NHS Greater Glasgow & Clyde

NHS Board Meeting –

December 2013

Robin Wright, Director of Health Information and Technology

Post incident report on recent ICT Systems Failure

Paper No: 13/58

1. Recommendation:

The Board is asked to note the findings of the post incident review into the recent ICT systems disruption. This report and recommendations have previously been discussed and noted at the November meeting of the Quality and Performance Committee.

2. Purpose of Paper

Further to the incident that resulted in the failure of a significant number of ICT systems during the period 1st and 2nd October 2013, the Board and Scottish Government jointly commissioned an independent review of:

- The technical environment that was in place when the failure occurred
- The response to the incident by ICT staff in the recovering services

The review followed a commitment by the Cabinet Secretary for Health and Wellbeing, to ascertain the 'root cause' of the problem, and to ensure that lessons learned in NHS Greater Glasgow and Clyde are available to be shared with other NHS Boards.

3. Key Issues to be Considered

The independent review was undertaken by industry experts selected by the Chief Information Officer at Scottish Government. The team members were:

Andy McClintock, Chief Technical Officer, Scottish Government,
Charles Batchelor, Director of Service Transformation, Police Scotland,
Neil Logan, Chief Technical Officer, Amor Group (a division of Lockheed Martin), and
Kenneth McLauchlin, Technical Specialist, Police Scotland

The specific terms of reference were to:

Consider the relevant NHSGG&C technical environment and the processes in place to handle incidents of the nature experienced on 1st and 2nd October. In particular, the review team were asked to focus on:

I. NHS Greater Glasgow & Clyde's implementation of 'Active Directory' (the software component that failed) and it's supporting technical environment.
II. The resilience of that technical environment to protect against service interruption.
III. The NHSGG&C ICT team's and suppliers' management of the incident, and the immediate aftermath and subsequent investigation.

4. Findings and recommendations:

The Review Team confirmed and noted the following:

a. the technical environment in NHS Greater Glasgow and Clyde relies heavily upon Active Directory (AD);
b. in the event of catastrophic failure of AD, a substantial service impact across the entire environment is probable;
c. reliance upon AD is commonplace globally. The product is market leading and has demonstrated considerable resilience and stability since its introduction to the marketplace over ten years ago;
d. a number of features built into the product should limit service impact in the event of the catastrophic failure of one or more servers;
e. the root cause of the failure could not at this point be established but ongoing forensic analysis of systems logs was continuing to be undertaken by Microsoft
f. the design and implementation of the NHS Greater Glasgow and Clyde Active Directory is 'fit for purpose' and resilient;
g. Microsoft and Charteris (a certified Microsoft agent) completed an Active Directory Risk and Health Assessment Programme in 2010 and again in May 2013, these set out a number of recommendations that were fully implemented prior to the incident.
    - The 2010 assessment concluded that; '*Overall, the Active Directory infrastructure is well configured and in excellent health, it conforms to Microsoft best practice*"
    - Of particular relevance to this critical incident the review team noted that the May 2013 report stated '*The servers are well configured and in good health*'
h. Microsoft stated that the NHSGGC configuration is consistent with a standard active directory deployment of this size.

Whilst the technical environment was assessed to be in accordance with industry standard best practice, the review team set out a number of areas that would provide additional security to the Board in the event of similar service failure in future:

Recommendation	**Importance**	**Status**
Consider implementation of Specialist 3rd party backup software which augments current facilities and supports full recovery of the AD infrastructure	Recommended	Under-consideration
Microsoft Windows Server native backup solution should be used in addition to any third party backup solutions in use.	Essential	Implemented
Consider implementing Active Directory auditing and configuration change software.	Recommended	Under-consideration
The restoration of backups from the XGGC domain should continue to be regularly tested to ensure full recovery can be achieved.	Essential	In-progress
Oversight of any third party vendor work being undertaken should be given greater attention and a decision log be maintained. This would ensure an audit trail of activities in the event of future failures	Recommended	~~Under-consideration~~Implemented
The immediately availability of spare or redundant hardware would be of assistance to NHS GG&C in the event of similar incident.	Recommended	Implemented
The availability of fuller team resources during an incident such as this could prove to be beneficial to recovery of systems and services.	Recommended	A review of on-call arrangements for ICT staff is underway
Consider the implementation of a Microsoft Premier Support agreement.	Recommended	Completed

5. Next steps

A second phase review and assessment covering all NHS Boards has been undertaken and the report from that will be published at end of December 2013. This was conducted by the National Computing Centre on behalf of Scottish Government, and concentrated on the resilience shown in NHS Greater Glasgow and Clyde (95 % of activity continued to be delivered) and was set up to assess whether :
a) Further improvements are necessary in NHS GGC contingency planning, and
b) Other Boards are equipped to operate to a similar level in the event of failure

Robin Wright
Director – Health Information & Technology
0141 201 4994

8 December 2013