PIAG
Patient Information Advisory Group

NHS
National Screening Programme for Diabetic Retinopathy

Factsheet: transfer and management of patient information in diabetic retinopathy screening programmes

Version 2.0, July 2005

1. Background

The management of a secure, systematic screening programme requires that a central list of patients is collated and managed effectively.

PCTs have been given the responsibility of ensuring that all their eligible patients with diabetes are offered the opportunity to have their eyes screened as part of a systematic programme run to national standards. PCTs are having to commission services together with other PCTs so that that programmes are of sufficient size to ensure that a robust service can be provided.

This means that for most PCTs there is a need to transfer basic patient data into a single list. That data comprises the patient's identifying details including name, date of birth, contact details, NHS number, and the GP's name and contact details, together with the disclosure of the fact of that patient's diabetes. That single list is usually managed by the PCT, or an acute trust. It is also possible that independent sector providers may also be involved in the screening process, those normally being optometrists, private companies specialising in screening or private individuals specialising in screening.

2. Patient Information Advisory Group (PIAG) and s.60 Health and Social Care Act support

The National Screening Programme for Diabetic Retinopathy ("NSC DR") approached PIAG for advice as to whether or not it was necessary to make a full application for s.60 support. A decision was taken in December 2004 by PIAG and has been minuted as follows:

> "10 **Diabetic Retinopathy Screening**
> PIAG considered a request from the national retinopathy screening programme for clarification about whether Section 60 support was required for the programme as information would need to be shared across several PCTs, hospital clinics and general practices. There had been reluctance on the part of some data controllers to release patient information to the screening programme because of confusion about this. The Advisory Group agreed that call and recall for retinopathy screening was part of the care pathway. As such, consent to sharing relevant data could be implied from information about how patient information is used by the retinopathy screening programme, being provided to patients, and by making it clear patients had the right to opt out. There was therefore no requirement to apply for Section 60 support."

This clarifies that it is possible to collate basic data to create a single collated list for a screening programme providing it held by a PCT, acute trust or general practices and managed by NHS staff, as all are direct NHS bodies. This can be done without s.60 applications as consent can be implied for that limited part of the operation. This enables programmes to communicate with patients to explain how they are going to manage their screening appointments and data, and to explain to patients which other organisations may be involved in the screening process who may need access to the patient data for that purpose.

When reviewing and managing their own information security measures and in the way they manage independent sector provider's security measures, programmes should take account of the

advice available on the PIAG web-site in this regard. See:
http://www.advisorybodies.doh.gov.uk/PIAG/applications.htm.

3. Independent sector

PIAG has advised that data should NOT be shared with non-NHS bodies (including optometrists) until the patient has communicated consent either directly by speech or by conduct (e.g. by the patient selecting an optometrist from a list of approved providers selected by the programme and going into the practice to ask for his or her eyes to be screened).

PIAG also say that it is important that any programme using any independent sector provider has effective contracts governing not only clinical standards and delivery, but also administrative standards and delivery. This should include provisions requiring them work in accordance with both the data protection standards and the confidentiality standards in the NHS. These policy documents should be included as part of the contract with the provider. In addition, robust management of the contract is required to ensure that the contractual obligations in this regard are being followed in practice.

Some programmes are considering outsourcing the entire running of the programme including the management of the central call/recall list. The single collated list, in those circumstances, can only be transferred to the independent sector provider once direct patient consent has been obtained by the trust or GP to that effect.

4. Opting out – programme and data sharing

A very small number of patients may choose not to participate in a screening programme or may have concerns about who would have access to their data.

Opt-out

PIAG have since advised that patients should be informed of their right to opt out of screening completely and how to go about it, but care should be taken to ensure that patients make such decisions on a fully informed basis and they should be encouraged to discuss this decision not only with the programme but also with their GP. In addition care should be taken to identify whether the patient wishes to opt out only temporarily or permanently. Programmes are advised that they should try and obtain confirmation of any desired opt out from the patient in writing, together with the terms of the opt-out. If it is temporary opt-out, then the programme should agree with the patient the interval that should be left before the screening programme approaches them to give them a further opportunity to have their eye screened. This needs to be flagged up in the administration system.

Even if the patient permanently opts-out he or she should be asked whether or not they would like to be approached to reconsider the decision in a specified period. The patient response should be recorded verbatim.

Patients may also be concerned about who will have access to their data and may seek to limit those who can be involved. If the programme is operating a mixed economy scheme the problems are likely to be capable of being overcome by allowing the patient to attend for one mode of screening rather than another (e.g. a fixed site rather than attending an optometry practice, or visa versa). Where programmes only offer one type of scheme then this problem may mean that the patient cannot be screened effectively because the patient is unwilling for a key participant or group of participants to undertake the screening. Whilst all reasonable efforts should be made to try and accommodate a patient's request this should not be at the expense of the secure systematic management of data. Programmes need to keep careful records of both their actions and their inactions. Indeed there is a legal requirement to maintain accurate patient records.

If this is the issue then the programme will have no option but to explain to the patient that it will not be possible to screen them within the programme. This should be communicated in writing both to the GP and the patient so they can discuss what other alternatives outside the programme can be offered to the patient.

However, if the objection is, for instance, that a particular screener, grader or physician is known to them and this would cause discomfort or embarrassment then this concern may well be overcome by ensuring that a different screener/ grader/ assessor works with this patient.

5. Patient information leaflets

The National Screening Programme for Diabetic Retinopathy has written patient information leaflets dealing with diabetic retinopathy, laser treatment and eye screening. PIAG has been consulted with regard to the latter and leaflets are in the process of crystal marking. We hope that they will be made available on the www.nscretinopathy.org.uk web-site by the end of August 2005. Whilst they deal with these issues in general terms, programmes will have to take care to provide patients with additional detailed information about how opt out and data sharing will be managed in their own programme. The precise groups that will have access to patient data should be clearly specified and care needs to be taken to ensure that the systems that underpin the programme are designed to ensure that data is moved to non-NHS bodies only once the patient specifically consents. This needs to be explained clearly to patients so that they understand the particular system that their programme is using.

6. Physical security of property

Patient data is stored in a number of places and in a number of ways. Clear guidance should be given to all staff involved in the screening process of the importance of keeping equipment in a secure environment. Laptops, particularly in mobile programmes, need to be kept secure at all times. Vehicles and offices need to be secured and the property (including laptops) needs to be securely secured within them to make theft difficult. The management of CDs and DVDs containing patient data needs to be carefully monitored so that secure process for their movement are put in place and monitored. Those programmes that have purchased approved software will automatically find that security measures are in place to control access to data even if the property containing the data is mislaid. The messaging specifications that are to be incorporated into the approved software will provide very heavy levels of encryption that will further secure data. Those programmes that have purchased outside the approved list should take immediate steps to ensure that their software provides similar levels of encryption.

This document has been reviewed and approved by the Patient Information Advisory Group (PIAG).

Comments on this document are welcome. The author can be contacted at:

Fionna O'Leary, Programme Manager fionna.o'leary@glos.nhs.uk