these times.

Requirement #4.2: The system must contain a main menu in order for the user to easily navigate through the application.

Specification: A menu ribbon will be used containing the various core functionality that the ClearView system offers.



Based on the user's role, some of the options may not be available to a given user. When an option is not accessible for a given user, the option will be removed and not displayed in the toolbar.

Requirement #4.3: The system must be windows based and be written using the .Net framework.

Specification: The application will be constructed using Visual Studio 2008 and will use C# as the base language. Mathematical analysis will be done using a combination of C# and Matlab.

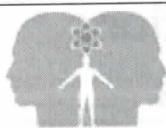
Requirement #4.4: The system must persist data in a Microsoft SQL Server Database, version 2005 or greater.

Specification: The application will be developed on Microsoft SQL Server 2005 but will also be fully compatible with SQL Server 2008.

Requirement #4.5: The system must synchronize with an external controlling server. This server will be used to provide authentication for scans, archival functionality for images and other tasks.

Specification: The system will sync through a series of web service calls with Software as a Service (SaaS) based application that is code named 'EPIC Central'. All transactions will take place across an encrypted https connection. ** This has not yet been made live, it will be turned on in a future release of the software.

Requirement #4.6: The system should allow patients to be added and managed.



Specification: A button is available on the main menu to allow the user to search the patient data and to enter new patient demographics. The specifications for the patient demographics are described in the Patient Demographics Functions- Specifications.

Requirement #4.7: The system should allow a calibration process to be performed on the scanning devices.

Specification: A button is available on the main menu to perform calibration. The process of calibration is described in the Camera Functions- Specifications.

Requirement #4.8: The system should allow for the capture of new images for a patient, as well as the analysis and results reporting for the images.

Specification: A button is available on the main menu to perform the capture process. The capture process itself is described in the Capture Functions- Specifications.

Requirement #4.9: The system should allow historical scans (i.e., patient energized images) and the analysis results (i.e., report displays) to be searched and reviewed by a user. The requirements for this functionality are defined in the Capture Functions- Requirements document.

NOTE: Scan functions include the Manage Patients functions, Capture functions, Camera functions, and the Report functions excluding the Admin Page and all associated functions.

Specification: A button is available on the capture search dialog that will allow a user to view a historical scan. The view process itself is described in the Capture Functions- Specifications.

Requirement #4.10: The system should display the version number in the upper section of the main page.

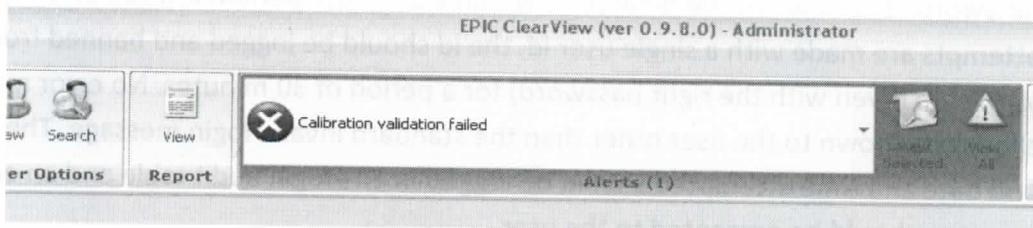
Specification: The version number is shown in the title bar of the application and therefore can be seen from any section of the application.



EPIC ClearView (ver 0.9.8.0)

Requirement #4.11: The system should allow for notifications to the user to be displayed in a noticeable area regardless of the function that is currently being performed.

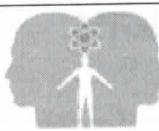
Specification: A notification area has been added to the application in the main menu area. The section will display that there is a message and the user can then drill into it to see the content.



Requirement #4.12: The system should allow the device settings to be modified and persisted. These settings will be used by the application when controlling the device. This section is accessible to the "administrator" or "techadministrator" login only. These settings include:

- Camera to use
- Firmware Type
- Brightness
- Gain
- Exposure Delay

Specification: A main menu link labeled 'Settings' will be available to the main menu for the "administrator" and "techadministrator" only; the link will not appear for any other user. Clicking on the link will take the user to a page that allows the values specified above to be set:



Device Settings

Interface Name:	USB <> Serial	Brightness:	84
Camera:	Philips SPC 900NC PC Camera	Gain:	63
Firmware Type:	HRFirmware	Exposure Delay:	310

Apply Settings

In addition to the required fields, another field called 'Interface Name' was added to the page. This is the device name of the USB controller for the scanner.

Requirement #4.13: A throttling mechanism should be put in place on the login screen to prevent a user from attempting to log in more than 3 times in a row with an invalid password. 'In a row' can be defined as within a 3 minute period. If three or more attempts are made with a single user id, the id should be logged and banned from logging in (even with the right password) for a period of 30 minutes. No error message should be shown to the user other than the standard invalid login message. The user id and date and time attempted should be logged in and login audit table and an error message should be presented to the user.

Specification: All failed login attempts to the ClearView software are now captured and saved in a database table. The table is shown below; it contains the name of the user that tried to log in as well as the failure time and date.

FailedLoginTracking	
<input type="checkbox"/>	FailedLoginTrackingId
<input type="checkbox"/>	UserName
<input type="checkbox"/>	FailedDateTime
<input type="checkbox"/>	TemporarilyBanned

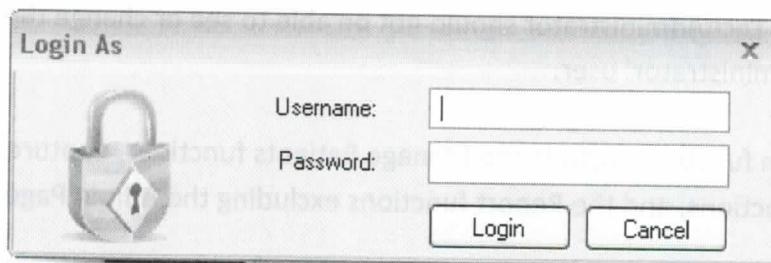
If three login failures for the same user happen within three minutes of one another, the username is marked as temporarily banned for a period of 30 minutes from the third failure. Any user that is temporarily banned will not be able to log in even with the correct credentials until 30 minutes has passed from the time of the infraction.

When a user has been banned, the user will receive the same login failure message as is received when the username/password combination is invalid. This is considered an

authentication best practice, as to not give the user any indication as to what logic is happening behind the scenes.

Requirement #4.14: The system must only be accessible to a user that has a valid User Id and password combination.

Specification: In order to gain access to any component of the ClearView application, the user must sign in with a combination of credentials (User Id / Password).



The passwords are required to be between 8 to 50 characters, and must contain at least one of each of the following character types:

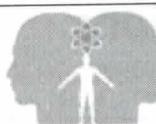
- Lowercase letters
- Uppercase letters
- Numbers
- Special characters (#, @, !, etc.)

This combination at a minimum provides a possibility of more than 2 billion combinations.

Requirement #4.15: The system should allow the currently logged in user to be changed without requiring a shutdown of the application.

Specification: An option is available on the main menu that allows a user to log in and effectively replace an existing user. The new user's permissions, etc. are then used to determine system behavior.

Requirement #4.16: Functions within the system must be delegated by role. There will be four roles in the system:



- EPIC User- has access to scan functions only.
- EPIC Administrator- has access to scan functions as well as user administrative functions like the Users functions.
- System Administrator- has access to all areas of the ClearView software including Administrative functionality in the Capture, Camera and Report functions.
- TechAdministrator- has access to camera setting functionality and will be shared with manufacturing parties and others that require access to camera settings. The TechAdministrator should not be able to see or change the core 'Administrator' user.

NOTE: Scan functions include the Manage Patients functions, Capture functions, Camera functions, and the Report functions excluding the Admin Page and all associated functions.

Specification: The four roles are recognized by the system, the first two are assignable within the interface (CustomerUser and CustomerAdmin), the other two roles are static and not assignable (Administrator, Technician).

CustomerUser accounts will have access only to the Manage Patients functions, Capture functions, Camera functions, and the Report functions. Any functionality identified in the specifications for these areas as accessible by the Administrator only will not be available to the CustomerUser accounts.

CustomerAdmin accounts will have access to the Manage Patients functions, Capture functions, Camera functions, and the Report functions. Any functionality identified in the specifications for these areas as accessible by the Administrator only will not be available to the CustomerUser accounts. Additionally, the CustomerAdmin accounts will have access to the Manage User functions.

TechAdministrator accounts will have the same full permissions as the base 'Administrator' (which has access to everything) with the following exceptions:

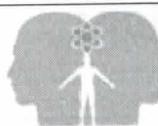
- They do not have access to the Export functionality
- They cannot manually load images
- They do not get the admin tab when viewing a patient's scan
- They cannot resubmit images
- They do not see the whole energized image on the Biofield display



Requirement #4.17: The system should allow for the creation and management of users. The following information should be captured for a user:

Field Name	Validation	Required
Username	(4 -50 Characters, Unique)	Yes
Password	(8-50 Characters, must have a minimum of 1 upper case letter, 1 lowercase letter, one number and one symbol)	Yes
First Name	None	Yes
Last Name	None	Yes
Middle Initial	None	No
Email Address	Valid format	No
User Role	Must be one of roles specified in this requirements document	Yes

Specification: The system will allow the creation of an unlimited number of users. There is a dedicated section for user creation that can only be accessed by a CustomerAdmin, Administrator, or Techadministrator user. The section allows the basics of a user to be created.



AddUserForm

Application User			
Login Info		General Info	
User Name:		First Name:	Mi: Last Name:
<input type="text"/>		<input type="text"/>	<input type="text"/>
Password:	<input type="password"/>	E-mail:	<input type="text"/>
Confirm Password:	<input type="password"/>		
Phone Number			
AreaCode	PhoneNumber	Extension	PhoneTypeId
<input type="text"/>			
<input checked="" type="checkbox"/> Login Enabled		<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>	
Role Assignment			
<input type="checkbox"/> CustomerAdmin <input type="checkbox"/> CustomerUser			

All values pertaining to a user are set here; the user will become active as soon as they are created. At any time, a user's attributes can be edited by a CustomerAdmin or Administrator user. The edit page is the same as the user creation page from the aspect of functionality.

Requirement #4.18: The administrator and techadministrator logins should have the ability to capture an image from the settings page in order to perform testing of the device.

Specification: A new tab has been added to the application page that appears when hitting the 'Settings' button from the main application menu. The 'Settings' button is only available to the administrator user and the techadministrator user. The new tab entitled 'Device Testing' and contains the functionality necessary to connect to a camera, energize the camera and collect images.



Application Functions Specifications

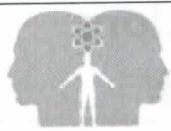
The screenshot shows a software application window titled "Application Functions Specifications". The left side has a sidebar with "Settings" and tabs for "Device Settings" and "Device Testing". Under "Device Settings", there are dropdown menus for "PwM0 Frequency" (set to 110Hz), "Exposure Duration" (set to 5 seconds), and "Boost Voltage" (set to 100% Power). There's also a section for "Other Options" with checkboxes for "Write Images to Disk" and "Write Settings on Image", both of which are checked. Below this are "Device Actions" buttons for "LED On", "LED Off", "Get Information", "Begin Exposure", "Boost Voltage On", "Boost Voltage Off", "Force Reset (R=1)", and "Abort". At the bottom are "Start Duty Cycle", "Clear Log", and "Save Log" buttons. The main area is divided into three sections: "Live Preview" (a dark video feed), "Captured Image" (a white placeholder box), and "Device Status" (a table listing various parameters like Device Status Code, LED Status, Exposure Duration, etc., all currently set to "Unknown").

On this page, the different settings for the camera can be manipulated

Requirement #4.19: The administrator and techadministrator logins shall have the ability to see the feedback from the firmware 'Get' command after an image capture has been performed on this page. This display would include the following values:

- Device Status Code
- LED Status
- Exposure Duration
- PwM0 Frequency
- PON State
- Boost Voltage Reading
- PwM0 Width
- Reset Condition Code

Specification: In the previously mentioned 'Device Testing' section of the application, the administrator can see the values below that are retrieved from the firmware.



Device Status

Device Status Code: 00
LED Status: On
Exposure Duration: 00.5
Boost Voltage Setting: 100
PwM0 Frequency: 1100Hz
PON State: On
Boost Voltage Reading: 125.2 volts
PwM0 Width: 14uS
Reset Condition: 1E
Firmware Version: 3.3

The administrator can either ask the device for the values directly (using one of the buttons supplied on the interface), or the call will automatically be made each time the device is energized to capture an image. The call is made to get the information approximately 200ms after the end of the exposure.

Requirement #4.20: The administrator and techadministrator logins shall have the ability to save the captured image (with or without the voltage and frequency displayed on the image).

Specification: The testing page provides two check boxes that can be toggled at any time in the process to achieve the requirements.

<input type="checkbox"/> Write Images to Disk	
<input checked="" type="checkbox"/> Write Settings on Image	

If the 'Write Images to Disk' checkbox is checked, each image that is captured will be saved in the same location as the location of the application. The images will be named 'SampleImageXXX.bmp' where XXX is a sequential number, incremented by one for each image captured.

If the 'Write Settings on Image' is checked, the image that is saved will have the Voltage and frequency stamped in it, both on the display and in the saved image.



Voltage = 100% Power
Frequency = 1100Hz

The user also has the option of right clicking on the captured image and manually saving the image to the location of their choice.

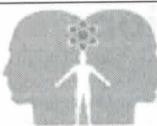
Requirement #4.21: The administrator and techadministrator logins shall have the ability to see a log of the commands that were sent to the device.

Specification: The testing page contains a list box that houses a log of all communications between the software and the device (at the protocol level). An example of the log can be seen below:

```
02:21:06.875 - Sending: l=1
02:21:06.906 - Received: >,00,l=1
02:21:08.796 - Sending: l=0
02:21:08.828 - Received: >,00,l=0
02:21:11.062 - Sending: f=1100
02:21:11.093 - Received: >,00,f=1100
02:21:11.093 - Sending: e=00.5
02:21:11.125 - Received: >,00,e=00.5
02:21:11.125 - Sending: v=100
02:21:11.156 - Received: >,00,v=100
02:21:11.156 - Sending: g
02:21:11.171 - Received: >,00,g
02:21:11.062 - Sending: f=1100
02:21:11.093 - Received: >,00,f=1100
02:21:11.093 - Sending: e=00.5
02:21:11.125 - Received: >,00,e=00.5
02:21:11.125 - Sending: v=100
02:21:11.156 - Received: >,00,v=100
02:21:11.156 - Sending: g
02:21:11.171 - Received: >,00,g
02:21:11.984 - Sending: i
02:21:12.062 - Received: >,00,i,0,00.5,100,1100,1,127.2,14,1E,3:3,R03.99.20
```

Requirement #4.22: The command log shall be able to be saved and cleared at any time.

Specification: A link exists below the log labeled 'Save Log', clicking on this link will bring up a dialog allowing the user to select where to save a copy of the log and what to call it. The file will be saved in standard ASCII format:



02:21:11.171 - Received: >,UU,g
02:21:11.984 - Sending: i
02:21:12.062 - Received: >,00,j,0,00,5,100,1100,1,127,2,14,1E,3:3,R03,99,:
[redacted]

[Clear Log](#)

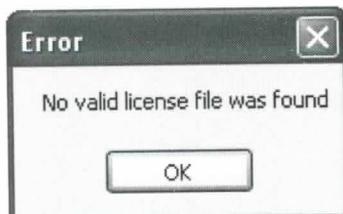
[Save Log](#)

Requirement #4.23: The ClearView system should require that a license file be present before the software can be used.

Specification:

Startup Behavior

The ClearView now looks at start up for a file named 'ClearView.lic' to be located in the same folder as the ClearView application itself. This file is a plain text file containing an encrypted string that represents the actual license structure. If the license file is not located by ClearView at start up, the following message is displayed and the software is not allowed to start.

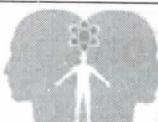


If the license file is located and found through inspection to be valid, the ClearView log in screen will appear as normal.

License Modes

Two types of licenses can be generated for the ClearView application, a 'Basic' license and a 'Full' license. The ClearView system has been architected to behave slightly differently based on the license it finds. In 'Basic' mode, the user will only get a single 'tab' after the analysis process containing a simplified version of the ClearView report. The simple version of the report will only display one section containing a listing of finger names and measurement points.

Right Thumb/Left Thumb {measurements}



In the second license mode configuration 'Full', the ClearView software will display all tabs after analysis, and the complete ClearView report will be displayed.

License Structure

The basic format of the license file is a simple XML file containing two nodes. This will likely be expanded in future releases. The format of the XML file is shown below:

```
<EPICLicense>  
  <CustomerName>EPIC Test License</CustomerName>  
  <LicenseType>Full</LicenseType>  
</EPICLicense>
```

The node <CustomerName> will contain the name of the customer as it appears in the EPIC Central system. Eventually EPIC Central will generate this license file. The node <LicenseType> will contain one of the following: Full or Basic

Encryption

The license file will never be deployed as an XML file, it will be encrypted before delivery to the ClearView system. The tool of choice for this encryption is a Freeware application and library called CipherLite.NET. This application and its associated library is used to encrypt the license key before delivery and decrypt it within the app as necessary.

The type of encryption selected is a 256 bit salted Rijndael algorithm. The license file is encrypted using the following Key and Salt values:

Key: A45u9\$lk*72ETH345wersg^

Salt: 74hdkjh35h2kjh34k2h3hkIKJ##4hjh3

License Deployment

The deployment of the license is simple; the file containing the encrypted string needs to be located in the same folder as the ClearView application and must be named "ClearView.lic".

Requirement #4.24: The license file should be strongly encrypted as to not be able to be modified by the average user.



Specification: A 256Bit Rijndael encryption algorithm was used to encrypt the string. Rijndael is the algorithm that has been selected by the U.S. National Institute of Standards and Technology (NIST) as the candidate for the Advanced Encryption Standard (AES).

Requirement #4.25: The ClearView system should support three types of licenses, Basic, Full and Cardiovascular (CV).

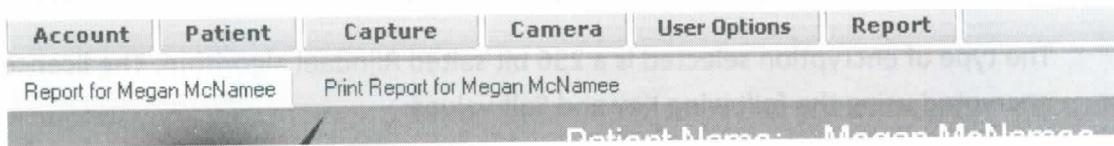
Specification: As describe above the license will contain three modes, 'Basic', 'CV' and 'Full'. This mode will be evaluated at runtime and the behavior of the application will act accordingly.

The node in the license file <LicenseType></LicenseType> will contain either 'Full' , 'CV' or 'Basic'. This will not be visible as the value contained in the license file is encrypted.

Requirement #4.26: A ClearView system utilizing a Basic license will display two output tabs upon completion of processing. One will contain the ClearView Basic printable report and the other will contain the working report (graphics, etc.).

Specification: The license file will be continually evaluated each time a scan is performed to determine which tabs to display as output from the processing algorithm.

If the license file contains the type 'Basic', the following will be displayed after a scan is performed and analyzed.

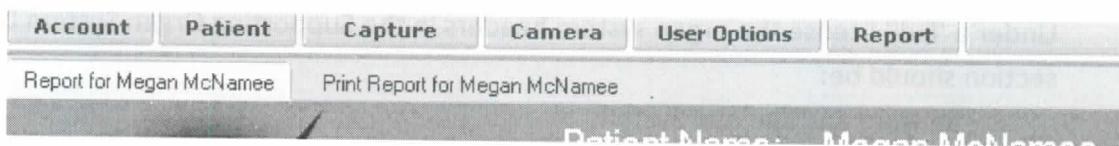


Requirement #4.27: A ClearView system utilizing a Full or CV license will display two output tabs upon completion of processing. ClearView Users, ClearView Administrators, and TechAdministrators will have the Print Report and working report tables. EPIC Administrators will have the above mentioned tabs and a tab of admin pages as well as a tab of Biofields.

Specification: The license file will be continually evaluated each time a scan is performed to determine which tabs to display as output from the processing algorithm.



If the license file contains the type 'Full' or 'CV', the following will be displayed after a scan is performed and analyzed.



Requirement #4.28: The ClearView report displayed in the ClearView system utilizing a 'Full' license will be significantly different in format and content than the report under the 'Basic' license. The report formats will be developed based on Regulatory department feedback and documented in the final Application Functions Specifications.

Specification: The report that is displayed under the 'Basic' license will have just one section that will show the Hand/Finger and measurement point description as well as the values measured.

The report that is displayed under the 'Full' license will have four distinct sections:

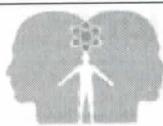
- Overview Text
- Overview Scores
- Detail Organ System Scores
- Organ Relationship Section

Requirement #4.29: The ClearView report displayed in the ClearView system utilizing a 'CV' license will be significantly different in format and content than the report under the 'Basic' license.

Specification: The difference between the reports will be the number, order and names of the section headers that appear in the 'Supporting Organ System Detail' section of the report.

Under a 'CV' license the organ system headers in the Supporting Organ System Detail section should be:

- Cardiovascular
- Respiratory
- Gastrointestinal System
- Hepatic, Endocrine, and Nervous System



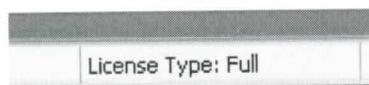
- Renal and Reproductive

Under a 'Full' license the organ system headers in the Supporting Organ System Detail section should be:

- Sensory and Skeletal System
- Hepatic, Endocrine, and Nervous System
- Cardiovascular System
- Respiratory System
- Gastrointestinal System
- Renal and Reproductive Systems

Requirement #4.30: The license type being used (Full, Basic or CV) should be displayed to the user in an easy to recognize location.

Specification: The type of license being used is displayed as soon as the application is started the title bar. The value will always read one of the following 'Full', 'CV' or 'Basic', if no license file is available, the application will not start.



Specification: Two assignable roles and one unassignable role will be created within the ClearView system. The roles will be referred to as :

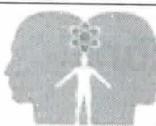
- ▲ CustomerAdmin
- ▲ CustomerUser

The relationship to the requirement is:

EPICUser = CustomerUser

EPICAdministrator = CustomerAdmin

The unassignable role is the system administrator and that will be only for the user 'Administrator'.



Requirement #4.31: The ClearView system must interact with EPIC Central (the SaaS application) on a regular basis. If communication does not occur for a configurable amount of time or longer, a scan cannot be performed.

Specification: The ClearView software will check for access to EPIC Central every 30 seconds when running. If access cannot be achieved, a counter is begun to track the amount of time that EPIC Central has been inaccessible.

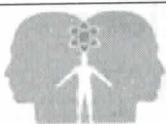
If the time that EPIC Central has not been accessible is greater than 48 hours, a new scan can not be performed. This check is made each time a user attempts to perform a scan.

As soon as a connection is re-established with EPIC Central, the access counter is reset back to zero and another 48 hours of no access can go by before scanning will be disabled again.

Requirement #4.32: The system must check prior to every scan, it is allowed to perform a scan. If it is not, the process of performing a scan must not be allowed.

Specification: Prior to the start of every scan, the following checks are done in order to determine if the scanning process should be allowed.

```
public static class SystemAccounting
{
    /// <summary>
    /// Helper method to determine if a scan can be performed. A multitude
    /// of checks are performed based on different potential situations
    /// such as the synchronizer being down, etc.
    /// </summary>
    /// <returns>Boolean indicating if a scan can be performed</returns>
    public static Boolean CanScanBePerformed(out String StatusMessage)
    {
        try
        {
            // Check if the synchronizer can be seen
            if (DataCacheManager.SynchronizerAvailable)
            {
                // Check if synchronizer has talked with EC, if not how much time has elapsed
                if (WSInterfaces.RecentContactWithHost())
                {
                    // Check if the device is authorized to perform a scan
                    if (WSInterfaces.IsDeviceAuthorizedToScan() == IsAuthorizedStatus.Authorized)
                    {
                        // Check if normal scans are available
                        if (DataCacheManager.Customer.ScansRemaining > 0)
```



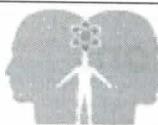
```
{  
    StatusMessage = "";  
    return true;  
}  
if (DataCacheManager.Customer.GraceScans > 0)  
{  
    StatusMessage = "";  
    return true;  
}  
StatusMessage = "The are no scans available for use in your account, visit EPIC Central to  
purchase additional scans.";  
return false;  
}  
StatusMessage = "This device has been deactivated and can no longer be used for scanning.";  
return false;  
}  
StatusMessage = "There has been no communication with EPIC Central for more than " +  
GlobalSettings.AutomatedMonitoring.MAX_INCOMMUNICADO_TIME_IN_MINUTES + " minutes, verify  
connectivity.";  
return false;  
}  
StatusMessage = "Synchronizer is not accessible, no scan can be performed.";  
return false;  
}  
catch (Exception ex)  
{  
    StatusMessage = ex.Message;  
    return false;  
}  
}
```

The system first checks to see if the Synchronizer is available, the synchronizer service is responsible for managing the interaction between ClearView and EPIC Central. If this is not available, the application is not allowed to start, or if the application is running, a scan is not allowed to start.

The system will then verify that ClearView has been able to access EPIC central within the past 48 hours, if not, scanning will be disabled.

The system will then check to see if the device at the location is authorized to be able to perform a scan. If this check fails, access to the scan dialog will be disallowed.

Finally, the system will check to see if the system has scans to use. The system will first check the scan pool, if there are no scans available to be consumed there, it will check the grace scan pool. If there are scans in either pool, the scan will be allowed, otherwise it will be prevented.



Requirement #4.33: The system must allow for a configurable number of 'Grace' scans to be performed when the number of paid scans reaches 0.

Specification: The system contains two 'buckets' of scans, paid scans and grace scans. The grace scan bucket is preset to a value of 50 and currently is not configurable via parameters.

The system will consume the paid scans each time a scan is performed until the value in the paid scan bucket reaches zero. At that point the grace scan bucket will begin to be consumed. When this bucket reaches zero, the ability to scan will be stopped.

When new scans are purchased, the grace bucket will be reset to the initial value of 50.

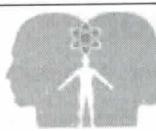
Requirement #4.34: The ClearView system must upload data to EPIC Central when a scan is completed, the data will consist of: (Patient Demographic Information, report data, and images).

Specification: Upon successful completion of a scan, the system will make calls to the synchronizer to schedule data to be synchronized between the ClearView and EPIC Central. The Treatment Id will be placed in the transfer queue, where the synchronizer will gather all associated data and transfer it in the background to EPIC Central.

The synchronizer works independently of ClearView, so once the entry is placed in the queue, ClearView can perform other actions regardless of the state of the data transfer.

Requirement #4.35: Users with the EPIC Administrator role must be able to see the number of scans the device has available to use.

Specification: A new menu items has been added that appears for users that have the EPIC Administrator role or greater specified.



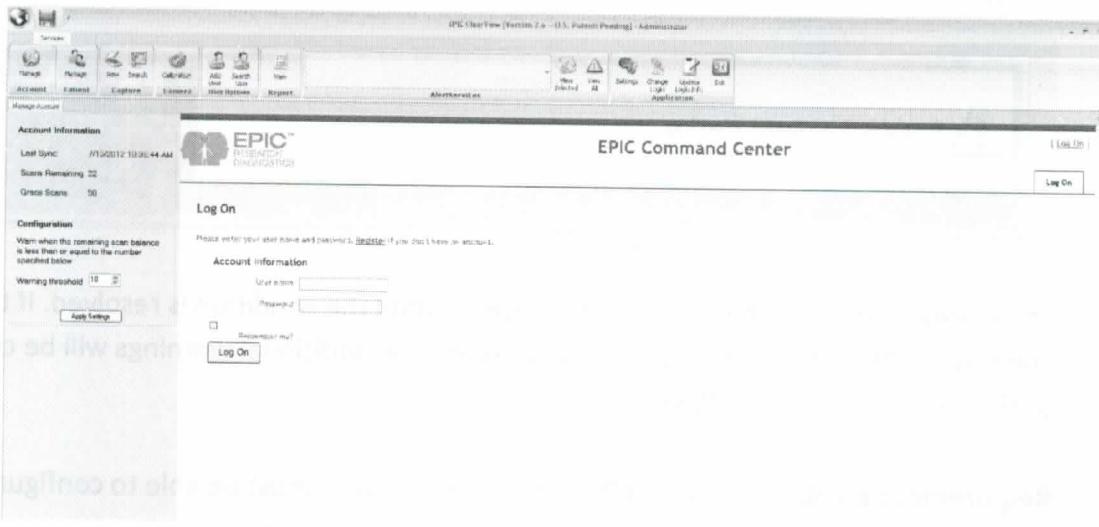
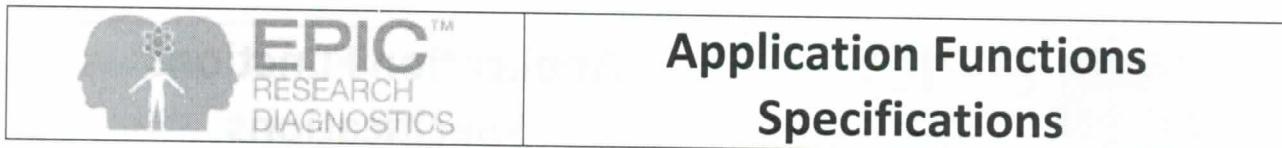
The 'manage account' tab will take the user to a page where the count of scans available and number of grace scans available can be seen. In addition, the last date and time a synchronization was completed is also displayed.

The screenshot shows a top navigation bar with tabs: Account, Patient, Capture, and Camera. The 'Account' tab is selected. Below the tabs, a sub-menu titled 'Manage Account' is open. Inside this sub-menu, there is a section labeled 'Account Information' containing the following data:

Last Sync:	7/13/2012 10:36:44 AM
Scans Remaining:	22
Grace Scans:	50

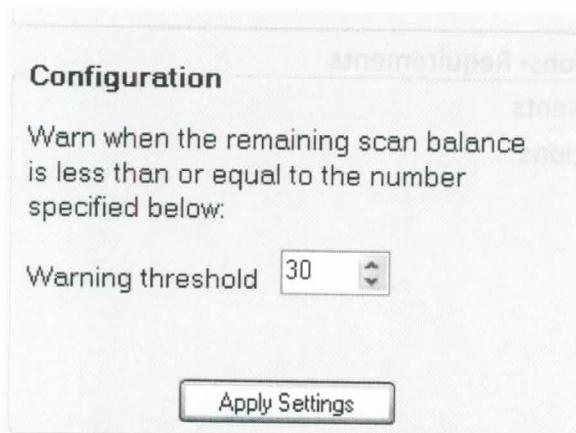
Requirement #4.36: Users with the EPIC Administrator role must be able to access the EPIC Central UI from with ClearView to make purchases and manage their account.

Specification: The 'manage account' tab mentioned above will also contain an embedded browser that will be defaulted to the EPIC Central URL. The user can log into EPIC Central through this browser and perform all of the functionality they could using a regular browser.

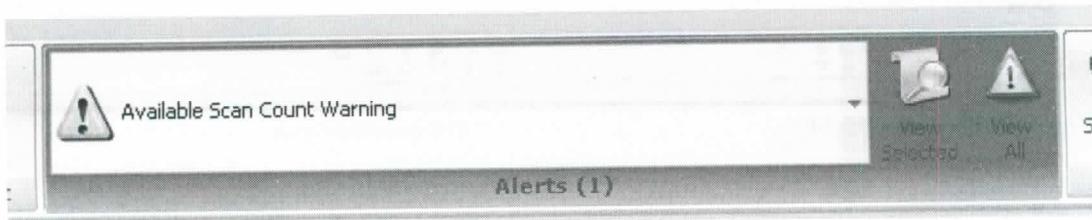
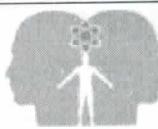


Requirement #4.37: ClearView must warn users when the number of scans available for a given device falls below a configured threshold.

Specification: The 'manage account' tab mentioned above will also contain an area where the user can configure the scan level that will trigger a warning to be displayed in the ClearView application.



When the number of paid scans reaches the number specified in the field above, the system will generate a warning that looks like the following.



The warning will reappear if the user deletes it, until the condition is resolved. If the warning is not removed during the users session, no additional warnings will be created, until a new session is initiated.

Requirement #4.38: Users with EPIC Administrator roles must be able to configure the scan count value that will trigger the “Low scan count” warning.

Specification: See #4.37 above.

5.0 Reference Documents

SS-001, Patient Demographics Functions- Requirements

SS-002, Capture Functions- Requirements

SS-004, Camera Functions- Specifications



Application Functions Specifications

Document Revision History