Headquarters
Executive Office
Gyle Square
1 South Gyle Crescent
EDINBURGH EH12 9EB
Telephone 0131 275 6000
RNID Typetalk 18001 0131 275 6000
Fax 0131 275 7530
www.nhsnss.org

Neil Findlay MSP
Convener of the Health and Sport Committee
T3.60
The Scottish Parliament
Edinburgh
EH99 1SP

Via Email: healthandsport@parliament.uk

Date 30th May 2017
Your Ref
Our Ref CS/sf/2017-05-30

Enquiries to Susan Ferguson
Direct Line 0131 275 7480
Email susan.ferguson4 @nhs.net

Dear Mr Findlay

IT Cyber Attacks

Thank you for your letter of 19th May regarding the recent cyber attack. You asked a number of questions on behalf of the Health and Sport Committee and I have provided answers below:

1. **What impact did the recent cyber-attack have on your organisation and the public?**
   - NHS National Services Scotland was not heavily impacted and we are not aware of any direct impact on the public from the issues we experienced as a Board. The NSS IT organisation was heavily involved in the coordinated NHS wide response to the incident, but the impact on NSS business delivery was minimal. Some of the precautionary measures taken over the weekend of the attack had to be reversed at the start of the new working week, but this amounted to minor inconvenience and no significant impact on service delivery.

     NSS IT are responsible for a number of national level systems only one of which was directly impacted by the attack. This did drive the need to shut down access to core national financial systems into the start of the new working week, but the recovery measures worked as planned and there was no impact from a data integrity perspective. The national data archive for digital imaging (PACS) was taken down as a precautionary measure but was found not to be infected. This necessitated business continuity measures to be put in place for urgent cross Board access to x-rays and scans over the attack weekend with no reported impact on service provision to the public.

2. **Following the cyber-attack how has your approach to prevention of such attacks been revised?**
   - Not significantly – The recommended security best practice measures already in place significantly limited the impact of the attack and the response actions in the immediate aftermath worked as they should. A full analysis of the incident however is still work in progress and the full lessons learned exercise has yet to be completed. We will revise our approach if required at that stage.

3. What additional support would assist in preventing such attacks?

- The range, scale and sophistication of security threats will continue to increase, as will the potential impact of any breach on an NHS which is increasingly dependent on a secure and reliable IT infrastructure. We need to increase our bandwidth in terms of specialist IT roles within NHS Scotland to address the situation before us. This burden could potentially be shared across the whole of the public sector through increased collaboration, but increased spending in this area is inevitable.

4. To what extent do you collaborate with other Boards on IT security issues?

- NSS IT collaborates heavily with other Boards and provides a consulting and coordination role on IT security issues across the NHS in Scotland. We link into Scottish Government and UK level policy on IT security matters, and provide practical guidance and frameworks for the assessment of local measures put in place to mitigate different types of threat. In the event of an incident, we act as a coordinator and clearing house for information sharing and provide central guidance back out to Boards on how best to deal with issues in real time. We link into all the national public sector support available (Cyber Security agencies within Scotland and the UK) and provide coordinated status information back to Boards and into Scottish Government eHealth directorate. We also provide recommendations on recovery and on any changes which need to be made to counter any repeated incidence and ensure delivery of incident reviews and lessons learned exercises. We also link into national level IT service suppliers on security issues and provide contract guidance on security aspects of all major IT purchases across NHS Scotland.

Thank you for the opportunity to respond and please do not hesitate to contact me if you have any further questions.

Yours sincerely

COLIN SINCLAIR
Chief Executive