Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

Feidhmeannacht na Seirbhíse Sláinte
Seirbhís Aisíoca Príomhchúraim
Bealach amach 5 an M50
An Bóthar Thuaidh
Fionnghlas
Baile Átha Cliath 11

Guthán: (01) 864 7100
Facs: (01) 834 3589

Health Service Executive
Primary Care Reimbursement Service
Exit 5, M50
North Road
Finglas
Dublin 11

Tel: (01) 864 7100
Fax: (01) 834 3589

Circular 030/15

18 December 2015

Re: Security Certificates

Dear Doctor,

As you know, access to HSE PCRS GP Application Suite requires the use of a security certificate. Globally, the algorithm which has been used with certificates has been SHA-1 and this is changing to the stronger SHA-2 algorithm before the end of 2016.

We are making arrangements to issue SHA-2 certificates in compliance with this global changeover in the months ahead in advance of the deadline. However, we also plan to take the opportunity to simplify how certificates are used.

You will see the following benefits;

1. A single certificate will be required per device, i.e. Personal Computer or Tablet.
2. A corresponding reduction in the time and support required for certificate renewal.

The reduction in the number of certificates required will be made possible with a standard login to your user account. The purpose of this letter is to give advance notice about the certificate changeover process.

Further information will issue to you when action is required but in the meantime we would welcome your input. Please write to me at ivan.mcconkey@hse.ie with the subject "Security Certificate Project". Your input will be used to assist with the preparation of a comprehensive FAQ for publication at a later date.

We are working towards the following project milestones;

1. Consultation, design and preparation will complete in February 2016
2. User account creation during March 2016

3. Commence issuing of a single SHA-2 certificate per device – April 2016 to June 2016

Please find enclosed an initial frequently asked question section for further information. We look forward to your co-operation with this project and also take the opportunity to offer season's greetings to you and yours.

Yours sincerely,

Ivan McConkey
Director of Information Systems

Appendix A: Frequently Asked Questions

Q1: What is this all about?

Globally, security certificates are being strengthened and this must be completed before the end of 2016. Various advisory notes are available on the subject as follows;

- https://technet.microsoft.com/en-us/library/security/2880823.aspx
- https://googleonlinesecurity.blogspot.ie/2014/09/gradually-sunsetting-sha-1.html

Q2: What do I need to do now?

Nothing immediately. Users of old computing infrastructure, e.g. operating systems such as Windows XP and old browser versions should make plans to support SHA-2 security certificates. At the end of 2016, inability to support SHA-2 certificates may limit or prevent use of the internet altogether for access to many web sites.

Q3: Will all the PCRS issued certificates need to be replaced?

No. Following the changeover project, a single (SHA-2) certificate per device will be required. In fact, a single certificate per "Practice" is feasible for those with the technical knowledge to configure that option, but we propose a certificate per device as the easiest and best configuration for GPs.

Q4: What will happen to the existing PCRS issued certificates on my computer?

These will become less relevant and will stop working or will expire during the course of 2016. However, you will have a new certificate in place before that happens to ensure uninterrupted access.

Q5: Will existing certificates continue to be renewed?

For now, yes. There will be no change until there is further communication. This means that as existing certificates expire these must be renewed to maintain your access to the PCRS GP Application Suite.

Q6: Will the new certificates work on Tablet devices?

Yes. It is planned to support tablet devices with both Android and Apple operating systems.