PointClickCare®
SHA Encryption Certificate Update – Frequently Asked Questions

1) **What is SHA-2?**

   SHA-2 is a specific cryptographic technology originally developed by the National Security Agency (NSA) in the United States. Using a complex mathematical algorithm, the SHA-2 Security Certificate ensures that web applications can confidently establish their digital identity to browsers used to access them. It is used by a growing number of web applications to establish a secure connection between a web application and a web browser as the predecessor technology, SHA-1 certificates, are being retired.

   For a detailed overview of the Certificate model used by web applications, please see this video: https://www.youtube.com/watch?v=LRMBZhdFjDI

2) **What are the minimum requirements for my systems to be compatible with the new SHA-2 Certificates?**

   The compatibility requirements are outlined in the Encryption Certificate Compatibility Guide: http://bit.ly/1HH0o8w

   While XP/Internet Explorer 8-based systems should be compatible with SHA-2, it is important to note that these systems are no longer supported by Microsoft or PointClickCare. Plans should be made to replace these systems as soon as possible. As of April 2015, testing of PointClickCare on IE8 is very limited. We do not guarantee we can resolve any issues that may be identified by customers who use IE8.

3) **What are the key deadlines I should be aware of?**

   March 2015: PointClickCare began to provide advance warning to partners and customers of the need to migrate to SHA-2 Certificates. Outbound emails were sent to vendor partners, and notice was added to the Customer Facing Roadmap.

Aug 2015: Outbound emails and Home Page Announcements were made to customers providing more details regarding the Encryption Certificate migration plan and timing. Incremental resources, including a compatibility test page (http://browsercheck.pointclickcare.com), were made available to customers to facilitate preparation for the migration.

September 2015: PointClickCare will enable SHA-2 Certificates. All compatible systems will begin to connect to PointClickCare using SHA-2. Most systems incompatible with SHA-2 will continue to be able to connect to PointClickCare using SHA-1 certificates. It is the responsibility of customers to test their systems prior to September using the test page launched in August.

Early 2016: PointClickCare will disable SHA-1 connectivity. By this time, all systems unable to use SHA-2 must be replaced or upgraded. Systems incompatible with SHA-2 will no longer be able to connect to PointClickCare.

4) **What happens if I do nothing?**
While the risk of incompatibility is low, after September 2015 incorrectly configured or incompatible systems may no longer be able to connect to PointClickCare. Once the SHA-1 Certificates are turned off in early 2016, systems incompatible with SHA-2 will no longer be able to connect to PointClickCare.

Users trying to access PointClickCare in either of the above situations will be presented with an error message stating that the system does not support the encryption technology required by PointClickCare.

5) **Why am I starting to get security warnings when I access PointClickCare?**
For users with up-to-date browsers / systems, the migration to SHA-2 Certificates should happen seamlessly in mid-September 2015.

In the meantime, the browser may start to "warn" users about the security of the connection with PointClickCare – since we are continuing to use SHA-1 certificates to validate PointClickCare's digital identity and to encrypt the communications between the web applications servers and the browser. This warning may come in the form of a "pop-up", or, as in the screenshot below, a red stripe across the "HTTPS" at the beginning of the PointClickCare URL in the browser.
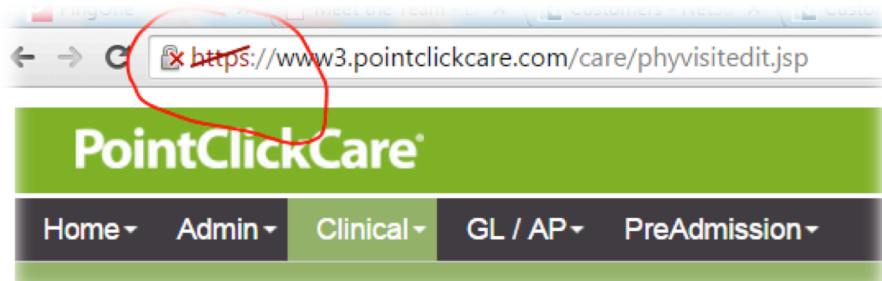
Users need not worry about these warnings, as they will disappear when the migration to SHA-2 certificates has been completed.

6) Why is PointClickCare making me upgrade all my hardware / software / browsers?
The National Institute of Standards and Technology (NIST) in the United States has declared that the commonly used SHA-1 certificates are no longer acceptably secure for use in web applications to establish a secure web application connection. As a result, web application providers as a whole, including PointClickCare, are taking the necessary steps to migrate from SHA-1 certificates to the more secure SHA-2 certificates.

As a responsible partner to our customers, it is important that PointClickCare do all we can to ensure the protection of our customers' data. This includes ensuring we meet the generally accepted security technology standards set by organizations like NIST and the NSA.

In addition to our general and contractual responsibilities to protect residents' and patients' privacy, US healthcare regulations have specific requirements for the protection of Protected Health Information (PHI). As a result, there is a regulatory requirement for PointClickCare to make the migration to SHA-2 certificates.

Systems that are incompatible with SHA-2 are generally no longer supported by their manufacturer (Microsoft, Apple, Google, Mozilla, etc.), nor by PointClickCare. As such, continued use of obsolete systems not only presents a compatibility issue with the new encryption standards, but also an increasingly significant risk to the security and protection of Protected Health Information (also known as Personal Health Information under the laws of certain Canadian provinces). These systems are no longer being patched for security vulnerabilities, leaving them increasingly at risk to malicious attack.

While XP/Internet Explorer 8-based systems should be compatible with SHA-2, it is important to note that these systems are no longer supported by Microsoft or PointClickCare. Plans should be made to replace these systems as soon as

possible. As of April 2015, testing of PointClickCare on IE8 is very limited. We do not guarantee we can resolve any issues that may be identified by customers.

7)   My organization is in Canada, will we be affected?
While US Regulations specifically require the upgrade to SHA-2 security certificates for PointClickCare's US customers, Canadian customers will also be required to upgrade to SHA-2 Security Certificates.

As a responsible partner to our customers, it is important that PointClickCare do all that is necessary to ensure the protection of customers' data in our servers. The general industry consensus is that a migration to SHA-2 certificates is necessary to ensure optimal data security protocols.

Over the next 6-18 months, many technology vendors will end their support of SHA-1 certificates. 3rd party Security Certificate vendors (e.g. Entrust, Geotrust) will no longer issue or renew SHA-1 certificates. Browsers will end their support for SHA-1 certificates over the next 6-18 months, as fewer web application vendors rely on them to establish identity.

As a result, PointClickCare will be migrating all customers on the same timeline.

8)   Is SHA-2 a Canadian regulatory requirement?
The move to SHA-2 is not a specific regulatory requirement for Canadian customers. However, the SHA-1 certificates currently in use will no longer be issued or renewed, and browsers have already begun to warn users about the 'insecure" use of SHA-1 certificates to access sensitive online applications. Canadian customers will be migrated to SHA-2 on the same timeline as US Customers.

9)   Is there a quick way to test if I am prepared for this change?
Yes. PointClickCare has established a test page (http://browsercheck.pointclickcare.com) to quickly check if your Operating System, browser(s) and workstation hardware (computer, kiosk, mobile device) are compatible with SHA-2 certificates. Instructions on how to use this test page are detailed on the page itself.

Note: Facilities with restrictions on internet access (IP-based firewall restrictions) may NOT be able to access the browser test page without changes to their firewall rules. Organizations in this situation can alternatively:
  a.   Temporarily modify their firewall rules to allow access to the test page for the purposes of testing their systems

Wait until September to test systems for SHA-2 compatibility – as the test page will be migrated inside PointClickCare infrastructure at that time.

10) I can't access the browser test page, why? What should I do?

Some PointClickCare customers restrict the ability for their workstations to access the "general internet". Workstations may only be able to access the PointClickCare and related applications.

The browser test page is not currently hosted within the same internet facilities as the PointClickCare application. Therefore, some facilities with restrictions on internet access (IP-based firewall restrictions) may NOT be able to access the browser test page without changes to their firewall rules.

In September, coinciding with the launch of the SHA-2 Certificates, the browser test page will be moved into the PointClickCare infrastructure, making it available to facilities that may initially be having issues accessing it.

Organizations finding themselves unable to access the test page prior to September can alternatively:
a. Temporarily modify their firewall rules to allow access to the test page for the purposes of testing their systems. This is something only a qualified IT staff person should attempt.
b. Wait until September to test systems for SHA-2 compatibility – as the test page will be migrated inside PointClickCare infrastructure at that time.

11) Why is PointClickCare not moving to SHA-2 certificates sooner?

The SHA-1 certificates that PointClickCare uses today are secure. However, it is a best practice to continuously increase the complexity of security encryption protocols and tools. Furthermore, the SHA-1 certificates will, over time, no longer be accepted by browsers as a mechanism for establishing the identity for web-applications.

PointClickCare's timeline for migration to SHA-2 certificates and elimination of SHA-1 certificates was designed to balance customer's time to prepare for this change with the need to continue to maintain a secure environment and stay in compliance with regulations.

12) What is PointClickCare's plan to support me through the migration to SHA-2 certificates?

PointClickCare has prepared a number of self-learning resources to assist customers to test and update (as required) their systems to support SHA-2 prior to the migration. These resources can be found in the following locations:

- Browser Test Page: http://browsercheck.pointclickcare.com
- Resource Page: http://www.pointclickcare.com/ sha-2-encryption-certificate-update-resources/

In addition to these self-learning resources, a dedicated Encryption Certificate Migration Support team has been put in place to assist customers who have technical questions regarding their migration preparation efforts. The Support team can be reached via email at: cuscertupgrade@pointclickcare.com

For those customers who desire more assistance in their migration preparation, PointClickCare has identified a select group of partners who can provide incremental assistance to customers. For details of their services, please see the following links:
- CareServ Technologies - http://www.careservtech.com/point-click-care/
- CareWorx - https://www.careworx.com/partners/pcc-solutions
- Integrated Health Systems http://pcc.ihs911.com/
- Tangent - http://www.tangent.com/long-term-care-solutions/pcc

13) Our facility has PointClickCare integrated to one or more 3rd-party systems. How will the migration to SHA-2 affect them and us?
PointClickCare is working with all of our integration partners to ensure they are prepared for the SHA-2 migration. They are updating their certificate management capabilities to ensure that, by mid-September, there will be no issues in the continued integration of our respective systems. As such, the changeover should be seamless.

For integrations with non-PointClickCare partner systems, you should contact the vendor to confirm they are taking the appropriate action to ensure compatibility of their systems with SHA-2 certificates. If you have any questions regarding these integrations, please contact cuscertupgrade@pointclickcare.com

14) We can't afford this. What financial alternatives exist?
We recognize that making hardware, software and/or IT Services investments can be a costly. It is, however, an essential investment in the protection of Protected Health Information. For organizations that have been continually investing in replacing obsolete technology, any necessary investment to support this change should be minimal.

For organizations that may be facing a larger investment in upgrading out-of-date technology, a select group of PointClickCare partners have been engaged to prepare migration support services and offers to help customers to amortize

the necessary short-term investment over a longer period of time. Please see the partner offers by following the links below:

- CareServ Technologies - http://www.careservtech.com/point-click-care/
- CareWorx - https://www.careworx.com/partners/pcc-solutions
- Integrated Health Systems http://pcc.ihs911.com/
- Tangent - http://www.tangent.com/long-term-care-solutions/pcc

15) Is there an IT Admin "script" I can run to test all my systems centrally?
No. To ensure each workstation (computer, kiosk, mobile device) is compatible with SHA-2 it is recommended each is tested individually. To facilitate testing PointClickCare has provided a "Test Page" that can be accessed by each workstation.

16) Is there an IT Admin "script" I can run to update all my systems centrally?
Depending on the tools and configuration of your IT Infrastructure, centrally upgrading and/or configuring systems could be possible. Developing and executing these "scripts" would be unique to each customers' IT Infrastructure. PointClickCare's capability to support the development and execution of IT Admin scripts is very limited due to the customer-specific nature of such activities.