# Diabetes Prevention Programme

# Information Governance and Data Flows Framework

NHS England and NHS Improvement

# Diabetes Prevention Programme
# Information Governance and Data Flows

Version number: 3.8

First published: May 2016

Updated: August 2019

Prepared by: NHS England Diabetes Programme Team and Data Sharing and Privacy Unit, NHS England & NHS Improvement

Publishing Approval Reference: 000899

# Contents

# 1 Executive summary

The NHS Diabetes Prevention Programme (NHS DPP) was announced in the NHS Five Year Forward View, published in October 2014, which set out our ambition to become the first country to implement at scale a national evidence-based diabetes prevention programme modelled on proven UK and international models, and linked where appropriate to the new NHS Health Check.

The purpose of this guidance is to support organisations participating in the NHS DPP in meeting their legal and contractual requirements relating to information governance. The main focus is to ensure that information flows are documented and established on a lawful basis.

# 2 Background

The NHS DPP is a joint initiative led by NHS England, Public Health England (PHE) and Diabetes UK, together the "National Programme Team". The programme delivers services to people with non-diabetic hyperglycaemia, who are at high risk of developing Type 2 diabetes, which are designed to lower their risk of onset of Type 2 diabetes.

Provision of the intervention in local geographies will be called off from the national framework according to local need and requirements. The costs of the intervention are met centrally by NHS England who are the contracting authority for the intervention.

GP practices and external NHS Health Check providers will be responsible for identifying at risk individuals and referring them to the provider of the intervention who will have responsibility for arranging attendance on the intervention.

# 3 Context

## 3.1 Purpose

The purpose of this guidance is to support organisations participating in the Diabetes Prevention Programme in meeting their legal and contractual requirements relating to information governance. It describes the responsibilities of respective organisations at each stage in the pathway, with a view to ensuring that:

- the use of patient data is lawful;
- that patients are appropriately informed about the use of their data;
- that the rights of individuals with regard to the use of their confidential information are respected.

The information in this guidance will be of use to those conducting privacy impact assessments of local implementations. Organisations participating in the NHS DPP should conduct data protection impact assessments (DPIAs), to assess the level of risk and the likelihood and severity of any impact of the processing on individuals.

## 3.2 Scope

It is for the individual organisations which comprise each local pathway to determine that their particular data flows are compliant with the relevant law, including the GDPR. This guidance is not designed to provide legal advice on the steps that should be taken to achieve such compliance, but is supporting guidance on matters which should be taken into account when assessing how to meet the requirements of the duty of confidentiality and the requirement under the GDPR to process personal data fairly, lawfully and in a transparent manner. Whilst the need for secure information management is referenced, details of specific security measures are only provided for contracted data flows.

The guidance describes the data flows required to support the NHS DPP and considerations for local health economies in designing the local pathway for the service. It covers:

- identifying and inviting at risk individuals
- key data flows between Primary Care and non- GP NHS Health Check providers to the providers of the behavioural intervention
- the collection and storage of data during the intervention
- the transfer of data from providers of behavioural intervention back to primary care
- the transfer of data from the provider to the commissioning authority.

The aim of the paper is to:

- describe the roles and responsibilities of different actors in the pathway with regards to the collection / processing and sharing of data, to support them in respecting the rights of individuals with regard to the use and disclosure of their personal confidential data and provide some guidance as to the relevant legal considerations (although it is for each individual actor to determine their legal compliance).

## 3.3 Audience

The audience for this guidance includes GP practices and organisations that refer into the NHS DPP, providers contracted to deliver the Programme, NHS England as the commissioner and partners including local authorities and Public Health England.

## 3.4 Definitions

Some key terms are set out in Appendix 1.

The word **must** is used in this document to identify a legal requirement.

The word **should** is used to indicate that, in particular circumstances, there may exist valid reasons to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

The word **may** is used to indicate a truly optional activity. This includes decisions where a permissive legal power is available.

# 4 Legal and contractual requirements

NHS England is required by the NHS Act 2006 to publish guidance for professionals and organisations registered with the Care Quality Commission (CQC) on the processing of patient information. [1] This guidance fulfils this obligation in relation to the processing of information in the context of the NHS DPP. In accordance with the 2006 Act, CQC registered professionals and organisations must have regard to this guidance when offering such services.

NHS DPP provider organisations are contracted to NHS England under the Standard NHS Contract. This requires that specified information governance requirements are met and in particular, comply with the relevant annual Data Security and Protection Toolkit (DSP Toolkit) across all its requirements. The DSP toolkit will require organisations to demonstrate that they are complying with the ten data security principles recommended by the National Data Guardian.

Providers, referring organisations and commissioners must ensure that patients' privacy and confidentiality are respected, and that information is shared lawfully. The organisations that deliver the NHS DPP are data controllers as defined in the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) and must comply with the Principles and other requirements of the GDPR and Data Protection Act 2018 (the DPA 2018).

Where a GP practice or provider, as a data controller, engages a data processor to process personal data on its behalf, a binding written data processing contract must be in place which, amongst other things, ensures that those processing the data are subject to a duty of confidence and requires the data processor to keep information secure and only act under the written instructions of the data controller.

This document provides guidance on how to meet the requirements of the duty of confidentiality and the requirement under the GDPR to process personal data fairly and lawfully, complementing contractual requirements, with reference to the flows of information that are required to support the Programme.

Please see appendix 2 for further information on legal and contractual requirements.

# 5 Options for referral

[1] NHS Act 2006 s. 13S, inserted by the Health and Social Care Act 2012 s. 23(1)

## 5.1 Referral routes

The referral pathway at annex A outlines the 3 main referral routes in to the NHS DPP following the identification of eligible individuals as follows:

1. Eligibility is identified by the patient's GP, following a GP NHS Health Check or opportunistic detection by a GP;
2. Eligibility is identified by a healthcare professional, following an alternative provider NHS Health Check, or diabetes risk assessment;
3. Eligibility is identified by the patient's GP following identification by the GP of existing cases of NDH on GP register (known eligible individuals).

Once eligible individuals have been identified they should be offered a referral into the NHS DPP by their GP or alternative NHS Health Check provider. The referring GP or alternative provider is required by the GDPR to explain to the individual how their data will be used at the point it is collected from them – i.e. before referring them. The process for how individuals are referred to the programme is for local determination and will require dialogue with providers. The contract sets out the expectation that it is the responsibility of the behavioural intervention provider to arrange attendance and provide further information to patients (fair processing) for those individuals that have been referred. It is for individual GPs to determine whether the personal data which needs to be transferred as part of that referral is done on the basis of having obtained specific consent from each individual patient, or whether they are satisfied that the 'public task' and 'healthcare' conditions (Articles 6(e) and 9(h) respectively) for processing under GDPR apply such that consent is not required.

## 5.2 Referral following NHS Health Check or Opportunistic Identification

Where eligibility for the NHS DPP is established as part of the NHS Health Check performed by a GP or alternative provider, or as part of opportunistic detection (routes 1 or 2 above), a referral may be made with the consent of the patient, provided that sufficient information has been provided to the patient, which may include:

1. general information about the NHS DPP:
    a. its purpose
    b. who provides the service
    c. benefits and risks to the individual
2. What information will be disclosed to and used by the provider
3. The lawful basis relied on for the processing under the GDPR
4. That information about the treatment received will be sent:
    a. back to the GP to update practice records
    b. to the commissioner of the programme for payment and quality assurance

Under the GDPR GPs or alternative providers are also required to provide patients with other information regarding the processing of their data (as set out in Articles 13 and 14 of the GDPR). This list assumes that that the other information has been provided by way of a fair processing notice; Appendix 4 contains a template fair processing notice, but it is for individual GPs to determine whether the information outlined above and that set out in the template provides the patient with sufficient information to discharge their obligations of transparency under the GDPR.

The referral, with accompanying information (see section 6.1), must be communicated securely to the behavioural intervention provider.

## 5.3 Identification of existing cases of NDH on GP register (known eligible individuals)

In route 3 queries are run on the registers held on practice systems to identify individuals that have blood glucose readings within the parameters that would indicate non-diabetic hyperglycaemia. This query creates a list of eligible patients and their contact details, which are then used to invite them to consent to referral into the Programme.

The Programme has developed a set of business rules to support case finding and developing registers of at risk individuals, this rule set includes relevant exclusions. This can be found in appendix 5.

There are two principal options for identification of eligible patients, which both have different information governance considerations. They are as follows:

**Option 1: GP practice undertakes identification**

Where the selection of eligible patients is carried out by GP practice staff, on practice systems entirely within the GP practice environment, this is considered to be direct care. NHS Digital Guidance *"A guide to confidentiality in health and social care: references"* provides that healthcare professionals may review patient records to establish a cohort of individuals who might then by invited to receive a particular type of intervention on the basis of implied consent, as it is considered to be direct care.

Practices must ensure the confidentiality and security of this data as part of their General Medical Services (GMS) contract, and in accordance with the GDPR / DPA 2018 and common law duty of confidentiality.

**Option 2: Using a data processor to identify the eligible population**

GP practices may choose not to manage the selection process themselves and contract the work out. In this option the selection of eligible patients is performed by a data processor acting under the specific instructions of the GP practice as data controller (for example a CCG, CSU or private company), using a query on the GP practice system to generate the lists of eligible individuals from the practice register. Patients would likely need to be informed by GPs in their fair processing notices that

the GP may use the services of a data processor (with GPs determining the extent to which this is necessary). Appendix 4 contains a template fair processing notice. Under the GDPR a binding written data processing contract must be in place which, amongst other things, ensures that those processing the data are subject to a duty of confidence and requires the data processor to keep information secure and only act under the written instructions of the data controller. It is for GPs to ensure that such an agreement is in place if they are going to engage a data processor to process data on their behalf. GPs will also have to consider whether they have a valid legal basis to transfer each patient's personal data to a data processor before doing so.

## 5.4 Referral of identified eligible individuals

Where eligibility has been established using existing registers then the GP practice must ensure that the referral process complies with the GDPR and does not breach confidentiality. Again, there are two main options to achieve this which have different issues to consider (as follows).

**Option 1: GP sends referral letter**

Where the invitation for referral is sent by the GP practice, under the GDPR, this is likely to be 'fair' because the purpose will be transparent (see below), in accordance with the patient's reasonable expectations and is unlikely to result in detriment. GPs may be able to rely on the public task lawful basis for processing if they consider that it is necessary for the public task of providing healthcare services. It may also fulfil one of the conditions of processing special category data if it is considered necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality. It may also not be a breach of confidentiality as patients' can be contacted by their GP for direct care purposes. However, these are all matters which only individual GPs can determine for themselves and this is offered as guidance, only, as to some of the legal considerations relevant to this particular option.

**Option 2: GP using a data processor to invite patients**

A GP practice may choose to commission a data processor to generate the invitations for referral. Where this is the case a binding written data processing contract must be in place (a legal requirement of the GDPR) which, amongst other things, ensures that those processing the data are subject to a duty of confidence and requires the data processor to keep information secure and only act under the written instructions of the data controller. This is a standard form NHS data processing contract and does not include any requirements specific to the NHS DPP that GP practices or providers may wish to include. GPs must determine for themselves that there is a legally complaint data processing contract in place before transferring personal data to a data processor.

The GP may wish to stipulate that the initial referral offer is in the form of a letter addressed from the GP practice. The letter may be generated by a data processor commissioned by the GP practice, but in doing so would need to use the practice letterhead if this is the preferred model.

GPs would need to consider whether they have a valid legal basis before sending out invitations for referrals for patients.

GPs may also wish to consider whether patients who have previously been invited for referral to the programme but have opted out should be sent another invitation for referral to the programme.

Whether the letter is generated via option 1 or 2, the GP may wish to consider including the following details in the letter. It is not designed to be an exhaustive list of everything which must be included to ensure legal compliance, as this is something which can only be determined by individual GPs. It is designed to be illustrative, only:

1. why the GP is writing to the patient – the invitation to participate in the programme
2. what the patient needs to do either to accept or decline the invitation
3. the role of the GP Practice in the Programme, and as the organisation responsible for the patient's personal data
4. general information about the NHS DPP:
    a. its purpose
    b. who provides the service
    c. benefits and risks to the individual
5. What information will be disclosed to and used by the provider
6. The lawful basis relied on for the processing under the GDPR
7. That information about the treatment received will be sent:
    a. back to the GP to update practice records
    b. to the commissioner of the programme for payment and quality assurance
8. information about any follow-up communications by or on behalf of the practice (e.g. by phone) that might happen to pursue the invitation
9. contact details for the GP practice, or if applicable data processor, to enable patients to ask questions and accept or decline the invitation.

Under the GDPR GPs or alternative providers are also required to provide patients with other information regarding the processing of their data (set out in Articles 13 and 14 of the GDPR). This list assumes that that the other information has been provided by way of a fair processing notice; Appendix 4 contains a template fair processing notice, but GPs must assess for themselves whether sufficient information has been provided to the patient in order to satisfy their obligations of transparency under the GDPR.

Once a patient has contacted the practice (or if applicable the data processor acting for the practice) and has agreed to the referral to the programme, the GP should consider sending a referral to the provider of the intervention so that attendance at an initial session can be arranged. The GP should record on the individual patient's clinical record that they have consented to being referred to NHS DPP.

# 6 Information requirements

## 6.1 Information supporting referral to the provider

The referral notification should contain the following information:

1. Date of Referral
2. General Medical Practice Code (Patient Registration)
3. NHS Health Check Provider Code (where relevant)
4. NHS Number of individual referred
5. Name of individual referred
6. Address of individual referred
7. Telephone number / E-mail address (where known)
8. Contact details (telephone number / e-mail address) of carer or representative (if appropriate)
9. LATEST HbA1c / FPG (including date recorded)
10. If individual is on the SMI register (where recorded)
11. Whether the individual has a learning disability
12. whether the individual has a physical disability / mobility issue
13. Where requirement for a translator or information in another language would be supportive (where known)

Once a patient has agreed to the referral the GP or other alternative provider may supply the information outlined above directly to the intervention provider.

## 6.2 Data to be collected during intervention

The Provider is required by the Contract to capture data relating to individuals that enter on to the programme. This includes socio-demographic information as well as records of attendance and outcomes achieved during the intervention.

The socio-demographic information includes the following fields: *ethnicity; religion; employment status; sexual orientation; housing tenure; disability status*. Patients' wishes not to provide socio-demographic information must be respected and recorded with the appropriate "not stated" or "declines to disclose" code.

The data to be collected are specified in Schedule 6 of the Contract.

The provider is also required to ask patients if they consent to be contacted by nationally appointed researchers undertaking evaluation of the NHS DPP to obtain their opinions. The outcome of this must be recorded in the field that maps to DPP38 in the Data Output Specification.

## 6.3 Data to be sent back to primary care

The intervention providers will provide the data identified below back to primary care. This is to enable GPs to update their records and inform ongoing future decisions about their patients' care. The notification back to primary care should include the information in the table below. The provider must ensure that patients are informed about the information that will be returned to their GP. Appendix 4 includes suggested text for inclusion in a NHS DPP provider's fair processing notice.

| Data Item | Relevant Clinical Code | | | Definition | Timing |
|---|---|---|---|---|---|
| | V2 | V3 | SNOMED CT | | |
| **General Medical Practice Code (Patient Registration)** | N/A | N/A | N/A | ORGANISATION CODE of the GP Practice that the PATIENT is registered with – See data format and codes | On notification of attendance / non-completion / completion |
| **NHS Number of individual** | N/A | N/A | N/A | The primary identifier of a PERSON, is a unique identifier for a PATIENT within the NHS in England and Wales | On notification of attendance / non-completion / completion |
| **Family name of individual** | N/A | N/A | N/A | | On notification of attendance / non- |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | completion / completion |
| **Given Name of individual** | N/A | N/A | N/A | This is the name recorded on a birth certificate. | On notification of attendance / non-completion / completion |
| **Address of individual** | N/A | N/A | N/A | | On notification of attendance / non-completion / completion |
| **Postcode of individual** | N/A | N/A | N/A | | On notification of attendance / non-completion / completion |
| **Attended NHS DPP** | 679m2 NHS Diabetes Prevention Programme started | XaeD0 NHS Diabetes Prevention Programme started | 1025271000000103 National Health Service Diabetes Prevention Programme started (situation) | Relevant where the individual attended the initial assessment session | |
| **NHS DPP not completed** | 679m0 National Health Service Diabetes Prevention Programme not completed | XaeCw NHS Diabetes Prevention Programme not completed | 1025211000000108 National Health Service Diabetes Prevention Programme not completed (situation) | Relevant where the individual has completed < 60% of the recommended dose | When it is established the individual will not continue with |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | the programme |
| **Completed NHS DPP** | 679m1 NHS Diabetes Prevention Programme completed | XaeCz NHS Diabetes Prevention Programme completed | 1025251000000107 National Health Service Diabetes Prevention Programme completed (situation) | Relevant where the individual has completed >60% of the recommended dose | At completion of programme |
| **Weight** | Value | Value | Value | | |
| **Date of weight measurement** | N/A | N/A | N/A | | |
| **Date of blood result** | N/A | N/A | N/A | | |

## 6.4 Commissioning datasets

The provider must submit the datasets specified in Schedule 6 of the Contract Particulars to the specified Data Services for Commissioners Regional Office of the NHS Digital. The legal basis for this submission is established by Directions issued by NHS England to NHS Digital.

Where a patient has not consented to be contacted for evaluation purposes – i.e. DPP38 is not 'Y' – the patient's contact details recorded in fields DPP6 to DPP11 must not be included in the dataset.

# 7 Data Protection Impact Assessments

The GDPR imposes an obligation to carry out a Data Protection Impact Assessment ("DPIA") where, in particular, using new technologies and where data processing is likely to result in a high risk to freedoms and privacy, and also where there is new or amended uses of personal data.

The DPIA must contain:

- A description of the processing which that technology will perform, and its purposes;
- An assessment of the necessity and proportionality of the processing operations in relation to those purposes;
- An assessment of the risks to the rights and freedoms of any potentially affected individuals; and
- The measures envisaged to address those risks, including any safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR.

A DPIA can only be conducted by those organisations proposing to implement the new technology where data processing is likely to result in a high risk to freedoms and privacy or involving new or amended uses of personal data. It is for local organisations to determine whether a DPIA is required, and if so what it should address.

# Appendix 1 – Definitions

| | |
|---|---|
| Consent | *"any freely given, specific, unambiguous and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed"*[2]<br><br>Consent is the approval or agreement for something to happen after consideration. For consent to be legally valid, the individual must be informed, must have the capacity to make the decision in question and must give consent voluntarily. This means individuals should know and understand how their information is to be used and shared (there should be 'no surprises') and they should understand the implications of their decision, particularly where refusing to allow information to be shared is likely to affect the care they receive. This applies to both explicit and implied consent.[3] Consent cannot be assumed by giving the data subject an opportunity to opt out; if using tick boxes to obtain consent, it must be a specific 'opt in' box which the patient is invited to tick if they do indeed consent. |
| Data controller | the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. |
| Data processor | A natural or legal person, public authority agency or other body which processes personal data on behalf of a data controller, who retains full responsibility for compliance with the GDPR. |
| Explicit consent | Explicit consent is unmistakeable. It can be given in writing or verbally (but must be evidenced, for instance by contemporaneous notes of what was said), or conveyed through another form of communication such as signing. A patient may have capacity to give consent, but may not be able to write or speak. Explicit consent is required when sharing information with staff who are not part of the team caring for the individual. It may also be required for a use other than that for which the information was originally collected, or when sharing is not related to an individual's direct health and social care. |
| Implied consent | Implied consent is applicable only within the context of direct care of individuals. It refers to instances where the consent of the individual patient can be implied without having to make any positive action, such as giving their verbal agreement for a specific aspect of sharing information to proceed. Examples of |

[2] European Directive 95/46/EC
[3] Information: To share or not to share? The information Governance Review
https://www.gov.uk/government/publications/the-information-governance-review

| | |
|---|---|
| | the use of implied consent include doctors and nurses sharing personal confidential data during handovers without asking for the patient's consent.<br><br>However, if a patient makes an explicit consent decision, for example requesting that their personal confidential data is not shared (or 'actively dissenting' to share), this decision replaces any implied consent and their decision should be respected. |
| Personal data | Personal data is defined by the GDPR as<br>Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.<br><br>The definition includes data held in electronic form, structured manual files, and for health records, any other form. |

# Appendix 2 – Legal and contractual requirements

This section highlights some of the legal and contractual considerations for GPs and providers in their delivery of the NHS DPP.

## The common law duty of confidence

The common law duty of confidence requires that where there is an established expectation of confidentiality between parties, for example a health professional and a patient, information imparted by the subject will not be further disclosed by the recipient without the consent of the subject. The duty is not absolute and information may be disclosed without consent where it is required or permitted by law, or in exceptional circumstances where the public interest outweighs the individual's right to confidentiality. This can, however, only be considered depending on the individual circumstances of each case, and so GPs would need to take their own view after weighing up all the relevant factors.

## The General Data Protection Regulation (GDPR)

GP practices, providers and commissioners are data controllers under the GDPR in respect of the data which they hold about their patients. As such, they must comply with the six principles and other requirements of the GDPR in their use and disclosure of information. Data controllers must be registered with the Information Commissioner's Office.

GP practices, commissioners and providers, for the purposes of providing the DPP, are public authorities and therefore must designate a Data Protection Officer; a person with expert knowledge of data protection law who is expected to monitor compliance with the GDPR (although responsibility for compliance remains with the GP).

To meet the First Principle of the GDPR, data controllers are required to process personal data fairly, lawfully and transparently. The common law duty of confidence and other relevant laws must be respected. Further conditions are specified, including for the use and disclosure of "special categories of personal data".

Data controllers are required to provide data subjects with information about the collection and use of their personal data. This is a key transparency requirement under the GDPR. This is usually in the form of a 'fair processing notice' or 'privacy notice' that identifies the data controller, the uses and disclosures of personal data, contact details of the data controller and other relevant information.

The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used. These should include business processes, operational procedures and provisions for staff training and awareness.

Where an organisation makes use of a data processor, under the GDPR it remains liable for their compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected. To meet this responsibility, there must be a written contractual arrangement in place that provides details of:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subject; and
- the obligations and rights of the controller.

The data processing contract must include the following terms:

- the processor must only act on the written instructions of the controller (unless required by law to act without such instructions);
- the processor must ensure that people processing the data are subject to a duty of confidence;
- the processor must take appropriate measures to ensure the security of processing
- the processor must only engage a sub-processor with the prior consent of the data controller and a written contract;
- the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- the processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;

- the processor must delete or return all personal data to the controller as requested at the end of the contract; and
- the processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their own obligations under the GDPR as data processor, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

## The NHS Standard Contract

General Condition 21 (GC21) in the NHS Standard Contract[4] sets out the information governance requirements that a Provider must comply with. Providers must complete and publish an annual information governance assessment and must demonstrate satisfactory compliance as defined in the NHS Information Governance Toolkit (or any successor framework), as applicable to the Services and the Provider's organisation type.

## The General Medical Services Contract

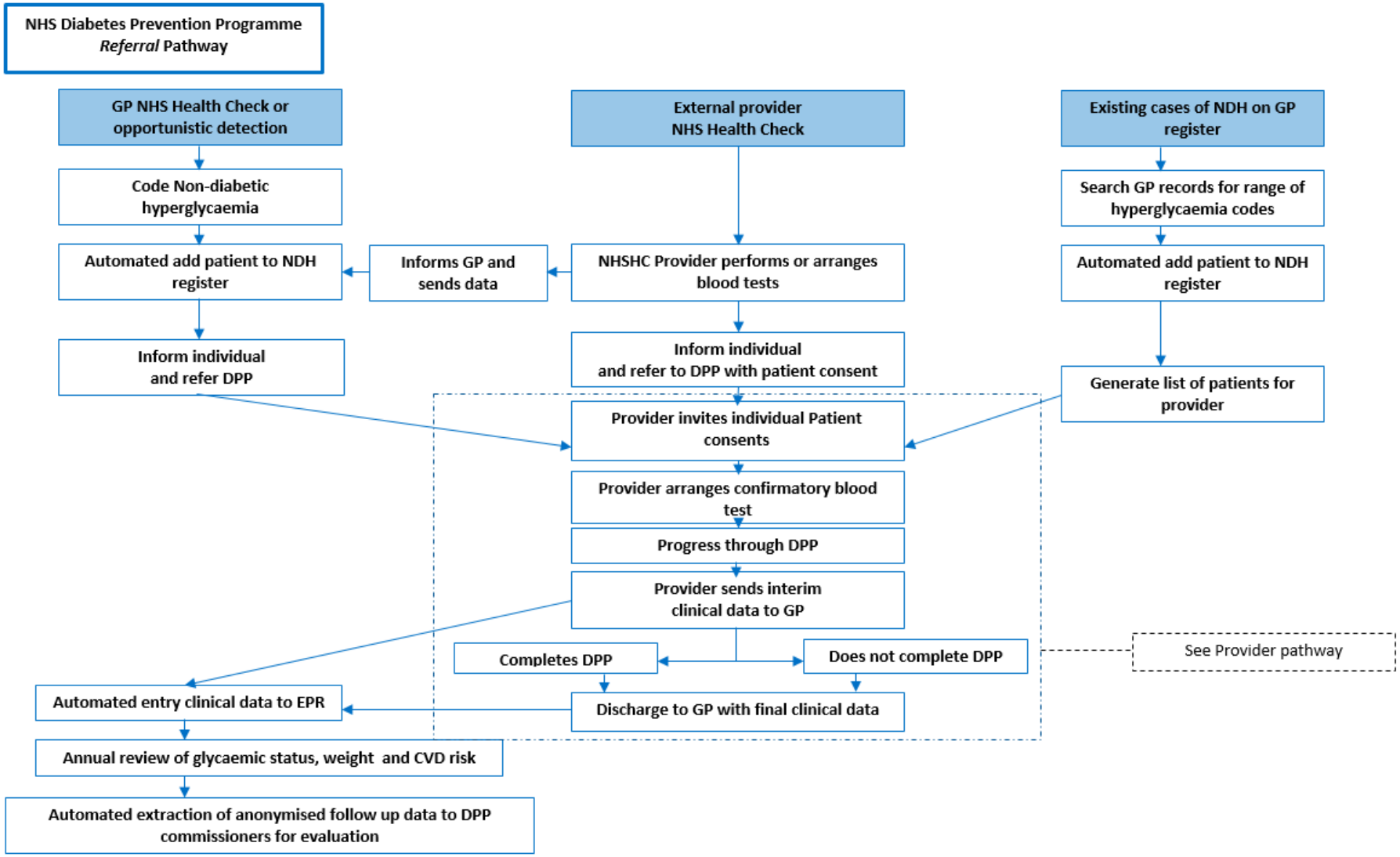
GPs are required under their contract[5] to comply with all relevant legislation and also to have regard to the *Good Practice Guidelines for General Practice Electronic Records*[6]. They are also required to nominate a person with responsibility for practices and procedures relating to the confidentiality of the personal data they hold.

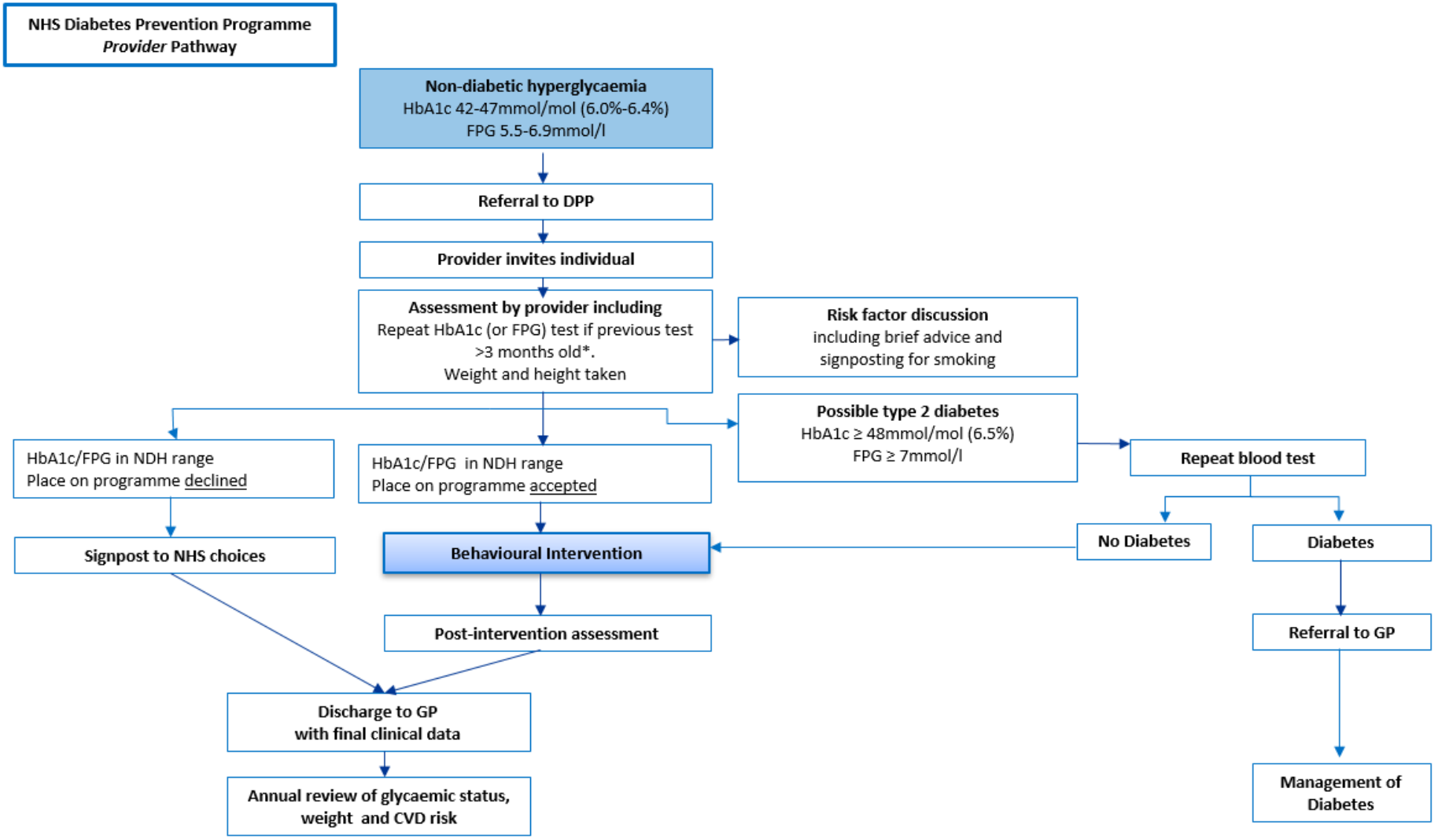
[4] https://www.england.nhs.uk/nhs-standard-contract/2017-19-update-may/

[5] Standard General Medical Services Contract, section 16

[6] *Good Practice Guidelines for General Practice Electronic Records* (Version 4, Department of Health 2011), available at https://www.gov.uk/government/publications/the-good-practice-guidelines-for-gp-electronic-patient-records-version-4-2011

# Appendix 3 – DPP referral pathways






*Repeat of blood test is to establish baseline only. Even if shows normoglycaemia individual will still be accepted onto programme on basis of previous result

# Appendix 4 – Fair Processing

It is a legal requirement that GPs and providers (as data controllers) have registered the purpose(s) for using personal data with the Information Commissioner's Office and provide fair processing information to patients of the information they process.

Fair processing notices must include

- Contact details of the data controller;
- Contact details for the data protection officer;
- The purposes for processing the data and the legal basis for processing the data
- Information about with whom data are shared;
- Any rights of objection which are available;
- That patients have the right to access their medical record and to have inaccurate data corrected
- Retention periods
  The right to lodge a complaint with the Information Commissioner's Office (ICO).

It is important that patients are provided with this information in relation to the NHS Diabetes Prevention Programme.

Practices and NHS DPP providers should make information available to all patients, for example, by displaying posters and providing information leaflets in patient waiting and treatment areas, and by posting information on their web sites. This information should be supplemented by the provision of information in the invitation letter as described in section 5.4.

## Example text for a fair processing notice – GP Practice

Our GP practice keeps records about you, your health and the care you receive, and is responsible for them as a data controller under the General Data Protection Regulation (EU) 2016/679).

The records we hold may include:

- basic details about you, such as address and next of kin
- contacts we have had with you, such as GP appointments and clinic visits
- reports about your health and any treatment or care you need
- details and records about the treatment and care you receive
- results of investigations, such as X-rays and laboratory tests
- relevant information from other health professionals providing care and treatment, relatives or carers.

We use this information to help us to assess your needs, provide you with appropriate care and for monitoring and managing our services. These records are retained until you are deceased.

In order for us to process, or use, your information in this way we must demonstrate that it is lawful in accordance with the GDPR. Under that law, we must demonstrate that using your information is necessary for achieving a particular purpose, and as your information relates to healthcare then is deemed more sensitive (known as a 'special category of personal data') and so we are required to demonstrate that the proposed use satisfies an additional purpose. In this case, the manner in which we use your information is lawful under the GDPR because it is necessary for the performance of our public function of providing you with health care (Article 6(1)(e) and necessary for the purposes of medical diagnosis and/or the provision of health care or treatment and/or the management of health or social care systems and services (Article 9(2)(h)).

To ensure you receive the best possible care, we may contact you to invite you to participate in health improvement programmes, for example the Diabetes Prevention Programme.

We maintain our legal duty of confidentiality to you at all times. We will only ever use or pass on information about you to others involved in your care and who have a genuine need for it. We will not disclose your information for other purposes without your permission unless there are exceptional circumstances, such as when the health or safety of others is at risk or where the law requires information to be passed on.

From time to time we may use the services of a data processor to assist us with some of our data processing, but this is done under a contract with direct instruction from the GP that controls how they will handle patient information and ensures they treat any information in line with the General Data Protection Regulation and Data Protection Act 2018, confidentiality, privacy law, and any other laws that apply. You have a right under the GDPR to:

- request a copy of information we hold about you. This is known as ‘the right of subject access’;
- request that we correct our records about you if they are found to be inaccurate or incomplete;
- object to the processing of your data;
- to request your personal data is erased, for instance where it is no longer necessary for us to retain such data (subject to certain exceptions);
- where there is a dispute in relation to the accuracy or processing of your personal data, request a restriction is placed on further processing; and
- to lodge a complaint with the Information Commissioners Office.

If you would like to know more about how we use your information, or if you do not want us to use your information in this way, please contact our Protection Officer who

is responsible for monitoring our compliance with the GDPR. [His/her] contact details are as follows [x].

**[contact details]**

## Example text for a fair processing notice – NHS DPP Provider

**[NHS DPP provider name]** keeps records about you, your health and the care we provide you and is responsible for them as a data controller under the General Data Protection Regulation (EU) 2016/679) They will include:

- your name, address and contact details
- information relevant to your treatment with us that we have received from your GP
- records of the treatment we have provided and the outcome.

We use this information to help us to assess your needs, provide you with the Diabetes Prevention Programme and manage our services. These records are retained until [x].

In order for us to process, or use, your information in this way we must demonstrate that it is lawful in accordance with the GDPR. Under that law, we must demonstrate that using your information is necessary for achieving a particular purpose, and as your information relates to healthcare then is deemed more sensitive (known as a 'special category of personal data') and so we are required to demonstrate that the proposed use satisfies an additional purpose. In this case, the manner in which we use your information is lawful under the GPDR because it is necessary for the performance of our public function of providing you with health care (Article 6(1)(e)) and necessary for the purposes of medical diagnosis and/or the provision of health care or treatment and/or the management of health or social care systems and services (Article 9(2)(h)).

When your treatment is complete we will send information about the treatment you have received and the outcomes to your GP practice to update their records.

We send information about the treatment that you have received to the commissioner of the NHS Diabetes Prevention Programme for payment and quality assurance purposes. This information will include your NHS Number and date of birth. If you have agreed to be contacted by a support organisation working for the commissioner to ask for your opinions about the service for evaluation purposes, we will also provide your name, address and telephone number(s).

You have a right under the GDPR to:

- request a copy of information we hold about you. This is known as 'the right of subject access';
- request that we correct our records about you if they are found to be inaccurate or incomplete;

- object to the processing of your data
- to request your personal data is erased, for instance where it is no longer necessary for us to retain such data (subject to certain exceptions);
- where there is a dispute in relation to the accuracy or processing of your personal data, request a restriction is placed on further processing; and
- to lodge a complaint with the Information Commissioners Office.

If you would like to know more about how we use your information, or if you do not want us to use your information in this way, please contact our Protection Officer who is responsible for monitoring our compliance with the GDPR. [His/her] contact details are as follows [x].

**[contact details]**

## Appendix 5 – Business rules for case finding

**NHS Diabetes Prevention Programme Audit Overview (v1.10)**

**NHS Diabetes Prevention Programme Audit Section Descriptions (v1.10)**

**NHS Diabetes Prevention Programme Audit Clinical Extraction Criteria (v1.10)**

**NHS Diabetes Prevention Programme Audit (v1.10)**

(If you require the above Business rules for case finding documents, please contact england.ndpp@nhs.net)

## Appendix 6 – Equality statement

Equality and diversity are at the heart of NHS England's values. Throughout the development of the policies and processes cited in this document, we have given due regard to the need to:

- Reduce health inequalities in access and outcomes of healthcare services integrate services where this might reduce health inequalities
- Eliminate discrimination, harassment and victimisation
- Advance equality of opportunity and foster good relations between people who share a relevant protected characteristic (as cited in under the Equality Act 2010) and those who do not share it."