Dear Mr Findlay,

Thank you for your letter of 19 May 2017 about the cyber-attack which was sent individually to each of us.

In Lanarkshire there was a whole-system response to the cyber-attack. This was successfully managed in a coordinated way across NHS Lanarkshire, South Lanarkshire Health and Social Care Partnership and Health and Social Care North Lanarkshire.

In recognition of this, the following response is a joint submission from the NHS Board and the two Integrated Joint Boards.

1. What impact did the recent cyber-attack have on your organisation and the public?

We assessed the presenting circumstances following the cyber-attack and agreed that the first objective was maintaining patient safety on all care settings in acute and primary care. Plans were made to move to business continuity, including identifying additional staffing needs.

Due to the risk of spread of the ransomware virus through NHS Lanarkshire’s networked systems a decision was taken between the strategic leadership team and senior clinicians to instruct staff to switch off non-essential computers and systems to avoid further propagation. By containing the spread of the malware at this point, we were able to subsequently recover systems and return to business as usual more rapidly.

Despite the challenges presented by the impact on IT systems, staff throughout the organisation showed outstanding commitment to deliver effective and safe care to patients. The eHealth Department worked tirelessly throughout the weekend with clinical teams to restore critical systems and secure the IT infrastructure.

As a result of the actions taken, the cyber-attack caused minimal impact to patient care in Lanarkshire.

Access to all three Lanarkshire emergency departments was maintained throughout the weekend following the attack. We also maintained safe and continued Out-of-Hours (OOH) GP services in consultation with NHS 24 colleagues.

99 per cent of outpatient clinics and planned operations went ahead as normal following the cyber-attack. Any patient procedures or appointments that were postponed were rescheduled as soon as possible.
Some GP systems were also affected as a result of the cyber-attack. NHS Lanarkshire’s staff contacted GP practices over the weekend to ensure their systems were operational and would be available to them on Monday morning. This expedient action identified a few practices with issues that were able to be addressed on the Sunday. Only a few practices had to operate business continuity arrangements on the Monday and all practices were back to full operational capacity by close of business on Tuesday 16 May 2017.

Following the disruption to IT systems due to the ransomware attack, NHS Lanarkshire was unable to process some blood samples for full blood count and B12 and folates that had been sent from GP practices to our laboratories on Friday May 12.

Our laboratory and clinical staff worked through the weekend to restore services and all specimens which had been labelled as urgent were processed.

Laboratory services were at full operational capacity by Wednesday 17 May and patients who required repeat tests to be carried out were contacted directly by their GP.

No patient data was compromised as a result of the attack.

2. Following the cyber-attack how has your approach to prevention of such attacks been revised?

In advance of the completion of the Significant Adverse Events Review, we have:

1. Accelerated the deployment of Microsoft Patches across the ICT Infrastructure.
3. Improved the pro-active monitoring of Threats and Vulnerabilities

Operational units have reviewed Business Continuity Plans to enhance the resilience of systems and services to any similar attacks/loss of electronic systems in the future.

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

1. Investment in improved security tools to prevent and detect threats and to maintain confidence in patching.
2. Additional IT staff resource to improve testing and deployment of security patches including monitoring and detection of threats.
3. Purchase and deploy enhanced endpoint product functionality specifically to address ransomware.
4. Improved training for staff on good practice guidance.
5. ICT security & service continuity training for GP practice managers.
4. To what extent do you collaborate with other Boards on IT security issues?

There is a strong network of IT Security / Information Governance Leads including National Services Scotland (NSS) and Scottish Government eHealth who share information, intelligence and learning about security matters.

NHS Lanarkshire has an IT Security Manager who represents the Board at the National IT Security Officers Forum and also the West of Scotland IT Security Group.

eHealth Leads agree and participate in collective procurements for products where appropriate and this has included security products.

The national eHealth Leads group meets regularly to consider the national shared components of NHS Scotland infrastructure and local common issues where collaboration is appropriate and effective. Our eHealth Lead, Donald Wilson is a member of the eHealth Leads Group.

Security was a substantive item at a recent two-day strategy meeting (April 2017) of the eHealth Leads where the group had useful discussions with NSS Security Lead Colin Howarth. The following was a short summary of the actions agreed reflecting a more joined up approach to sharing good practice as well as reaching economies of scale.

Extract from eHealth Leads Minute (April 2017)

1. **Security Briefing (Colin Howarth)**

   Colin Howarth reported that his presentation would cover the following – current NHSS security position, areas of excellence, developing our information security capability and recommended next steps.

   A discussion took place around these points and the leads made a number of suggestions including,

   - ensuring that third party suppliers who hold our data are part of our agreements,
   - holding a one day training session to share learning on the SANS top 20 controls and to understand the gaps across boards.
   - Discuss further the proposals on managed security services as the complexity is increasing in this area
   - common approach would be beneficial with recommended products.

<table>
<thead>
<tr>
<th>REF.</th>
<th>ACTION</th>
<th>OWNER</th>
</tr>
</thead>
<tbody>
<tr>
<td>240417/19</td>
<td>Pull together a progress report &amp; future plan with the IS officers which includes a Health Board model of security (small, medium &amp; large), convergence roadmap, best practice/tools, recommendations on what can be achieved regionally and nationally and how cloud solutions fit in with the landscape.</td>
<td>CH</td>
</tr>
<tr>
<td>240417/20</td>
<td>Pen Testing – review the schedule/costs for this year as a first step as well as the current products being procured, last year spent and product use; a product matrix/costs to be established.</td>
<td>Regional PM’s</td>
</tr>
<tr>
<td>240417/21</td>
<td>Penni Rocks to liaise with CH regarding attending meetings of the various governance groups.</td>
<td>PR/CH</td>
</tr>
<tr>
<td>240417/22</td>
<td>Provide progress update at the eHealth Leads meeting in July.</td>
<td>CH/CC</td>
</tr>
</tbody>
</table>
The Board’s eHealth Department also works closely with the IT departments of North and South Lanarkshire Councils in relation to the two health and social care partnerships.

I hope this information is helpful in assisting the committee. Please let us know if you require anything further.

Yours sincerely

Val de Souza    Calum Campbell    Janice Hewitt
Director, Health & Social Care    Chief Executive    Chief Accountable Officer
South Lanarkshire H&SCP    NHS Lanarkshire    H&SC North Lanarkshire