NHS England

NHS ENGLAND – BOARD PAPER

Title: Lessons learned review of the WannaCry Ransomware Cyber Attack
Lead Director: Will Smart, Chief Information Officer for Health and Social Care
Purpose of Paper: This paper presents to the Board the completed review (Appendix One) by Will Smart, the NHS's Chief Information Officer for Health and Social Care (CIO), of the lessons learned and recommendations following the WannaCry Ransomware Attack that occurred in May 2017.
The Board is invited to note: 1. The content of this paper and CIO review; 2. The 22 recommendations set out in the review.

Lessons learned review of the
WannaCry Ransomware Cyber Attack

Purpose

1. This paper presents to the Board the completed review (Appendix One) by Will Smart, the Chief Information Officer for Health and Social Care (CIO), of the lessons learned and recommendations made following the WannaCry Ransomware Attack that occurred in May 2017.

Background

2. The Department of Health and Social Care's (DHSC) Data Security Leadership Board (DSLB) commissioned the Chief Information Officer (CIO) for the health and social care system in England to carry out a review of May 2017's WannaCry cyber-attack. The objectives of the review were to:

   - Analyse key lessons learned from the WannaCry cyber-attack;
   - Assess actions required to mitigate the risk and impact of a future cyber attack looking in particular at infrastructure, incident response and resilience; and
   - Ensure this learning is shared widely across the health and care system.

3. In reaching its conclusions, the review draws upon:

   - Expert input from members of the review's steering group, which included representatives from the National Cyber Security Centre, Cabinet Office, Department of Health and Social Care, NHS Digital, NHS England, NHS Improvement, Chief Information Officers and Local Government Association.

   - Local lessons learned reports and post incident audits following written communication from the review team to Chief Executives of NHS Trusts and Clinical Commissioning Groups to provide an insight into local responses to the incident.

Progress to date

4. The CIO Review has analysed the lessons learned and the actions taken to date, identifying clear recommendations on further measures that are required to ensure the entire health and social care system is as robust as it can be in reducing the risk and impact of a future cyber attack.

Conclusion

5. The Board is invited to note:
   - The content of this paper and CIO review;
   - The 22 recommendations set out in the review.