Document filename:	**NHS WIFI Policies and Guidance**		
Project / Programme	**NHS Wi-Fi**	Project	**NHS Wi-Fi**
Document Reference	**NWS_WIFI_POLGUID**		
Project Manager	**Andy Smith**	Status	**Approved**
Owner	**David Corbett**	Version	**1.1a**
Author	**Richard Willocks**	Version issue date	**11/07/2017**

NHS WI-FI Technical and Security Policies and Guidelines

Document management

Revision History

Version	Date	Summary of Changes
v0.1		GTS CTS Wi-Fi blueprint as source material
V0.1-7		Misc. updates post internal peer reviews
V0.8	21/11/16	Document restructure post TRG feedback
V0.9	29/11/16	Document content uplifted post TRG CCC leads feedback
V0.10	7/12/16	Document content uplifted post feedback from GDS, Innopsis, HSCN, TechUK
V0.11	14/12/16	Major review post internal review.
V0.12	14/12/16	Moved to NHS Digital Controlled document template.
V0.13	20/12/16	Document content uplifted post additional feedback from NHS Digital Security SME
V1.1	24/3/17	Document uplifted after NHS stakeholder review, including: aesthetic changes, amended requirement for Public and Guest Access, amended requirement for WPA2-Personal/WPA2-PSK, addition of roaming guidance, new reference numbers in Security section, additional legislation and regulation guidance.
V1.1a	11/7/17	Document uplifted to encompass Secondary Care provision and amendment to BPCA008

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version

Approved by

This document must be approved by the following people:

Name	Signature	Title	Date	Version
David Corbett		Programme Director		
Shaun Fletcher		Chief Technical Architect		
Dan Taylor		Head of Information Security		

Glossary of Terms

Term / Abbreviation	What it stands for
2FA	Two-factor authentication

AES	Advanced Encryption Standard
AP	Access Point
AUP	Acceptable Use Policy
BYOD	Bring Your Own Device
CRL	Certificate Revocation List
DNS	Domain Name System
DoS	Denial of Service
EAP	Extensible Authentication Protocol
GDS	Government Digital Services
IP	Internet Protocol
IWF	Internet Watch Foundation
LAN	Local Area Network
MAC	Media Access Control
MU-MIMO	Multi User Multiple Input Multiple Output
OCSP	Online Certificate Status Protocol
PID	Patient Identifiable Information
PKI	Public Key Infrastructure
PSK	Pre-shared Key
RADIUS	Remote Authentication Dial-In User Service
SSID	Service Set Identifier
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
WAN	Wide Area Network
WPA2	Wi-Fi Protected Access 2

Document Control:

The controlled copy of this document is maintained in the NHS Digital corporate network. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Contents

1 Introduction

1.1 Purpose of Document

This document provides a set of policies and guidelines defined by NHS Digital to assist NHS organisations in the delivery and provision of NHS Wi-Fi across the Health and Social Care settings so as to ensure that deployments of NHS Wi-Fi are secure, scalable and where possible consistent.

1.2 Background

The aims of this document are to:

- define a consistent NHS Wi-Fi standard
- make access to NHS Wi-Fi as straightforward as possible
- ensure that the NHS Wi-Fi service is secure
- reduce the costs of procurement and implementation of NHS Wi-Fi
- provide deployment patterns that may be followed when implementing NHS Wi-Fi in local organisations

1.3 Scope

The scope of this document is currently limited to the technical and security implementation of NHS Wi-Fi in Primary and Secondary Care only.

Out of scope are details about NHS Wi-Fi funding arrangements, procurement, service management and business benefits realisation.

1.4 Intended Audience

This is a technical document and should be used by

- IM&T management and staff working in NHS and Social Care organisations intending to procure or upgrade a NHS Wi-Fi network.
- Suppliers of Wi-Fi network products and NHS services to the NHS.

1.5 Definitions and how to use this document

Two key definitions are employed in this document to assist the reader as to how the enclosed content is to be applied.

- **Policies** – these are critical and must be implemented as part of NHS Wi-Fi deployments. Within the policy tables, policies fall into the following category; *Policy* (P)
- **Guidance** – is important and should be considered as part of NHS Wi-Fi deployments. Within the policy tables, guidance falls into the following category; *Guidance* (G)

2 Requirements

2.1 Industry Standards

Reference	Classification	Requirement	Rationale
IS001	P	IEEE 802.11x standards	These are the fundamental network standards that provide high-throughput Wireless LAN services
IS002	P	WPA2-Enterprise/WPA2-802.1x	This is the industry standard method for providing secure Wi-Fi
IS003	P	WPA2-Personal/WPA2-PSK	This is a recognised industry standard for providing basic Wi-Fi encryption, normally employed in residential or small business installs. In the context of NHS Wi-Fi, this basic form of encryption should only be employed after a full risk assessment of the proposed environment has been conducted.

2.2 Government Guidance

Reference	Classification	Requirement	Rationale
GG001	G	Government Digital Service Technology Code of Practice & Service Device Manual	This guidance is seen as the UK Government best practice for the deployment of Wireless networks

2.3 NHS Standards

Reference	Classification	Requirement	Rationale
NS001	P	Information Governance (IG) Toolkit	The IG Toolkit draws together the legal rules and central guidance set out by DH policy and presents them in in a single standard as a set of information governance requirements.

2.4 Network Access Profiles and Authentication

Reference	Classification	Requirement	Rationale
NAPA001	P	Identify the appropriate user classes to be adopted for the environment.	Not all Wi-Fi user classes will apply to every environment e.g. Patient/Citizen Wi-Fi access would not be required in a

Reference	Classification	Requirement	Rationale
			location where physical access by the public is restricted.
NAPA002	P	Define appropriate network access profiles for the various user classes	To support the implementation of the various levels of authentication required by the individual user classes identified.
NAPA003	P	Map network profiles to Standard Service Set Identifiers.	To support the logical separation of traffic across the various user classes
NAPA004	P	User class – Corporate	An employee of the organisation who has been identified as requiring access to the corporate network using a corporate device. The level of access requires an assured level of service availability and also a level of security to support the transmission of patient-identifiable information (PID). This user class should also be considered for the support of members of regional NHS Wi-Fi initiatives where participating organisations may require roaming users to have access into a specific, private extension of the base-location WAN.
NAPA005	P	User class - Guest	An employee of the organisation using a personal device or an individual who is visiting the organisation or site in a business capacity and has demonstrated a valid requirement for access. The user requires basic access to Internet services whilst needing to maintain a level of security, reliability and guarantee of service over and above that provided through Public access. This user class should also be considered for members of regional NHS Wi-Fi initiatives where participating organisations may require authentication and Internet access that supports VPN.

Reference	Classification	Requirement	Rationale
NAPA006	P	User class – Patient[1], Citizen (Public)	A member of the public. The user requires basic access to Internet services.
NAPA007	P	Medical Device	Wi-Fi enabled medical devices and appliances deployed within the corporate network environment. The level of access requires an assured level of service availability and also a level of security to support the transmission of patient-identifiable information

2.5 Standard Service Set Identifier (SSID)

Reference	Classification	Requirement	Rationale
SSID001	P	Utilise a common set of SSIDs	The implementation of a central service to support authentication across a group of participating organisations, sites, buildings or even departments provides the ability for users to roam between locations whilst maintaining the perception of a single wireless network
SSID002	P	Advertise Patient/Citizen Wi-Fi access using the nationally agreed SSID of: NHS Wi-Fi	This will provide a common, branded and trusted method for members of the public to access NHS Wi-Fi across the NHS estate, whilst providing a suitable platform to support any national roaming initiatives for the public across the NHS in the future.
SSID003	P	For Corporate and Guest SSIDs, any organisations and/or sites participating in a regional Wi-Fi initiative to locally agree and adopt a standardised SSID naming convention for the user classes supported	To easily identify suitable Wi-Fi networks that may be available to join, and to support regional roaming
SSID004	P	Connect Wi-Fi enabled medical devices to a separate, dedicated SSID and where the practicalities of usage allow, logically separate the traffic and hide the SSID from the general Corporate access.	To support the security, integrity and confidentiality of Wi-Fi enabled medical devices
SSID005	G	Consider, as part of the Wi-Fi service procurement, the requirement to	To enable the support of established Wi-Fi roaming

[1] The availability and access to NHS Wi-Fi for patients should be considered in the context of the local care setting and the needs of the patient e.g. Mental Health setting where it might be necessary to restrict or prevent patient access.

Reference	Classification	Requirement	Rationale
		support SSIDs relating to established cross-government and educational roaming initiatives	initiatives through the local configuration of defined SSIDs e.g. GovWiFi, Govroam, eduroam
SSID006	G	Keep the number of SSIDs broadcast to an efficient number.	Ensure the Wi-Fi performance is not degraded due to an unnecessary number of SSIDs generating broadcast traffic

2.6 Security

Reference	Classification	Requirement	Rationale
S001	P	Where the requirement exists to support the secure transmission of Patient Identifiable Information (PID), access is secured, at a minimum, to WPA2-Enterprise.[2]	WPA2-Enterprise is the industry standard method for providing secure Wi-Fi
S002	P	Protect access to all network infrastructure management interfaces either directly or indirectly using two-factor authentication (2FA)	To mitigate the risk of a stolen password compromising the security of the entire organisation
S003	P	Employ techniques to isolate Wi-Fi clients from one another[3] and document any exceptions where P2P connectivity is to be supported.	To prevent a compromised device attacking others on the same network
S004	P	Ensure all local network infrastructure and gateways are secured and risk assessed.	Assurance of local network infrastructure and gateways to identify and mitigate any risks to the corporate domain. IG Toolkit
S005	P	If Pre-Shared Key (PSK) is employed, ensure it is not advertised openly and a robust process is established to support its distribution	To assist with ensuring access to the service is restricted to verified and legitimate users only.
S006	P	Ensure the PSK is changed frequently	To assist with ensuring access to the service is restricted to verified and legitimate users only.
S007	G	CareCERT subscription	To keep appraised of emerging threats to wireless networks in order to implement appropriate

2 https://nww.carecertisp.hscic.gov.uk/display/CC/Local+Area+Network+%28LAN%29+Security?preview=/4032010/4032008/Local%20Area%20Network%20Security%20GPG%20v2.0.pdf

3 https://nww.carecertisp.hscic.gov.uk/display/CC/Firewall+Technologies?preview=/4032003/4032002/Firewall%20Technologies%20GPG%20v%202.0.pdf

Reference	Classification	Requirement	Rationale
			mitigations
S008	G	Consider, in line with the scale of the deployment, employing periodic Wi-Fi specific IT Health Check / penetration testing to identify vulnerabilities and rogue Access Points	To mitigate the risks posed by rogue Access Points that can be used to exploit the security, confidentiality and integrity of networks
S009	G	Ensure the privacy rights, security and traceability of all users of the service is considered[4]	IG Toolkit Legislation compliance e.g. • Data Protection act, European Directive for Data Retention Regulations 2009 • Anti-Terrorism, Crime and Security Act 2001 • Regulation of Investigatory Powers Act 2000 • Digital Economy Act 2010 • Privacy and Electronic Communications (EC Directive) Regulations 2003
S010	G	Ensure the auditability of the solution is considered[4]	IG Toolkit Legislation compliance e.g. • Data Protection act, European Directive for Data Retention Regulations 2009 • Anti-Terrorism, Crime and Security Act 2001 • Regulation of Investigatory Powers Act 2000 • Digital Economy Act 2010
S011	G	Consider implementing location based restrictions to services e.g. geofencing tools	To restrict access to back-end systems from specific locations e.g. medical devices, clinical systems.

4 https://nww.carecertisp.hscic.gov.uk/display/CC/Local+Area+Network+%28LAN%29+Security?preview=/4032010/4032008/Local%20Area%20Network%20Security%20GPG%20v2.0.pdf

2.7 Access

Reference	Classification	Requirement	Rationale
A001	P	Minimise the intervention required by Patient/Citizen users trying to gain Wi-Fi access e.g. clear signage supporting the enrolment process and helpdesk, automated enrolment	To ensure the user enrolment and registration process is as effective and as simple as possible, and that any staff management overhead is minimised.
A002	P	Facilitate access to the Patient/Citizen Wi-Fi service through the standard NHS Wi-Fi landing pages defined by NHS Digital.	To support an effective and standardised user enrolment and registration process.
A003	P	Assess the suitability and associated security risks of implementing a landing page to support Guest access	A genuine and legitimate landing page/captive portal can be copied by a hacker and used to establish a rogue captive portal to harvest information from unsuspecting users devices as they connect.
A004	P	NOT facilitate access to the Corporate / privileged network through a landing page	Landing page/captive portals are unnecessary for corporate/ privileged access and present security risks.
A005	P	Clearly communicate to the user on enrolment whether the Wi-Fi service is secured or unsecured and its suitability to support the transfer of personal/sensitive information. WPA2-Enterprise is classified as secure Wi-Fi. Standard Public Wi-Fi networks are normally unencrypted and classified as unsecure.	To ensure the user is fully aware of the level of security the service provides and to allow them to make an informed decision on the risks associated with using the service to transfer personal/sensitive information. To minimise the risk of unsecure networks being used, inadvertently or otherwise, by Corporate users for business sensitive activity.
A006	P	Provide an acceptable use policy (AUP) for all users and user classes, preferably as part of the enrolment process.	Ensure that all Wi-Fi users have signed an AUP and are aware of the terms and conditions of the respective service. Note that Corporate users may already be suitably covered by an existing LAN/WAN AUP
A007	P	If non-anonymised data is captured and persisted, obtain user consent through an AUP or individual agreement	Conformance with data protection legislation
A008	P	Ensure that logging and auditing of Wi-Fi network use is in line with the organisation security policy and legal requirements	Conformance with organisation requirements and relevant legislation.

Reference	Classification	Requirement	Rationale
A009	P	NOT allow Guest or Patient/Citizen access to internal or privileged networks	To ensure the security of the Corporate network is maintained
A010	G	Employ techniques to restrict access to unsecure networks from Corporate devices	To minimise the risk of unsecure networks being used, inadvertently or otherwise, by Corporate users for business sensitive activity.

2.8 Corporate Access

Reference	Classification	Requirement	Rationale
CA001	P	Provide Corporate NHS Wi-Fi using WPA2-Enterprise/WPA2-802.1x as a minimum	This is the industry standard protocol for providing secure Wi-Fi
CA002	G	Consider certificate-based authentication as the preferred authentication method to support Corporate access.	Certificate-based authentication is considered to be the simplest, safest and most robust authentication method within WPA2-Enterprise, as it removes the reliance and overhead of username/password management, and provides a seamless, faster authentication process
CA003	G	Consider password-based authentication where: Corporate devices do not support certificates A risk assessment of adopting a non-certificate-based approach has been completed	Whilst recognising certificate-based authentication being the preferred method, it is acknowledged that a password-based method can provide a cost-effective and secure approach to employing WPA2-Enterprise where the estate has not widely adopted the use of certificate-based authentication.
CA004	G	Password Strength	Follow the NHS password policy guidance that will ensure that passwords are secure and not easily broken.

2.9 Guest Access

Reference	Classification	Requirement	Rationale
GA001	G	Consider providing Guest NHS Wi-Fi using WPA2-Enterprise/WPA2-802.1x	This is the industry standard protocol for providing secure Wi-Fi
GA002	P	Employ password-based authentication as the minimum authentication method to support Guest access over WPA2-	In most cases Guest access will be from non-corporate devices managed outside the corporate domain, therefore

Reference	Classification	Requirement	Rationale
		Enterprise/WPA2-802.1x.	making password-based authentication the most practical option.
GA003	G	Assess the suitability of employing an unencrypted, unsecure service as a cost effective alternative.	Where the level of security, reliability and guarantee of service required for Guest access is not considered essential and can be clearly communicated to the user, an unencrypted, unsecure service may provide a cost effective solution.

2.10 Public Access

Reference	Classification	Requirement	Rationale
PA001	P	Ensure Public NHS Wi-Fi access includes a robust enrolment and registration process using valid credentials.	To control access to the service and to assist with the traceability and validity of users of the Wi-Fi service.
PA004	G	Consider the opportunities and benefits, balanced against the level of complexity and cost, of providing a WPA2-Enterprise based solution	Local opportunities / arrangements where management and cost overheads can be minimised may allow for the availability of secure Wi-Fi for public use.

2.11 Network Separation

Reference	Classification	Requirement	Rationale
NS001	P	Ensure mechanisms are in place to isolate wireless Wi-Fi traffic by either of the following: SSID certificate authority, identified by a device certificate	To maintain differentiation of the Wi-Fi services being offered by an organisation. Higher levels of service and security policies can then be mapped to individual SSIDs
NS002	P	Provide a mechanism for separating Wi-Fi network traffic belonging to particular user classes using one of the following methods: connecting to separate virtual local area networks (VLANs) at the Wi-Fi access point (AP) or separating traffic at a central point like a wireless controller	To maintain differentiation of the Wi-Fi services being offered by an organisation. Higher levels of service and security policies can then be mapped to individual SSIDs and VLANs

Reference	Classification	Requirement	Rationale
NS003	P	Employ virtual routing and forwarding (VRF) technologies to maintain separation across layer 3 infrastructure e.g. VRF-lite	To maintain differentiation of the Wi-Fi services being offered by an organisation. Higher levels of service and security policies can then be mapped to individual VRFs
NS004	P	Employ separate IP addressing[5], routing and access controls for each Wi-Fi network	To support differentiation of the Wi-Fi services being offered by an organisation.
NS005	P	IP addressing requirements are be considered in terms of: the demand for connectivity and number addresses required the frequency and transience of users and the appropriate DHCP lease/expiry times of allocated addresses	To ensure the service is scaled in terms of the number of IP addresses that are required to support the connecting users, and the period of time connectivity is required.

2.12 Bandwidth Provision and Content Access

Reference	Classification	Requirement	Rationale
BPCA001	P	Internet Connectivity	Ensure Internet connectivity is available to support content access requirements of the relevant user classes of the service
BPCA002	P	Ensure internet traffic filtering is enabled	To minimise the availability through the Wi-Fi service of potentially criminal Internet content, specifically images of child sexual abuse (including child pornography) hosted anywhere, and criminally obscene adult content in the UK and to minimise the risk of organisational reputational damage.
BPCA003	P	Internet Watch Foundation	THE IWF creates and maintains filters that stop user access to illegal sites.
BPCA004	P	Filtering policy is regularly reviewed	To ensure that the agreed internet filtering policy is maintained and that meets the regulatory and organisations standards while assessing new content such as:

[5] Ensure compliance with the latest NHS Digital IP Addressing guidance

Reference	Classification	Requirement	Rationale
			• guns and weapons • gambling • pornography • anonymiser/proxy sites
BPCA005	P	NOT direct public Internet traffic through any centrally provisioned Internet gateway that has been procured exclusively for NHS business purposes.	To prevent the contravention of existing arrangements supporting any services specified and procured exclusively for NHS business purposes
BPCA006	P	Ensure capacity planning and management includes all application group and user class bandwidth requirements and user volumes e.g. dedicated medical devices, patient/citizen access to steaming services etc.	To ensure a reliable and consistent service is maintained for all user classes
BPCA007	P	Ensure that the underlying network infrastructure supporting the Wi-Fi service, is scaled to meet the anticipated user volumes and bandwidth requirements	To ensure a reliable and consistent service to the relevant user classes
BPCA008	P	Avoid blocking access to high bandwidth applications, in preference to managing bandwidth effectively e.g. QoS This should be considered in line with the scale of the deployment where a high demand for Public access is anticipated, e.g. large campus site, and the most cost effective method of offering services over and above basic Internet browsing.	This allows for a wide variety of media rich applications e.g. streaming media and helps to avoid employing complex systems and policies to curb user requirements
BPCA009	G	Consider the most cost effective way to maintain and improve user experience at a site	To ensure the user experience is maintained to an acceptable level through the most cost effective means possible. For example: • transparent caching technologies to minimize the impact of software updates • employing bandwidth management technologies to prioritise and protect specific user classes and services e.g. QoS • upgrading bandwidth using commodity internet services

Reference	Classification	Requirement	Rationale
			• employing techniques to minimize the opportunities for piggybacking • contingency planning for both anticipated and unexpected periods of high utilisation

2.13 Administration and Monitoring

Reference	Classification	Requirement	Rationale
AM001	P	Provide remote monitoring to manage usage and support of the service e.g. usage reporting, alerting to potential attacks or where radio quality is compromised for a significant period etc.	To support proactive and dynamic support to the service.
AM002	G	Consider, in line with the scale of the deployment, using tools that show both current and historical network activity.	Combined with building floor plans and access point locations this can provide a visual insight into coverage and use of the service across large or distributed sites and can assist in planning.
AM003	G	Consider, in line with the scale of the deployment and the business need, using location data to support business operations e.g. real time people/equipment/resource finder, queue length reporting, hot desk/meeting room usage etc.	To leverage improvements to and support existing business operations.

2.14 Roaming

Reference	Classification	Requirement	Rationale
R001	P	NOT develop a national roaming solution.	Discussions are underway with Cabinet Office regarding the development of a coordinated strategy that will take into consideration existing and developing initiatives to support pan-government roaming. Further information will be shared by the NHS Wi-Fi Programme as and when it becomes available.
R002	G	For regional roaming initiatives, participating organisations should agree the scope of services and service levels to be supported.	To ensure a common, minimum set of standardised services are available across the consortium.

Reference	Classification	Requirement	Rationale
		The two main service types seen in operation today are: Standard Internet Roaming (SIR) - enables the roaming user to gain easy access to the Internet to launch a corporate VPN and gain access to resources on the internet. Advanced Private Roaming (APR) - enables the roaming user to access their own private network from the roaming location.	
R004	P	For regional roaming initiatives, a standardised approach for authentication should be adopted across all participating organisations.	To ensure a common, dynamic and transparent approach to authentication.
R005	P	For regional roaming initiatives, the 'home' organisation remains primary authenticator for the roaming user.	To support effective management of roaming users e.g. revoke, approve access

3 References and Further Reading

The document is based on existing content generated and released by Government Digital Services (GDS) in the GDS Technology Code of Practice & Service Design Manual.

Sharing workplace wireless networks https://www.gov.uk/guidance/sharing-workplace-wireless-networks

GCHQ - Cyber Essentials & WiFi Architecture Pattern

Wi-Fi Alliance - http://www.wi-fi.org/

Internet Watch Foundation (IWF) – https://www.iwf.org.uk/

Information Governance (IG) Toolkit - https://www.igt.hscic.gov.uk/