Requirements for a Digital Future Care Plan Service for Wales

Items highlighted in yellow require clarification with NWIS regarding interoperability with NHS Wales

Introduction

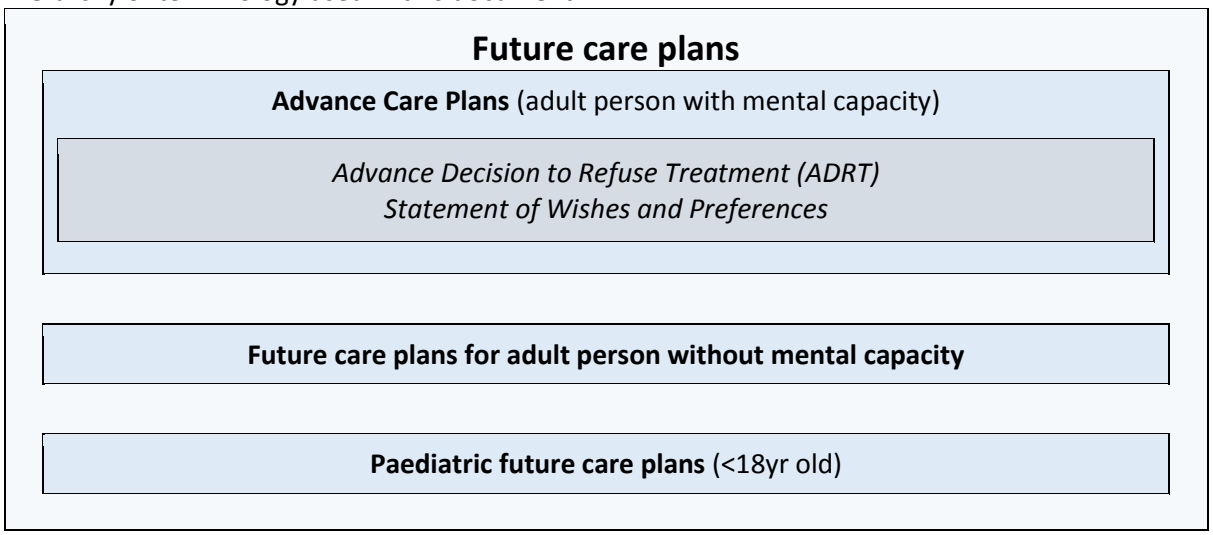
Purpose of document

The purpose of this document is to specify the requirements for a digital future care plan service for Wales.

Note on Terminology

The term *Advance Care Planning* has been defined as referring solely to individuals with decisional capacity [1]. This document therefore uses the term *Future Care Plans* as an inclusive term, to include: care plans for adult individuals who lack mental capacity, paediatric care plans which may apply to children with or without some decisional capacity, and *Advance Care Plans* for people with mental capacity.

Hierarchy of terminology used in this document:



Environment

The IT solution will be expected to interact with other IT systems in Wales:

	Usual patient record IT system
NHS Secondary care & Non-NHS Hospices	WCP (Welsh Clinical Portal) - NWIS
A&E departments	[Various bespoke systems]
Primary care	Vision Microtest
GP Out of hours	Adastra
WAST (Welsh Ambulance service)	C3
NHS 111	Capita

Requirements

Overview

The IT solution should:

- enable an e-Form (electronic record) to record future care plan information

- enable paper or electronic future care plans to be uploaded and attached to the record as scanned or electronic documents
- enable wishes/plans about CPR to be recorded as part of the record
- enable direct access by patients to write and submit their own advance care plan

It should also:

- require explicit consent from the patient (or equivalent permission by those making a best interests decision) for the record to be shared
- be readily accessible to all healthcare professionals (who have valid clinical reason), in a timely manner, and in all relevant settings across Wales
- take account of developments across the UK with a view to facilitating transfer of information from ACP records across the border to and from England

1. The supplier shall provide an overview of their proposed digital future care plan service.
2. The service must be live in a healthcare environment. The supplier shall identify a minimum of one such environment where their service has been implemented, describe the scope of the implementation in terms of care settings and organisations and state the date since the service has been live.
3. The supplier shall provide information on the number of participating organisations, users and future care plans created in a period in the identified healthcare environment where their service has been implemented.
4. The supplier shall identify a minimum of 2 referees from the identified healthcare environment where their service has been implemented. For each referee the supplier must provide name, role, organisation and address, email address and telephone number.
5. The supplier shall identify and describe the key benefits realised by their service in the identified healthcare environment where their service has been implemented.
6. The supplier shall provide any evidence such as publications and reports to support each the key benefits that they have identified and described.
7. The supplier shall describe how their service supports collaborative, multidisciplinary digital future care planning and communication, and their approach to clinical transformation.
8. The supplier shall describe how their service and future care plans are connected digitally to all urgent care services including NHS 111, ambulance services, out of hours (OOH) GP services and A&E departments.

Service Overview

9. The service must be available 24 hours per day, 7 day per week.
10. The service must be underpinned by a scalable, web-based IT solution. The supplier shall provide an overview of their IT solution.
11. The supplier's proposed solution must enable patients to access their future care plans.
12. The supplier's proposed solution must enable care providers to access future care plans on mobile devices, including smart phones.
13. The supplier shall identify clearly any limitations on the use of their proposed IT solution, including any limitations on the numbers of organisations and end users accessing the system and the numbers of care plans supported.

14. The service must include a robust information governance model. The supplier shall provide an overview of their approach to information governance, particularly the sharing of patient data across multiple care settings, organisations and care professionals and must set out if third party providers will have any access to such data
15. The service must include future care plan clinical quality management. The supplier shall describe their approach to clinical quality management.
16. The service must include information reporting. The supplier shall describe their approach to information reporting.
17. The service must include end user training in both the end user IT application and clinical aspects of care, including consent and having difficult conversations with patients. The supplier shall describe their approach to training.

IT Solution Features

User Interface

18. The IT solution must support the different views of the future care plan required by different user groups, for example the creators and the (urgent care) consumers of care plans.
19. The IT solution user interface must be highly intuitive. Use of the system must require virtually no formal training to use.
20. User mouse clicks required to complete any tasks must be minimal.

Patient Consent

21. The supplier shall describe their patient consent model for the creation of a future care plan.
    - The consent model should clearly distinguish: adult patients with capacity, adult patients without capacity, and those under 18 years old.
    - The model should record explicit consent to share the plan, informed by an understanding of the implications of sharing, and supported by a national information leaflet.
    - Mental capacity (or the lack of capacity) to make the decisions included in the care plan should be recorded by the clinician user
22. The supplier shall explain how the system supports the principles of best interests decision making (Mental Capacity Act 2005), when recording a plan made on behalf of an adult without capacity.
23. The IT solution must not enable a future care plan to be created until consent is recorded.

Personal Demographics Service

24. The IT solution must be linked to the NHS Wales Personal Demographics Service (PDS).
25. The supplier shall describe the IT solution link to the PDS and how it is used when a future care plan is both created and updated.
26. All future care plans must include the patient's NHS Number and their registered GP practice.
27. The IT solution must not allow the creation of patient records with duplicate NHS Numbers. The supplier shall describe how this is achieved.

Legitimate Relationships

28. The supplier shall describe how end user legitimate relationships with patients are managed.

Future Care Plan Creation and Updating

29. The IT solution must be compliant with NHS Electronic Palliative Care Coordination System (EPaCCS) requirements (systems and Information Governance (IG)).
30. The IT solution must also comply with NHS Digital's information standard SCCI1580 (formerly ISB1580), which specifies the core content to be held in an EPaCCS.
31. The supplier must provide a list of their future care plan data set.
    In addition to the core content of SCCI1580, the data set should include:

    - A record of mental capacity (or equivalent for paediatric document)
    - Date of mental capacity assessment (Future care plan for adult without capacity – only)
    - Details of who the care plan has been discussed with
    - For attached documents:
        - Date of document – date when the original (paper) document was written or signed
        - Location of original paper document e.g. in patient's house

32. The IT solution must guide users through care plan creation and update in a logical manner.
33. The IT solution must include best practice validation, must highlight incomplete mandatory fields, and must include context help text.
34. All system screens in the IT solution must display the current logged in user and their associated organisation, and a patient banner identifying the currently selected patient.
35. The patient banner must also display alert icons, which should include Do Not Resuscitate Orders, Advance Decisions to Refuse Treatment, and patient allergies.
36. The IT solution must enable users to create and update care plans both in one go and by saving changes to resume and finalise later.
37. The IT solution must include a postcode look up for patient and patient contact address look up.
38. The IT solution must enable users to upload and attach documents to future care plans.
39. The supplier should describe how versioning will be handled of multiple attached documents, in order to allow more than one document to co-exist (e.g. DNACPR form and LPA document) whilst avoiding the risk of superseded documents remaining on the system when out of date.
40. The solution must enable documents attached to future care plans to be viewed, printed and also removed.
41. The IT solution must enable administrative staff creating or updating a care plan on a clinician's behalf to submit the care plan for clinician approval before it can be published and made available to urgent care. This should include attaching documents.
42. The IT solution must enable administrative users to make changes to patient demographic and contact information without the need for clinical approval.
43. The IT solution must enable clinician users to create and update care plans and approve them, making them accessible by urgent care.
44. The IT solution shall record and display the name, NADEX ID, and role of the last clinician user to have created, approved or updated the record.

45. The IT solution must enable a review date (which may be optional) to be set when a future care plan is approved.
46. The IT solution must enable clinician users to re-approve (revalidate) plans at any time.
47. The IT solution must provide a way of monitoring and managing future care plan statuses and associated user tasks, for example care plans waiting to be finalised, clinically approved or reviewed. The supplier shall describe their approach to such care plan status and associated task management.
48. The supplier shall describe how their approach to care plan status and associated task management includes an escalation process to mitigate those tasks not actioned in a timely manner.
49. The IT solution must enable future care plans to be printed. The supplier shall describe the care plan print process and any restrictions.
    - Copies of a future/advance care plan that are printed on paper from the record (including any attached documents), should be marked on each page with the date of printing, and contain a warning for the clinician to ensure this is the latest version
    - When future care plans are printed, they must include: patient details (name, DOB, NHS No, address), metadata (date of creation, name of authorising clinician etc.), consent statements, and date of approval.
    - If printing a record with status of Pending Approval, watermarks on every page should clearly indicate the status of the document.
50. The IT solution must enable Do Not Attempt Cardiopulmonary Resuscitation (DNACPR) form (consistent with the All-Wales DNACPR form) to be printed. The supplier shall describe the DNACPR form print process and any restrictions.

Patient Lists

51. The IT solution must enable end users to create and use interactive patient lists to manage their patients, for example during multidisciplinary team (MDT) meetings.
52. The supplier shall identify the selection criteria that are available to end users in order to create such lists. This should include lists of all patients with future care plans:
    - pending approval by the current user.
    - pending approval by anyone in a specified GP practice
    - who are registered with a specified GP practice – indicating date when last approved.
    - approved by the current user – indicating date when last approved

Urgent Care View

53. The IT solution must ensure that when urgent care users access a patient's future care plan they are presented with a summary view of information that will be important to them. The supplier shall describe their approach to urgent care viewing of care plans.
54. The IT solution must enable urgent care users to drill down from the summary view into the detailed information held in the care plan quickly and easily.
55. The IT solution must enable urgent care user accesses to a care plan to create a history of urgent care access in the care plan itself, viewable as part of the care plan.

56. The IT solution must enable urgent care users accessing a patient's care plan to record brief details of the patient encounter along with the access history event.

Recording Patient Death

57. The IT solution must enable users to record patient death, including the actual place of death and the reason for any variance between it and the patient's preferred place of death.
58. The IT solution must ensure that deceased patient records are no longer accessible by urgent care users.
59. The IT solution must enable system administrator users to remove a record of patient death recorded in error.

Withdrawing Consent

60. The IT solution must enable clinician users to record the withdrawal of patient consent.
61. Withdrawal of patient consent must remove the patient's future care plan from the IT solution, such that it can no longer be accessed by any system user.
62. If a patient who has withdrawn their consent subsequently decides that they would like a future care plan, the IT solution must enable a new care plan to be created for them.

Care Plan Deletion

63. The IT solution must enable a future care plan to be deleted permanently. A description of the deletion and what was deleted must, however, remain , so that future governance, legal and complaints processes can obtain such data at a future date, where it is needed as evidence (see Audit Data)

Subscription

64. The IT solution must enable users to subscribe to receive automatic notifications of individual patient's future care plan events, e.g. access by urgent care users, recording death.
65. The IT solution must enable users to subscribe to future care plan events for individual patients and groups of patients.
66. The IT solution must enable users to unsubscribe to future care plan events for individual patients and groups of patients.
67. The supplier shall describe their subscription functionality and identify the future care plan events that are supported.

Patient Portal

68. The IT solution must include a patient portal, which will enable patients to initiate their own future care plans and view and request changes to their clinically approved care plans.
69. The patient portal must be available in both English and Welsh language.
70. The IT solution must enable clinicians to enrol individual patients in the patient portal. The supplier shall describe the enrolment process for patients.
71. The supplier shall describe the patient portal functionality that enables a patient to view their future care plan and any limitations on the care plan details that the patient can see.
72. The supplier shall describe the patient portal functionality that enables a patient to request changes to their future care plan and any limitations on the care plan details that the patient can request changes to.

73. The supplier shall describe how patient requested changes to their care plan are incorporated in their clinically approved plan.
74. The patient portal must enable patients to initiate their own future care plans. The supplier shall describe the patient portal functionality that enables patients to initiate their own care plans and how their care plan becomes clinically approved.
75. The IT solution should enable the patient's GP to be alerted whenever a new plan is submitted by a patient.
76. The supplier shall identify any differences in the patient portal functionality that is available to patients and to their proxies.

Mobile Device Support

77. The IT solution must be technology independent and function fully in a "bring your own device" environment.
78. The IT solution must operate on mobile devices with intelligent rendering of the user interface.
79. The supplier must identify any technology limitations associated with their IT solution, including browsers and devices.

User Access and Login

80. Users must be able to access the IT solution via both NHS Wales and non-NHS networks.
81. The IT solution must implement two factor authentication for non-NHS access. The supplier shall describe their approach to the authentication of access to the IT solution via non-NHS networks.
82. The IT solution must require users to have a valid user accounts with a username and password.
83. The supplier shall describe how the user account shall be synchronised with the NADEX database.
84. The supplier's IT solution must support multiple user roles and associated role based access control (RBAC).
85. The IT solution must enable the same user and user account to be linked to different roles at different organisations, e.g. GP practice and out of hours GP services.
86. The IT solution must support a single sign on facility for users who regularly access the system from their usual operational system in the context of the currently selected patient record.
87. The IT solution must force individual users to agree to an Acceptable Use Policy (AUP) the first time that they login under an individual organisation.
88. The IT solution must be configurable to enable users to reconfirm the AUP at regular intervals.
89. The IT solution must enable the AUP to be updated.
90. The IT solution must be configurable to force all users to reconfirm their AUP, for example following an update to the AUP.

Interoperability

91. The IT solution must be capable of linking to third party systems to enable third party systems of urgent care users to be alerted to the existence of a future care plan in real time.

92. The IT solution must support a click through link from third party systems, in the system user and selected patient context.
93. The supplier shall describe their approach to this third party system patient flagging, and describe any implementation already in place.
    - 3rd party systems used by urgent care users: Welsh Clinical Portal (secondary NHS care and non-NHS hospices), various A&E departmental systems, Vision and Microtest (GP systems), Adastra (OOH GP service), C3 (Welsh Ambulance service), and Capita (NHS 111).
    - Most systems will use the patient's NHS number to identify the correct record.
    - The current system used in WAST (C3) will need to match the caller's address.
    - The current system used in NHS 111 (Capita) will need to match the caller's demographics taken by the call-handler (e.g. name, address, and date of birth).
94. The IT solution must be capable of linking to third party systems to enable creation, updating, approval and cancellation of future care plans.
95. The IT solution must support a click through link from third party systems, in the system user and selected patient context.
96. The IT solution must be capable of linking to third party systems to enable third party systems users to be alerted to the existence of a future care plan which is awaiting approval, when in selected patient context.
97. The IT solution should enable the patient's GP to be alerted whenever a new plan is approved in any setting other than primary care.
98. The supplier shall describe their approach to this linking, and describe any implementation already in place.
    - The 3rd party systems which will be used to access the IT solution for creation, updating etc. of care plans: Welsh Clinical Portal (secondary NHS care and non-NHS hospices), Vision and Microtest (GP systems).

Audit Data

99. The IT solution must maintain a complete audit log of all system events.
100. The audit events logged must include the transaction type, the transaction data and time, the user and associated organisation and the associated data.
101. The IT solution must make some audit data available to end users, for example who last clinically approved a care plan. The supplier shall describe what audit data is available to end users.

Clinical Leadership

102. The service must be clinically led. The supplier shall identify their clinical lead and summarise their role and associated qualifications.
103. The supplier shall provide an organisation chart, identifying key roles and numbers of resources and flagging those key roles held by experienced clinicians.
104. The service must facilitate and action service user feedback. The supplier shall describe the process and any supporting governance structures that facilitate service user feedback and continuous service improvement, for example stakeholder and patient groups.

Information Governance

105. The supplier shall provide a detailed description of their approach to information governance.
106. The supplier shall describe their approach to managing and controlling organisation and individual access to their service, including their supporting IT solution.
107. The supplier shall describe their approach to organisation Information Sharing.
108. The suppler shall describe their approach to individual Acceptable Use.
109. The supplier shall describe their approach to end user training requirements.

Training

110. The supplier shall provide training services for the duration of the contract.
111. The service must provide end user training. The supplier shall describe their training strategy.
112. The supplier shall describe their training approach, including whether training is available in multiple formats, such as online eLearning modules, face to face and remotely via WebEx.
113. The supplier shall identify any limitations on the training it will provide, for example number of sessions, trainees etc.

System Administration

114. The supplier shall provide system administration and configuration as part of the service.
115. The supplier shall manage all system configuration and reference files / dropdown lists centrally.
116. Where appropriate reference file / dropdown list values must be mapped to equivalent SNOMED CT values.
117. The supplier service must include the creation and maintenance of organisations, individuals, users and their inter-relationships.
118. Where appropriate organisations and individuals must be sourced from NHS Digital Organisation Data Service (ODS) files, e.g. GP practices, GPs, acute trusts, consultants.
119. The IT solution ODS files must be updated at least quarterly.
120. The supplier service must enable regional inter-organisation relationships to be created and maintained, for example the health boards, GP practices, 111 services, OOH GP services, ambulance services, nursing homes and hospices where patients' collaborative urgent care plans are shared in a region.

Data Retention & Destruction

121. The IT solution must support patient record retention and destruction policies and processes. The supplier must describe their patient record retention and destruction policies and processes.
122. Patient record retention and destruction policies and processes must be implemented in line with NHS best practice and the Data Protection Act.

Information Reporting

123. The supplier shall provide a comprehensive set of information reports as part of the service.
124. The supplier shall list the standard reports available. These shall include the following standard reports:

- Number of FCPs currently active (patient alive) – by Health Board, GP, and GP practice
- Number of FCPs added in the last period – by Health Board, GP, and GP practice
- Number of FCPs pending approval for more than 1 month – by Health Board, GP, and GP practice
- Number of FCPs last approved more than 6 months / 1 year ago – by Health Board, GP, and GP practice

125. The supplier shall provide ad hoc information reporting as part of the service. The supplier shall describe any limitation on the ad hoc information reporting provided.

Quality Assurance

126. The supplier shall provide a regular review of the quality of urgent care plans created and provide feedback to organisations to encourage a continuous improvement cycle as part of the service.
127. The supplier shall describe their data quality review and feedback service.

Clinical Safety

128. Clinical risk management must be embedded in the supplier's end to end service.
129. The IT solution must comply fully with Clinical Risk Management standard SCCI0129 as applied to the manufacture of health IT systems.

Help Desk

130. The supplier shall provide an appropriately skilled and experienced Help Desk that is available inside office hours Monday to Friday 09:00 to 17:00, excluding bank holidays as part of the service.
131. The supplier shall provide a password reset service and the ability to report severity level 1 issues outside office hours of Monday to Friday 09:00 to 17:00, and including bank holidays as part of the service.

Managed Service

132. The supplier shall provide a fully hosted managed service.
133. The supplier's service management shall conform to best practice as defined in ITIL (IT Infrastructure Library) and comply with the ISO20000, ISO27001 (Information Security Management Systems: Requirements) and ISO27002 (Code of Practice for Information Security Management) standards.
134. The supplier's service shall provide proactive service monitoring, including interactive service availability, interface availability, normal completion of scheduled processing, successful processing of incoming and outgoing interoperability messages, appropriate transmission and logging of outgoing email and attempted security breaches. Service monitoring must be used to drive timely intervention to prevent interruption to service.
135. The supplier shall carry out all maintenance activities in pre-agreed maintenance windows.
136. The supplier shall describe the technical architecture of the IT solution.

Service Level Agreement

137. The IT solution performance must be as follows: 80% of transactions will complete within 2 seconds, 90% of transactions will complete within 3 seconds and 99% of transactions will complete within 5 seconds. Initial login will take less than 5 seconds.
138. The IT solution availability must be as follows: the system will be available 99.90% of the time, excluding planned outages.
139. The supplier shall propose incident severity response and resolution times and update frequencies.
140. The IT solution RPO and RTO must be as follows: the system will adhere to a Recovery Point Objective (RPO) of 5 minutes data loss for live SQL and unstructured data and 15 minutes data loss for all remaining production servers and a 4 hour live environment Recovery Time Objective (RTO).

Implementation Services

In addition to training services to be available for the duration of the contract:

Project Management

141. Implementation of the service must include project management services.
142. The supplier shall describe their approach to project management and the proposed service, including any project management methodology used.
143. The supplier shall provide a proposed project plan for the implementation of the digital future care plan as part of this submission.
144. The suppliers proposed project plan shall clearly identify actions and tasks to be undertaken by the supplier and the purchaser.
145. The supplier shall provide an initial risks and issues log, including proposed mitigations for the implementation of the digital future care plan as part of this submission.

[1] Rietjens J, et al White Paper: Definition and recommendations for advance care planning. An international consensus supported by the European Association for Palliative Care. The Lancet Oncology, Volume 18, Issue 9,2017, pp e543-e551,ISSN 1470-2045, https://doi.org/10.1016/S1470-2045(17)30582-X.