Health and Social Care Integration Directorate
eHealth Division

Scottish Government
Riaghaltas na h-Alba
gov.scot

1 March 2019

Dear Colleagues

Amalgamation of the Information Security Policy Framework and the Scottish Public Sector Cyber Resilience Framework.

- NIS Regulations (NIS)
- Information Security Policy Framework (ISPF)
- Scottish Public Sector Cyber Resilience Framework

We currently have in existence the Information Security Policy Framework 2018 issued by the Scottish Health Competent Authority and the draft Scottish Public Sector Cyber Resilience Framework created by the Scottish Government Cyber Resilience Unit.

The introduction of Network Information Systems Regulation and General Data Protection Regulation (GDPR) in May 2018 placed legal compliance requirements on health boards which necessitated the updating of the existing ISPF to include guidance provided by the National Cyber Security Centre (NCSC) and Information Commissioner's Office (ICO) on the information and cyber security elements of these regulations. The guidance comprised of the Cyber Assessment Framework (CAF) for NIS and the Cyber Security Outcomes for GDPR.

The Scottish Health Competent Authority (CA) incorporated the NCSC and the ICO guidance into the 2018 ISPF as a means to minimise the regulatory burden on health boards and facilitate NIS compliance.

The draft Public Sector Cyber Resilience Framework is the next evolution and effectively incorporates the requirements set out in the ISPF and shall apply to all public sector organisations in Scotland. The Deputy First Minister has recently written to all Scottish public sector organisations, including health boards, seeking views on the draft framework to help strengthen and finalise it.

The long term goal is to incorporate both frameworks into one with the aim of providing a common, effective way for Scottish public sector organisations to assess their cyber resilience and align with key wider cyber-related requirements under

GDPR, NIS and other standards. This will also align health boards with local authorities in both the health and care regimes.

NHS Boards in Scotland are asked to follow the ISPF until further development on the Scottish Public Sector Cyber Resilience Framework (CRF) has completed. We shall, of course provide updates on how this work is progressing.

The compliance assurance audits that will be commissioned by the CA shall be conducted against the ISPF and structured in a manner consistent with the CRF to aid health boards in mapping across over time to the CRF.

We would encourage health boards to provide feedback on the draft Framework to help ensure it is appropriately aligned with your specific interests, and with a view to ensuring that the longer term transition is as smooth as possible.

George Irvine
Information Assurance Manager, Digital Health and Care Division
Directorate for Health and Social Care Integration
T: 0131 244 2258
M: 07580 906669
Tw: @eHealthScotland

Scottish Government
Room BR.12 | St Andrew's House
Regent Road
Edinburgh | EH1 3DG