Introduction

Philips Respironics’ EncoreAnywhere software allows members of a patient’s care team to manage patient information. EncoreAnywhere is offered by Philips Respironics as a service to its home care provider customers, who have the ability to access their patients’ data as well as the option to create "users," such as a patient’s physician and other members of the care team, who can also access the data. The software provides a central data management system that tracks patient progress, collects and analyzes compliance and therapy data, and provides valuable reports about the data. The system is accessed through a supported Web browser, thereby enabling anytime, anywhere access to patient data.

This document provides information on the security and privacy features of EncoreAnywhere and its implementation in the United States.

Intended Use Statement

EncoreAnywhere is for use by clinicians or home care providers to gather, store, manage, and view compliance data created by many Philips Respironics sleep and home respiratory therapy devices. The software also includes the ability to enter therapy device setting information and transmit the settings to Philips Respironics therapy devices. Users can also enter other therapy and business information regarding patients. Data can be displayed in graphic and tabular form for both individual patients and across groups of patients to assess patients’ compliance with therapy and to perform business analysis. The software does not perform automatic scoring or diagnosis. The data it provides is only one of several elements to consider when evaluating patient compliance with therapy.

Product Security at Philips

We at Philips recognize that the security of Philips Healthcare products and services is an important part of your organizational security planning. We are dedicated to helping you maintain the confidentiality, integrity and availability of both electronic personal data (e.g., Electronic Protected Health Information – ePHI) and the Philips hardware and software products that create and manage these data. We encourage you to review our Philips Healthcare Product Security Policy Statement, which can be found on the product security page on the Philips Healthcare web site:

http://www.healthcare.philips.com/main/support/productsecurity

EncoreAnywhere is developed using industry and customer driven security requirements, a security risk assessment process, and an FDA-regulated quality system.

Privacy at Philips

Philips Respironics is committed to conducting business activities and making decisions in a manner that respects the personal data privacy of our customers, business partners and employees. The Philips Privacy Rules establish a uniform set of rules that apply to personal data. Our objective is to develop, implement and maintain a comprehensive privacy program enabling us to operate in compliance with applicable privacy laws and regulations and the Philips Privacy Rules.

User Requirements to Access EncoreAnywhere

EncoreAnywhere is designed so that users can access the service from their own workstations using their selected web browser. EncoreAnywhere does not involve the installation of server software or server equipment at customer locations.

The minimum requirements for user workstations to access EncoreAnywhere are:

Operating System Requirements	• Microsoft Windows (except “Home” editions of Windows XP or Vista) • the installation of some components, such as the data card server require administrator privilege, but administrative privilege is not required for normal use
Web Browser Requirements	• Microsoft Internet Explorer 7 or later or Mozilla Firefox • Popup blocker disabled for `https://www.encoreanywhere.com` • JavaScript • Cookies are required, but 3rd party cookies are not used • TLS (version 1.0 or later) with 128 bit minimum encryption • Browser plug-in required to upload data from SmartCards or SD cards to EncoreAnywhere
Cookies	• Used for session tokens and session keep alive.
Malicious Code Protection	• For the protection of the workstation and its data, the customer is encouraged to keep the software up-to-date with security patches and workarounds and use up-to-date anti- virus software
Other Software Requirements	• Microsoft Silverlight ○ 4.0 or greater • Adobe Acrobat • If the SmartCard card reader is used to upload therapy data and download therapy device settings: ○ the Infineer DT3500 driver is required to be installed ○ a card reader browser plug-in is required The following technologies are not used and can be safely disabled for this application: ▪ Java ▪ Adobe Flash ▪ Active X
Hardware Requirements	If the optional capability to upload patient therapy device data and to download prescription information from EncoreAnywhere to the therapy devices via SmartCards is used, the Infineer DT3500 by Mako Technologies is required. The DT3500 is tested, approved, and distributed by Philips. To upload therapy data and download prescription information between EncoreAnywhere and therapy devices via SD Cards, an approved SD Card Reader (P/N 1047300) is required.
Printers	Printing is supported but not required. Any printers that are capable of printing from Internet Explorer or Adobe Acrobat are supported. Not certified with any specific printers.

Network Connection Requirements	The EncoreAnywhere web application makes outbound connections to: ▪ HTTP (TCP port 80) ▪ HTTPS (TCP port 443) If data card server is used, the data card server running on the local computer will connect to the local computer using these ports: ▪ TCP port 943 ▪ TCP port 4523 If a host application white listing or a host firewall is used, the DataCardServer.exe application should be added as an authorized application.
Local Storage	No local drive storage required. There is an optional utility for migrating existing Encore data from EncorePro into EncoreAnywhere, and it stores data in flat files on the local hard drive. These files are automatically removed after the transfer of data is complete.
Backups and Data Archiving	Backup, archive and restore of data locally is not required or supported.
Other	RFID is not used as part of the solution.

Managing Users in EncoreAnywhere

User account management in EncoreAnywhere is completely under the customer's control. A customer can designate an employee to be the local EncoreAnywhere Company Encore Administrator. The Company Encore Administrator creates and deletes user accounts, resets user passwords, and assigns roles to employees. The Company Encore Administrator can view the list of users within the EncoreAnywhere application. The primary user roles are *Clinical User, Report User, Clinical Assistant User, Company Encore Administrator*, and *Office Encore Administrator*. The user interface only presents features to the user that they are authorized to access. The application authenticates users and verifies the user's authorization on each access. User accounts can have access privileges removed and can be deactivated without requiring deletion of the user account. User account logins and failed login attempts are logged (for more information on auditing, please see the section *Governance, Security and Privacy Policies, Compliance, and Audit*).

There are two sets of password policies, *standard* and *enhanced*. The company administrator can select the policy to apply to all of the company's accounts. The default policy is the 'enhanced' policy.

Usernames are unique per user. The usernames can be between 6 and 50 alphanumeric characters. The password rules for user accounts are:

	Standard	Enhanced
Users are forced to change passwords after any password reset or on initial login.	Yes	Yes
Users can change password at any time	Yes	Yes
Minimum password length	6	8
Valid characters	ASCII values (33-126)	ASCII values (33-126)

	Standard	Enhanced
Password composition	• At least one numeric character • One alphabetic character (A-Z, a-z)	• At least one numeric character • One alphabetic character (A-Z, a-z) • At least one special character: ~ ! @ # $ % ^ * , . ; : | = + -
Expiration	Every 90 days (the company encore administrator can change this default to expire passwords between 15 and	Every 90 days (the company encore administrator can change this default to expire passwords between 15 and 365 days).
Password reuse	Previous five passwords cannot be reused	Previous four passwords cannot be reused
Number of failed login attempts resulting in account lockout[1]	5	5
Prohibited passwords		• “password” • Password cannot contain user’s username
Password resets		An automatically generated temporary password 13 characters in length is generated.

Passwords are hashed (using SHA1), are not stored in plain text in EncoreAnywhere, and cannot be viewed by system administrators or customer service.

The password is masked as the user enters it.

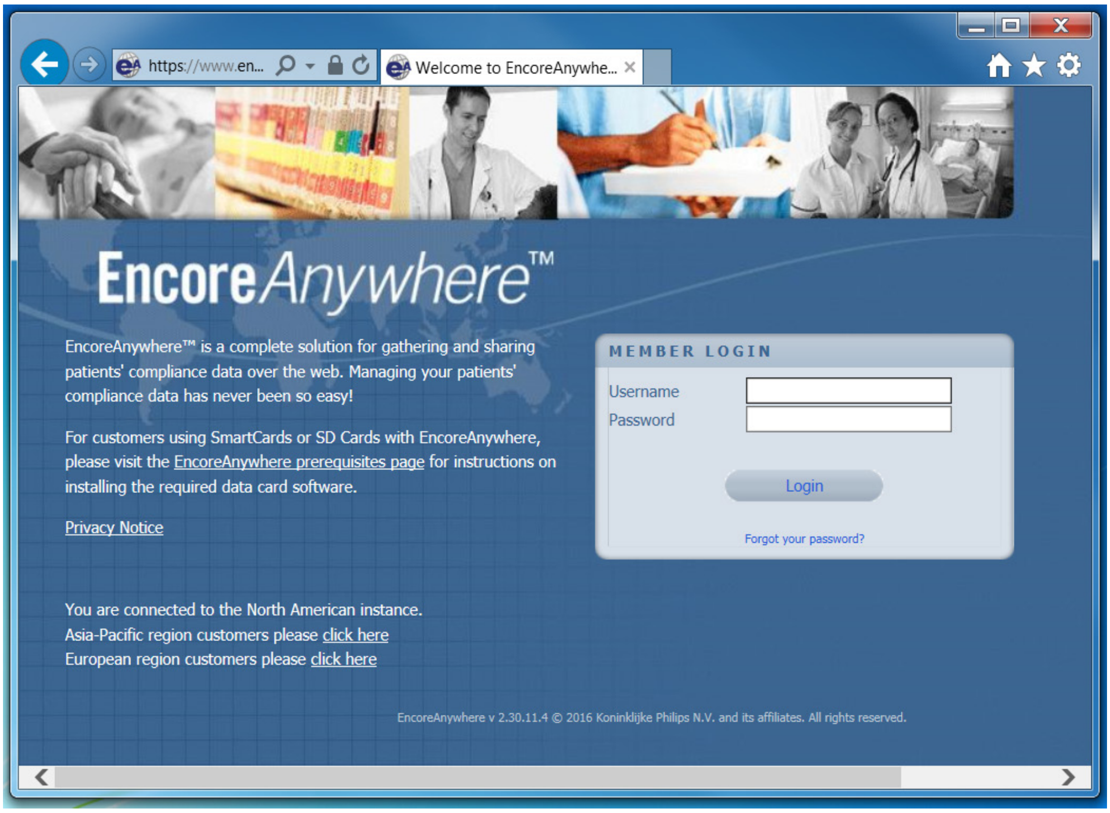
By default, users are logged off after 30 minutes of inactivity. The Company Encore Administrator can change this default to a value between 10 and 120 minutes. The automatic logoff does not cause the screen to be blanked. Customers desiring that functionality should enable the operating system screen saver/screen lock functionality to blank the screen after a pre-set period of inactivity.

The company Encore Administrators can obtain a report listing the last login date for their company’s users.

[1] Reactivation of locked user accounts requires customer administrator intervention.

Connectivity to EncoreAnywhere

We have implemented EncoreAnywhere using industry standard cryptographic methods to protect all information when it is communicated between EncoreAnywhere and patients, clinicians, customers, and medical devices.



EncoreAnywhere™ is a complete solution for gathering and sharing patients' compliance data over the web. Managing your patients' compliance data has never been so easy!

For customers using SmartCards or SD Cards with EncoreAnywhere, please visit the EncoreAnywhere prerequisites page for instructions on installing the required data card software.

Privacy Notice

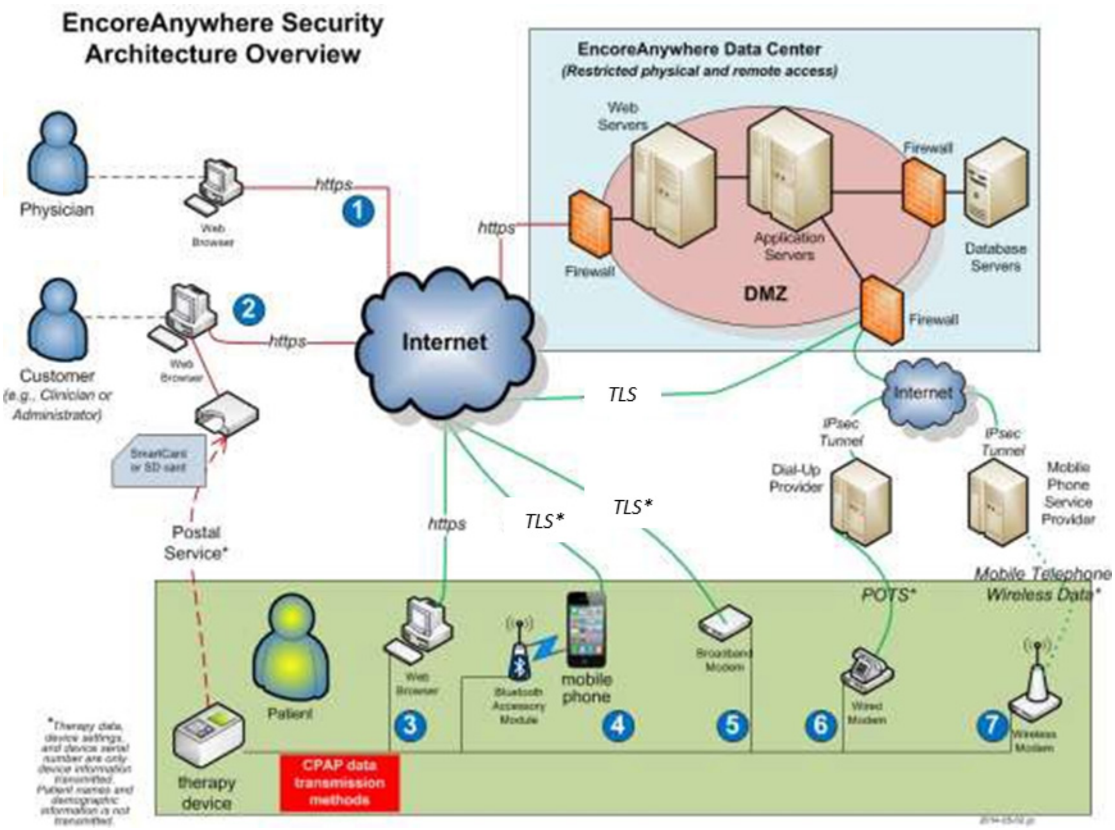
You are connected to the North American instance.
Asia-Pacific region customers please click here
European region customers please click here

EncoreAnywhere v 2.30.11.4 © 2016 Koninklijke Philips N.V. and its affiliates. All rights reserved.

There are three ways to connect to the EncoreAnywhere system:

- Customers and clinicians may connect to the EncoreAnywhere web application, WWW.EncoreAnywhere.com.
- Therapy devices may communicate with EncoreAnywhere to upload therapy data and download settings.
- Patients can connect indirectly through the DreamMapper mobile app or web site.

These connections are illustrated in EncoreAnywhere Architecture Overview diagram.


EncoreAnywhere Security
Architecture Overview
Physician
Web Browser
https
1
Customer
(e.g., Clinician or Administrator)
Web Browser
2
https
SmartCard or SD card
Postal Service*
Internet
https
EncoreAnywhere Data Center
(Restricted physical and remote access)
Web Servers
Firewall
Application Servers
Firewall
Database Servers
DMZ
Firewall
TLS
Internet
IPsec Tunnel
IPsec Tunnel
Dial-Up Provider
Mobile Phone Service Providar
https
TLS*
TLS*
POTS*
Mobile Telephone Wireless Data*
Patient
Web Browser
3
Bluetooth Accessory Module
mobile phone
4
Broadband Modem
5
6
Wired Modem
7
Wireless Modem
therapy device
CPAP data transmission methods
*Therapy data, device settings, and device serial number are only device information transmitted. Patient names and demographic information is not transmitted.

Customer and Clinician Access to EncoreAnywhere

A customer or clinician may connect to EncoreAnywhere from a web browser running on the customer's or clinician's workstation, and use commonly installed software, such as:

- Internet Explorer or Mozilla Firefox
- Adobe Acrobat
- Microsoft Silverlight
- JavaScript

The customer's or clinician's web browser connects to EncoreAnywhere using TLS with 128 bit minimum encryption.

Therapy Device Access to EncoreAnywhere

Therapy devices in use by patients also connect to EncoreAnywhere to upload therapy data and download device settings. These connections are illustrated in the EncoreAnywhere Architecture Overview diagram as the connection types three through seven.

	How the user/device connects	Security for the connection
●	Physician or clinician access to EncoreAnywhere through a web browser.	Connections to this web site are encrypted using *https (TLS).* Access via this connection cannot be restricted by IP address.
●	Customer or clinician access to EncoreAnywhere through a web browser.	Connections to this web site are encrypted using *https (TLS).* Access via this connection cannot be restricted by IP address.
●	The patient can connect and login to www.Philips.com/DreamMapper and upload data from their therapy device's SD card to EncoreAnywhere and download device settings.	Connections to this web site are encrypted using *https (TLS).*
●	The patient can connect via the DreamMapper mobile app (available for iPhone, iPad, iPod, and Android mobile devices) connecting with the Bluetooth Accessory Module attached to their therapy device. The mobile app serves as a pass-through to upload therapy data from the therapy device to EncoreAnywhere and download device settings to the therapy device.	Connections between the Bluetooth Accessory Module and the mobile phone are encrypted and connections between the mobile phone and DreamMapper are encrypted using *TLS*.
●	The patient's therapy device can connect to EncoreAnywhere via a Broadband modem attached to the patient's home network.	Connections to EncoreAnywhere from the Broadband Modem are encrypted using *TLS*.
●	The patient's therapy device can connect to EncoreAnywhere via a wired modem attached to the patient's telephone line.	Connections between the dial-up provider and EncoreAnywhere are encrypted using an *IPsec Tunnel*.
●	The patient's therapy device can connect to EncoreAnywhere via a wireless modem which connects over a commercial mobile phone network.	Connections between the mobile phone service provider and EncoreAnywhere are encrypted using an *IPsec Tunnel*.

EncoreAnywhere can also be used to send device settings from a clinician to a patient's therapy device. Both EncoreAnywhere and the therapy device verify the integrity of the configuration settings and verify they are delivered to the correct patient's therapy device.

Data Export Service

The Encore Patient Data Exporter simple query (EPDEsq) utility is a tool for generating a list of compliance and therapy data of patients in a given company within the EncoreAnywhere database. The output is a text file in either XML (Extensible Markup Language) or CSV (Comma Separated Values) formats and is filtered by export time period (e.g., start and end dates). The exported file is encrypted with AES-256 encryption and placed on an SFTP (Secure File Transfer

Protocol) site in a directory unique to each company, and that directory can only be accessed by IP (Internet Protocol) addresses for which the customer requests access in order to preserve the security of patient data. These IP addresses are specified in the export request form which must be filled out to begin scheduling a recurring data export. A unique username and a 16-character password containing both alphanumeric characters and symbols is generated for the company to access the location through a web browser or SFTP client and provided to the company requesting the data.

The SFTP server connections (version 2) can be authenticated using combinations of username, password, IP address, and client keys/certificates.

Operation and Development of EncoreAnywhere

The EncoreAnywhere servers are located in a secure data center in Andover, MA, with a backup/disaster recovery site in Santa Clara, CA. The service is managed by Philips personnel based in Pittsburgh, PA. The data center physical facilities are managed by NaviSite, a Time Warner Cable Company, and the facilities have received an SSAE-16 SOC-1 audit by an independent auditor within the past year. Access to the data center is strictly controlled and requires security measures such as identity and authorization verification, and badge access. The facilities have monitored environmental controls, including redundant HVAC, fire suppression systems, and CO_2 or halon extinguishers. They have an uninterruptible power supply (UPS) with a diesel backup generator and redundant internet connections.

EncoreAnywhere is physically segregated from other customers of NaviSite. The data in the database is encrypted at rest. It operates on an isolated production network with access restricted to only required protocols and services. The network has redundant, high availability network-based firewalls and intrusion detection systems (IDS). Routine vulnerability scanning is conducted and third-party security audit and intrusion detection providers are used. The network has deployed IP spoofing protection (RFC 2827/RFC 1918).

The EncoreAnywhere infrastructure is operated and maintained in accordance with an Information Security Management System (ISMS). The ISMS designates responsibilities related to information security and contains the security policies and procedures governing the operation of the infrastructure. Administrative access to the production environment is highly restricted and developers do not have privileged access to that environment.

All system changes are performed and tested in a controlled environment that mimics the production environment before being introduced to the real production environment. Changes to the environment are reviewed and approved by a change control board.

Access to servers is restricted to authorized system administrators. On all servers, unused services are disabled and unused ports are blocked. Industry leading anti-virus software is used and virus signatures are regularly updated.

Servers are dedicated to operating EncoreAnywhere and only run the applications and services required for the specific function they perform. The EncoreAnywhere system infrastructure has patch deployment policies and procedures. These include managing patches from vendors whose technology is used in the EncoreAnywhere application. Patches are reviewed based on criteria such as criticality and impact, and are installed on a regular basis through a predefined release cycle. Patches may be installed outside of the routine release cycle if a patch is determined to address a critical risk. During the deployment of patches, the application is thoroughly tested during each phase of the release cycle to identify any potential issues that might affect the proper functionality of the EncoreAnywhere application.

Regular backups of EncoreAnywhere data are performed every 15 minutes to intermediate disk storage and to the secondary data center. Philips Respironics sanitizes information system digital media removed from service using an approved, industry standard media sanitization procedure which includes tracking, documenting, and verifying media sanitization actions and periodically tests sanitization equipment/procedures.

Our development processes follow the Agile development methodology and include internal code reviews, independent reviewers, external vendor testing as design changes dictate, a documented change management process, quality assurance testing, and a security risk assessment process. External vendor testing includes web application security scanning.

Customer Service and Product Support

Philips Respironics product support and sales will assist you and your users with training before you start using EncoreAnywhere. Online help is available for all user and administrative functions in the “Help” section, and a printed system administration guide is available upon request.

In providing support to you for user assistance and problem resolution, Philips Respironics Customer Service might ask to remotely connect to the computer that is being used to access EncoreAnywhere. This remote access is optional and is used with customer permission only. Remote access is not required to use the EncoreAnywhere application or to receive support.

Philips uses a third party software package, BOMGAR, to provide this remote support. For more information concerning how this software works on the customer computers and networks, please see the “Ports and Firewalls” section of the BOMGAR Representative Guide in the Document Library on BOMGAR’s web site:

https://www.bomgar.com/docs

Customers are notified of updates to EncoreAnywhere by a notification that is displayed when logging into EncoreAnywhere. These notices inform users of when the update will occur and what changes will be made.

Governance, Security and Privacy Policies, Compliance, and Audit

EncoreAnywhere processes personal and sensitive data on behalf of our customers who manage patient compliance with sleep therapy devices which are prescribed by physicians for the treatment of sleep-disordered breathing patients. EncoreAnywhere can be used by home care providers to track their patients' compliance, by physicians to communicate prescription changes to their patients' sleep therapy devices, and by both home care providers and physicians to develop and manage patient records.

EncoreAnywhere is operated in compliance with the Philips Privacy Code and Privacy Rules. All of the third-party data processors that are currently involved with processing for the EncoreAnywhere application following binding corporate rules. The EncoreAnywhere / Philips Privacy Code and Privacy Rules are available at:

https://www.encoreanywhere.com/EncoreNetWeb/marketing/Privacy/privacy.aspx

There is a product and services security policy for Philips Healthcare which describes the governance structure for product security across all Healthcare business units. It establishes a set of requirements that products and services must meet. These requirements are derived from governmental regulations (such as HIPAA in the United States), industry standards, and customer requirements. It establishes the position of Director of Product Security and establishes a Product Security Leadership Council to regularly review and update product security policies and requirements.

Philips Respironics ensures that for any service provided by a subcontractor involving access to or processing of patient personal information, the subcontractor has executed a Business Associate Agreement (BAA) with Philips that complies with HIPAA. Philips Respironics has evaluated the security of our contracted service providers.

The NaviSite data centers have received an SSAE-16 SOC-1 audit by an independent audit within the past year.

EncoreAnywhere does not process credit card or financial transactions and, therefore, is not PCI certified.

Within EncoreAnywhere, data cannot be deleted by a user. Data is retained for minimum of 7 years.

At the customer's request, audit log data can be provided. The audit data includes:

- Capturing user access activity such as successful logon, and unsuccessful logon attempts
- Capturing data access inquiry activity such as screens viewed
- Creation and modification of ePHI

Philips Respironics follows a security and privacy event management policy for managing response to incidents and possible breaches. This policy complies with the requirements of HIPAA and HITECH, and includes customer notification as appropriate. If customers become aware of a problem or possible incident, they should report it to Encore Product Support:

- +1 800 345-6443, prompts 1,4,1,2; or
- encoreanywhere@philips.com

Philips Respironics' policy is to review incidents to determine the root cause, so that the appropriate system, security, or procedural remediation can be implemented.

Philips Respironics and our contractors have an effective system of recruiting and vetting personnel. Philips Respironics and our contractors also maintain formal procedures to restrict access to EncoreAnywhere data for departing employees or employees whose role changes.

Employees of Philips Respironics and our contractors receive ongoing privacy and security training, including the protection of Personally Identifiable Information (PII), Electronic Protected Health Information (ePHI), and other confidential information entrusted to Philips Respironics.

Respironics Inc.
1001 Murry Ridge Lane
Murrysville, PA 15668 USA

🏭

Respironics Deutschland
Gewerbestrasse 17
82211 Herrsching, Germany

EC REP

CE

1104773 R04
JLW 6/01/2016