Health and Social Care Board

Northern Ireland

Paperlight Accreditation Policy

Version 1.0

BMA

RCGP NI Royal College of General Practitioners

DHSSPS Department of Health, Social Services and Public Safety www.dhsspsni.gov.uk

Contents

1 Introduction

1.1 Approval by the HSC Board to keep electronic patient records is a requirement of the GP contract and is vital to ensure that practices have appropriate and robust procedures in place to enable them to operate safely through the transition from paper-based to electronic records.

1.2 The HSCB will need to be satisfied that an applicant practice is ready to be paperlight. The term 'paperlight' relates to a practice that uses its computer system as the main place where patient records are held. Practices will no longer be dually recording that information on paper. They will be using the computer system contemporaneously in the consultation and recording their findings according to standards set out in the *Good Practice Guidelines for GP Electronic Patient Records (Version 4).* Manual notes may be referred to for historic information but all new and current clinical information is available on the computerised or electronic patient record.

1.3 Practices applying for HSCB approval to keep computerised records in whole or in part must complete and return the Self-Assessment Checklist at Appendix 2 of this document.

1.4 The GMS Contract requires practices applying for approval to have regard to any guidelines issued by the Department of Health, Social Services and Public Safety (DHSSPS).

1.5 If a practice is unsure as to their state of readiness to become paperlight or if the practice would like additional assistance or advice in preparation to become paperlight they should contact the HSCB.

1.6 If there is doubt as to the readiness of a practice to become paperlight, the HSCB will consult with the LMC and a practice visit may be arranged to address the area(s) of concern.

1.7 A practice that does not meet the standards will not be approved and therefore will need to continue to maintain paper records. The HSCB will work with the practice to develop an action plan to move towards gaining approval.

1.8 If at any time after approval has been granted, the HSCB has reasonable concerns as to the practice's ability to maintain adequate and secure electronic

patient records, the HSCB will notify the practice and the LMC immediately that the approval is under review. The HSCB in conjunction with LMC will undertake an investigation into the concerns and if it finds that an approved practice is not complying with a standard, it will work with the practice to develop an action plan to achieve compliance. If this is not achieved, the approval may be withdrawn and the practice will need to reinstate paper record keeping.

2 Paperlight

2.1 The decision to keep computerised patient records must be supported by the whole practice team. All clinical team members will require access to the practice's clinical system. Practices will need to carefully consider and plan for the transition from paper-based to electronic records.

2.2 At this stage, there is no precise definition of what the electronic record should contain, however practices must have regard to the *Good Practice Guidelines for GP Electronic Patient Records (Version 4).* The content of the record will be determined by the practice and should be consistent with the former paper records held in the Patient Record Chart. Where this is the case, and practices have achieved HSCB approval, then it will not be necessary to continue to maintain paper records.

2.3 It is a requirement that the Health and Care Number is recorded in patient registrations.

2.4 All systems in use by GPs must be GPSoC Level 0 with NIMSS Level 2 compliant (or later versions of this standard). All systems presently supplied in Northern Ireland are compliant.

2.5 The approval process will not include specific checking of the quality of electronic records. The practice will be asked to certify that it has:

- A fully operational clinical record keeping policy which sets out what information is recorded in an exclusively electronic format; and
- Procedures in place to ensure information is available when needed to support clinical-decision making.

2.6 The components of a safe record keeping system are outlined in the practice Self-Assessment Checklist at Appendix 1. These standards are intended as a statement of the minimum requirements to hold electronic records, to ensure that clinical information is fit for purpose and is held and shared safely to support the delivery of clinical care.

2.7 When a patient leaves a practice a full patient record must continue to be forwarded when requested to Business Services Organisation (BSO), with the

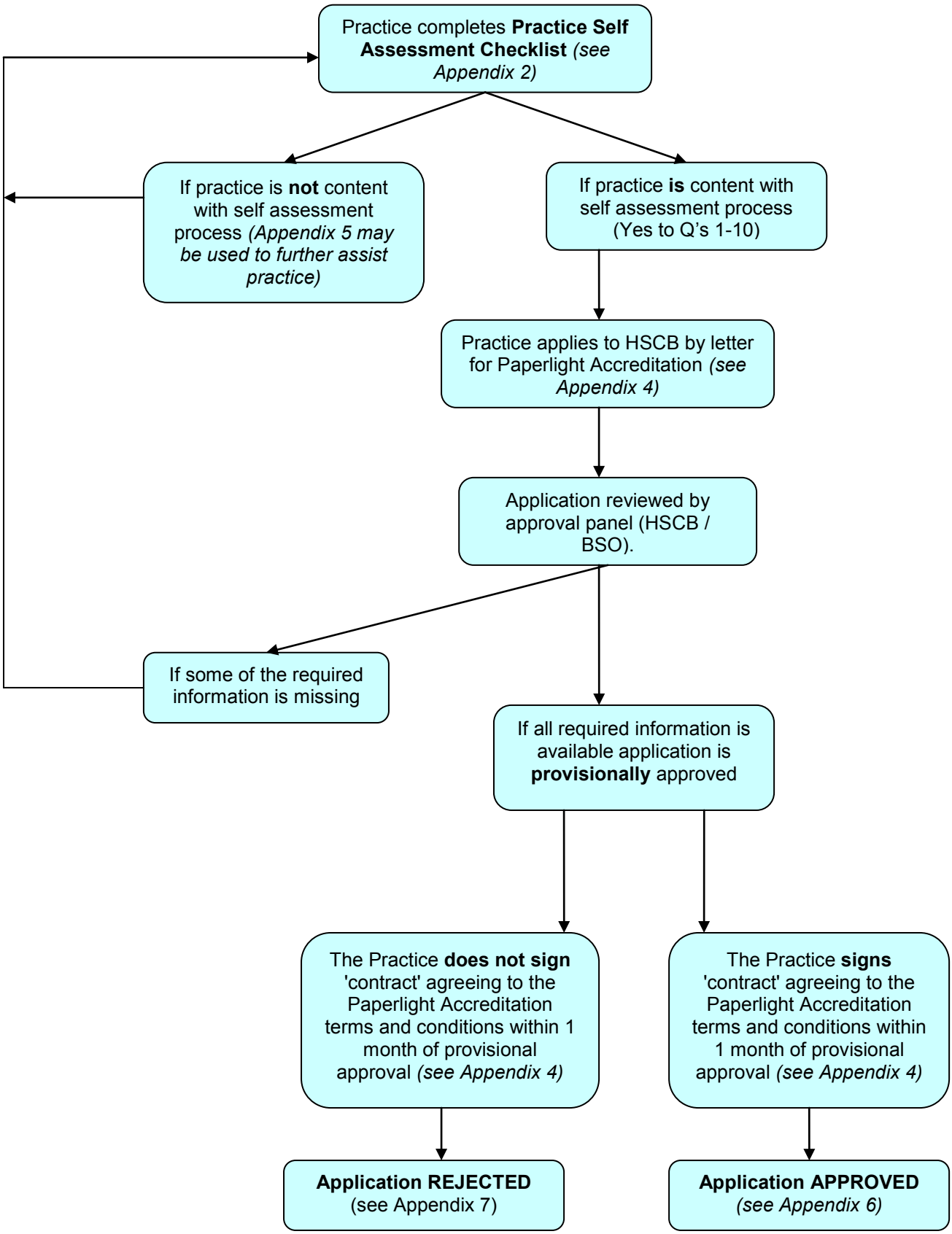
existing Patient Record Chart and that record must contain all relevant paper records including a printout of the entire computer record and word processed or scanned documents.

2.8 All significant clinical information must be recorded contemporaneously in the computerised record by all clinicians consulting regularly at the practice. This process gives a practice approval to hold electronic patient records.

Appendix 1

Approval Process

This approval process is based on *The Good Practice Guidelines for GP Electronic Patient Records Version 4 (2011)*:



Appendix 2

Health and Social Care Board

Practice Self-Assessment Checklist

1. For each question on the Checklist tick "Yes", "No", "Not Known" (N/K) and add notes and comments as appropriate.

2. If “Yes”, the answer should be backed up by supporting evidence and documentation as required.

3. If answering "No" or "N/K", a practice should consider whether it is ready to apply for approval to hold patient records solely in electronic format and regard should be given to the *Good Practice Guidelines for GP Electronic Patient Records (Version 4).*

4. **Unless all the answers to questions 1-10 are “Yes”, the HSCB will not approve the application.**

5. The evidence/comments box should be used to:
   - Reference evidence of good practice, submitted with the Checklist;
   - Indicate where conformance is only partial;
   - List exceptions;
   - Indicate frequencies where applicable;
   - Name individuals with responsibility for specific areas.

6. Appendix 5 may aid in-house planning towards becoming fully compliant with the accreditation process.

Health and Social Care Board

Application to become Paper Light in Primary Care
Practice Self-Assessment Checklist

Notes to assist practices in the completion of the Self-Assessment Checklist are provided at Appendix 2

Assessment Area	Question	Supporting Evidence Required	YES	NO	N/K	Evidence / Comments to be Submitted
1. Information security and confidentiality	a) Has the practice assigned responsibility for Information Governance to appropriate member or members of staff?	Documented Information Security and Confidentiality Policy (see HSCB model) including: Named Data Guardians.				No evidence required to be submitted, evidence to be retained at practice in event of visit.
	b) Does the practice hold a current, valid Data Protection notification?	Copy of the notification.				No evidence required to be submitted, evidence to be retained at practice in event of visit.
2. Back-ups	a) Are back-ups carried out regularly according to documented procedures?	Documented procedures and log of back-ups.				No evidence required to be submitted, evidence to be retained at practice in event of visit.
	b) Are back-ups which are held on-site stored in a secure place away from the server location, and are fire risks and theft taken into account?	Details of media safe which complies with British Standards. Manufacturer = Model =				No evidence required to be submitted, evidence to be retained at practice in event of visit.
3. Access	Are there sufficient terminals available to ensure that data can be entered contemporaneously?	Written confirmation that all staff who require access to the clinical system are able to gain access to a workstation.				No evidence required to be submitted, evidence to be retained at practice in event of visit.
4. System availability	Are there procedures in place to minimise the occurrence and impact of system downtime, and facilitate a	A copy of the Practices Business Continuity Plan. A log of system downtime and power failures including actions and lessons				No evidence required to be submitted, evidence to be retained at practice in event of visit.

Health and Social Care Board

Application to become Paper Light in Primary Care
Practice Self-Assessment Checklist

Assessment Area	Question	Supporting Evidence Required	YES	NO	N/K	Evidence / Comments to be Submitted
	speedy and full recovery of the clinical system and data?	learned.				
5. Secure Access	a) Is access to records password controlled and only available to designated trained staff (including locums and temporary staff)?	A separate Access Control Policy or a section within Information Security Policy.				No evidence required to be submitted, evidence to be retained at practice in event of visit.
	b) Are all system security measures and audit functions enabled?	Evidence to show audit trail enabled and that practice know how to access it.				No evidence required to be submitted, evidence to be retained at practice in event of visit.
6. Training and awareness	Is there a training programme in place for all staff that input data to the system (including locums and temporary staff)?	• Induction Checklist. • Locum pack.				No evidence required to be submitted, evidence to be retained at practice in event of visit.
7. Virus Protection	Are appropriate steps taken to protect patient records from corruption?	• Virus protection measures to be documented in Information Security Policy. • Evidence that virus protection software has been updated and is regularly run. • In the event of virus protection failure BSO Helpdesk has been notified.				No evidence required to be submitted, evidence to be retained at practice in event of visit.

Health and Social Care Board

Application to become Paper Light in Primary Care
Practice Self-Assessment Checklist

Assessment Area	Question	Supporting Evidence Required	YES	NO	N/K	Evidence / Comments to be Submitted
8. Data Quality and records management	Does the practice have agreed policies on record content and information management?	• Documented Clinical Record Keeping Policy. • Evidence that patient information flows have been reviewed.				No evidence required to be submitted, evidence to be retained at practice in event of visit.
9. Patient Record transfer		Written procedure for transferring records when a patient leaves the practice documented in Clinical Record Keeping Policy.				No evidence required to be submitted, evidence to be retained at practice in event of visit.
10. Operating as Paperlight	Is all significant clinical information added contemporaneously to the electronic patient record by all clinicians consulting regularly at the practice.	Paper-light practice is documented in the Clinical Record Keeping Policy.				No evidence required to be submitted, evidence to be retained at practice in event of visit.

Health and Social Care Board

Appendix 3

Notes to assist practices with the completion of the Self-Assessment Checklist (see Appendix 2)

A Practice application for approval must provide evidence which demonstrates the following issues have been addressed.

Assessment Area	Evidence required	Check √
1. Information security and confidentiality	a • Documented Information Security and Confidentiality Policy (see HSCB model) including named Data Guardian. • Evidence of compliance with the Data Protection Act and the DHSSPSNI Code of Practice on Protecting the Confidentiality of Service User Information (2012)	
	b • A copy of a valid Data Protection registration certificate needs to be provided.	
2. Back-ups	a & b • Separate policy, or part of practice Information Security and Confidentiality Policy, which sets out: i. Documented procedures and log of back-ups. ii. Details of media safe which complies with European Standards (S 120 DIS [EN 1047-1] and 120 Diskette [NT Fire 017]). iii. Documented procedure for back-up and tape verification. **Points to consider in preparing evidence:** • For practices using clinical systems on a remote central server: do you have copies of the supplier's back-up procedures?(N/A as yet in Northern Ireland) • For practices using clinical systems on their own server; what back-up procedures do you follow? • Who is responsible for ensuring the back-up was successful? • Who is the deputy? • Is there a full rota to ensure all staff are clear of their responsibilities? • Is there a daily back-up log to show who checked the back-up and where the tapes are stored? • Are the back-up tapes sent for monthly tape validation? • Are the tapes changed first thing in the morning in case there is a fire or accidental overwrite? • Is the current back-up tape kept in a fireproof safe on site in case it is required for an immediate recovery? The fireproof safe should ideally be to BS 476 part 20 standard – UK tested. • Is an earlier back-up tape kept off site in case of problems on site? • How many weekly cycles of tapes are kept? Minimum of two weeks are required. • Are the tapes rotated on a regular basis? • Are the tapes renewed on a regular basis? • Is the date the tape is first used marked on the outside? • Is back-up verification performed on a quarterly basis? • Is a full system back-up undertaken daily? This should also include scanned attachments and referral letters. • Is there an appointments back-up procedure? • Is the appointment system backed-up to floppy disk for viewing on a PC using Excel or onto the 'C' drive of a PC, or are printouts taken of appointments on a regular basis?	

	• Which individuals within the practice have the authority to load software? • Can the practice provide copies of the last three months tape validation reports from the clinical system supplier? • Does the practice back-up any other data e.g. personnel records, payroll, accounts?	
3. Access	• Written confirmation that all staff that need to access the clinical system are able to gain access to a workstation.	
4. System availability	• Documented system downtime procedures	
5. Secure Access	a & b • A separate Access Control Policy or a section within Information Security and Confidentiality Policy. • Evidence to show audit trail enabled and practice knows how to access it e.g. anonymised audit trail report. **Points to consider in preparing evidence:** ***Each and every update of patient records must be attributable to an individual member of staff in terms of both data entry and ownership. The policy/evidence required must cover the following:*** • Who is responsible for enabling staff access to the clinical system? • Is there a list indicating which members of staff have access to the clinical system? • Are all staff given access to areas of the system according to their role? • Does it include the level of access for each member? • Is this list updated when staff leave? • What is the procedure for removing a staff leaver? i. Are leavers passwords disabled as per Information Security Policy? ii. Keys returned? iii. Alarm codes changed? • Can the practice produce a report of the audit trail from the clinical system? • Are they aware that they must not share this password with anyone else? • If staff have been away from their workstation, do they check to ensure they are using their own login? • When staff are away from their workstation do they sign off? • Are staff aware of the legal implications of password sharing? • Are there any disciplinary procedures relating to password sharing? • Are staff aware that passwords should not be written down and clues can be kept off-site? • Are staff aware that a mixture of letters, numbers and special characters should be used to avoid the possibility of guessing the password? • Are staff aware of the minimum length of password? • Are staff aware that they should not use easily guessable passwords e.g. children, spouses or pet's name? • Are staff aware that they should change their password if they think it has been guessed or used by another member of staff? • How many attempts are allowed before the password is disabled? • Does any member of staff have remote access to the practice network and clinical system? What additional safeguards are in place to prevent unauthorized access? • Are all staff briefed regarding the content of the practice's Access Control/Information Security Policy? • What is the length of time that your system forces a password change?	
6. Training and	• Induction checklist.	

awareness	• Locum pack. **Points to consider in preparing evidence:** • Are the staff trained on the standards and procedures that the practice operates, according to the requirements of their role? Specifically this training must include making staff aware of the need to keep their workstation secure and information confidential. • Is the training completed before the staff use the clinical system? • Does the practice carry out annual Training Needs Assessments? • Is the training undertaken by each member of the practice team linked to his or her Training Needs Assessment and personal development plan? • What training do staff receive on information security and confidentiality, on induction, and on a regular basis? • Are the staff trained on how to use the clinical system? Who provides this training? • Is there a training and support pack for locums as well? • Is there a log of staff training & dates completed, including induction training of new staff, locums and relief staff? • Can staff readily access hard and electronic copies of the practice's Information and Security policies and protocols?	
7. Virus Protection	As described in appendix 2	
8. Data Quality and records management	• Documented Clinical Record Keeping Policy. • Evidence that patient information flows have been reviewed. **Points to consider in preparing the evidence:** • Does the practice have procedures in place to ensure completeness and consistency of data capture in order that information is available and reliable when needed for making clinical decisions? • Is any information still routinely dual recorded on paper as well as computer? • What quality checks are undertaken in respect of scanning and clinical coding? • Is the practice aware of and operating in compliance with the Good Practice Guidelines for GP Electronic Patient Records Version 4? Does the practice have procedures for the secure storage, transfer/disposal and destruction of records? • Do GPs enter data directly, or indicate for non-clinical staff what data needs to be entered, from incoming clinical correspondence? • Do clinicians routinely enter their own consultation data contemporaneously on to the computer system? • Do staff entering clinical data receive training on the clinical system, read codes and, for non-clinicians, medical terminology? • Has the practice mapped clinical information flows? • Does the practice have a Clinical Record Keeping Policy (or equivalent), which sets out its agreed policy on record content and management for the following areas? i. Patient contacts with practice clinicians ii. Practice referrals iii. Test / investigation results iv. Hospital letters v. Out of Hours contacts vi. Drug therapy, prescriptions and medication reviews vii. Refinement / amendment of the clinical record viii. Notes Summarisation ix. Scanning (where applicable) x. Temporary residents • Does the practice scan letters? i. In what format?	

	ii. What data quality checks are undertaken? iii. Are scanned images backed up along with other areas of the clinical system? iv. What happens to the paper copy?	
9. Patient Record transfer	• A written procedure for transferring records when a patient leaves the practice.	
10. Operating as Paperlight	• Paper-light practice is documented in the Clinical Record Keeping Policy. **Points to consider in preparing evidence:** The practice's Clinical Record Keeping Policy should cover the following: • Is all significant clinical information added contemporaneously to the electronic patient record by all clinicians consulting regularly at the practice? • Are paper notes routinely pulled for consultations? • Can paper notes be readily accessed if required, and if so, within what time period? • Are any notes stored off-site? What security arrangements are in place for these records? • Are any clinical entries made only in the paper record? • Has the practice achieved 80% summarized records (QOF Indicator – Records 18)? • Does the practice scan in-coming clinical correspondence?	

Health and Social Care Board

Appendix 4

Application for Paperlight Accreditation in Primary Care

Practice name:

Practice address:

Re: Paper Light Accreditation
I /we the undersigned wish to apply for consent to keep our HSC patient medical records in electronic format.

Furthermore, I /we confirm that:

1. The practice has completed Q 1-10 of the self assessment checklist and said 'Yes' to all.
2. All GP Systems in Northern Ireland meet the agreed accreditation standard (RFA99 V1.1) however the implementation and use of each clinical varies by practice therefore does the implementation of the GP Clinical system in your practice meet the operational requirements of the practice and as such is it considered fit for purpose.
3. The computer system security measures and audit functions are enabled.
4. The practice will not seek to disable the security and audit functions.
5. All the Partners to the Contract in the practice are aware of and undertake to have regard to the *Good Practices Guidelines for GP Electronic Patient Records Version 4.*
6. The Partners to the Contract are responsible for ensuring that all other staff in the practice are aware of and undertake to have regard to the *Good Practice Guidelines for GP Electronic Patient Records Version 4.*
7. The practice has IT recovery arrangements verified by the BSO on behalf of HSCB.
8. The practice has in place a security policy that complies with current good practice.

Practice computer system name and version:

.....

Practice registered name and number under the Data Protection Act:

.....

I /we agree that a full patient record will continue to be forwarded when requested to the BSO and that all relevant paper records will be included in it. Practices must provide a printout of the entire computer record and including word-processed or scanned documents or transfer the same on electronic media.

Health and Social Care Board

Appendix 4

Paperlight Contract

I /we am /are aware that compliance with these conditions can reasonably be audited by the HSCB and that approval is subject to routine review every 3 years. If, at any time after approval has been granted, the HSCB has reasonable concerns as to the practice's ability to maintain adequate and secure Electronic Patient Records, the HSCB will notify the practice and the LMC immediately that the approval is under review.

The Practice Manager and <u>all</u> Partners to the contract within the practice <u>must</u> sign below:

PRINT NAME	SIGNATURE	DATE

Original to HSCB, copy retained at practice.

Appendix 5

Sample Action Plan

Issue & Objective	Action & Timescale required	Constraints and/or impacts of not applying the action	Accountability	Monitoring
Use this column to identify areas of non compliance	*Tasks and steps required to meet the objective*	*Identify constraints, if any in achieving the outcome and/or the impact of doing nothing*	*Who is responsible (job title or name) for taking the action forward*	*How will outcome continue to be measured to check that the improvement is being maintained?*
Example *Clinical Coding* *To create a Policy for Clinical Coding*	*1. Adopt generic document & amend to suit practice.* *2. Clinicians review and agree amendments* *3. Policy implemented with staff awareness training. Within 4 months*	*1. GP too busy* *2. Coding becomes inconsistent*	*GP Secretary* *Practice Manager*	*Quality of clinical coding*

Health and Social Care Board

Appendix 6

Authorisation Form

This certifies that the HSCB Paperlight approval panel consents to practice____ application to keep electronic records as required in Part 15 of the Standard General Medical Services Contract 2004. Specifically, the HSCB is satisfied that:

- The clinical computer system upon which the practice proposes to keep the records is accredited to Requirements for Accreditation – GPSoC Level 0 with NIMSS Level 2 compliant (or later versions of this standard);
- The security measures and the audit functions incorporated into the computer system have been enabled;
- All Partners to the Contract are aware of, and have signed an undertaking, that they will have regard to the *Good Practices Guidelines for GP Electronic Patient Records Version 4*;
- The practice will inform the HSCB of any changes that may alter this certification;
- The practice will allow the HSCB to review this approval at any time for any reason.

Partner/ Lead GP

Name

Practice

Name: **Address:**

HSCB Authorising Officer

Name: **Role:**

Signature: **Date of approval:**

Original retained at HSCB, copy sent to Practice

Health and Social Care Board

Appendix 7

Failure to sign Form

The HSCB Paperlight approval panel cannot consent to practice____ application to keep electronic records due to failure to sign the ‘Paperlight Contract’.

The Practice may wish to resubmit a signed Paperlight Contract to enable application to be approved. Please review appendix 1 for Approval Process to become Paperlight.