Enhancements to eDSM

FAQs

Document History

This section should only be used when a new version of an existing document is created. Newer versions should detail which sections have been amended/added.

Version	Date	Description
1.0	10/10/2017	Document created.
1.1	13/11/2017	Amendments from internal review

These instructions are correct at the date of writing. For further assistance, consult the SystmOne Online Help.

Contents

Background to the changes

What is the background to these changes? Who has been consulted?

TPP has been working closely with NHS England, NHS Digital and the ICO, with support from the SystmOne National User Group and the BMA, to review the existing Enhanced Data Sharing Model (eDSM) and to provide additional controls for data controllers. Particular consideration has been given to supporting compliance with principles 1 and 7 of the Data Protection Act. The eDSM developments have been designed to ensure that GPs have greater flexibility and control over which organisations have visibility of their patient's SystmOne EHR and can work in partnership with their patients.

It is hoped that GPs will share their records more readily with non-GP organisations whilst respecting their patient's wishes and expectations.

Using the 'Allowed', 'Prohibited' and 'Verification' lists

Who can control the lists?

GP organisations will have the ability to set up the lists for their patients who are fully GMS registered. GP Practices can set this on an organisation-wide and/or patient-specific basis. The patient can also set up the 'Allowed' list via SystmOnline.

What decisions do I have to make and when do I have to make them?

No changes to sharing will occur until the GP Practice activates the new controls.

GPs will have the option to decide whether organisations are allowed to record a share-in, prohibited from recording a share-in or need to go through an extra verification/security step in order to confirm the patient's consent. Until you choose to set this up, nothing will change regarding your patients' sharing preferences. The default will be 'No Organisations Require Verification' and sharing will continue as normal.

Also, note all these changes are additional to the existing controls within eDSM. Therefore, GP records that are not shared out are unaffected by these changes. If a patient record is not set to be shared out by the GP practice (dissent to share out), the new controls above do not need to be used. The option 'No Organisations Require Verification' should be set for such patients to ensure record sharing between other SystmOne organisations is not affected.

What will happen if I don't do anything?

Until you choose to make any changes, nothing will change regarding your patients' sharing preferences and eDSM will continue to function as it does currently.

What is fair processing and do I have to do it?

Fair processing is your organisation's responsibility as a Data Controller to ensure patients are informed of how their personal information is used including how, when, why, and what data is shared to which other organisations, as well as the options available to them. Staff should be trained in how to carry out adequate fair processing and processes should be in place to ensure this happens.

TPP has produced documentation to aid organisations with fair processing of personal and confidential data by your organisation. The documents advise you on how SystmOne allows (or does not allow) your patients' records to be made available to other organisations, across a variety of healthcare settings (subject to your permission).

This document can be used, in conjunction with your own fair processing documents, to help inform patients of the options available to them. For complete guidance on how to construct a Fair Processing Notice please refer to the Information Commissioner's Office website.

How do I handle requests from patients who want a specific arrangement?

As well as setting a practice default, you can also set a specific custom setting on an individual patient basis from within the patient record. This is to cater for any patients that have specific needs regarding the sharing of their health record.

Does changing the preference in SystmOne override the patient's preference on SystmOnline?

SystmOne will take the most up-to-date preference, which is set for the patient. This means that the patient can change the GP's decision, and vice versa. However patients cannot add organisations to the Prohibited list, this must be done via their GP within SystmOne.

Are the preferences my patient has changed on SystmOnline auditable?

Not currently, but we are looking at developing an audit so you can see which users have made changes to the lists, or what the patient has changed on SystmOnline.

What happens to a patient's preferences when they move GP Practice?

If a patient has opted for the 'GP default' at your GP practice, when they move to a new practice they will inherit the new practice's default.

If a patient has opted for a Custom setting, their custom preferences will be carried over to the new practice.

Can the patient set their sharing preferences on the SystmOnline app?

Currently, patients can only control their sharing preferences and verification/security requests via the browser version of SystmOnline through their phones or desktop, not through the app.

Verification process

What does my patient need to be able to verify their consent? Do the mobile and e-mail addresses have to be verified to work?

They will need with either:

- an SMS number, set up by an organisation that is not the organisation attempting to access the shared record
- an email address, set up by an organisation that is not the organisation attempting to access the shared record
- access to their GP SystmOnline account

What about patients who don't have access to technology?

As the patient's Registered GP, you can set preferences for which organisations are able to record a share-in for the patient without the verification/security process, and which cannot record a share-in for the patient, on an individual patient basis, or at an organisational level. This means that when the patient presents at a SystmOne organisation with permission to record a consent in, they will be asked for their consent in person, in line with the current eDSM operation, but they will not be asked for their verification/security code.

How will this work in urgent care settings where patients are unconscious?

If the urgent care organisation is on the 'verification' list and the patient is unable to verify their consent, the clinician will be unable to access the shared record. Organisations should contact the patient's Registered GP if it would be suitable for their organisation to be on the 'Allowed' list for that patient or for all the GP practice's patients. Clinicians will still be able to access the Summary Care Record.

How will this impact on patients who have proxy access to makes these decisions on their behalf?

People with proxy access will be able to access the patient's sharing preferences via SystmOnline.

How long will the verification/security code be valid for?

The verification/security code (PIN) will be valid until you cancel out of the Verification dialog. Once this dialog has been cancelled, the code will expire, however patients can still approve the request for verification through SystmOnline. Another code will be generated and sent to the user when consent to view the shared record is recorded again.

What if I do not have face-to-face interaction with my patients so can't get the verification code (e.g. Child Health, Referral Triage Centres, EPR Core)?

A number of options are available:

- Contact the patient's Registered GP, who will be able to decide whether your organisation does in fact need to complete the extra verification step.

- If the patient/Registered GP has decided that your organisation requires verification, the patient can approve the request to share-in the record through SystmOnline, or provide you with the verification/security code sent via SMS and/or email, over the phone.

- If the patient/Registered GP has decided that your organisation is to be placed in the allowed list, then eDSM will function as before.

A practice has placed my organisation in the Prohibited list, but the patient wants my organisation to view their record. What can I do?

If the patient has access to SystmOnline, they will be able to remove organisations from the Prohibited list if appropriate. If not, the patient or your organisation should have a conversation with the Registered GP about their choices for record sharing.

If a non-GP organisation has not added an NHSmail account to their system or have an SMS integration, how are the verification messages sent?

The verification code will attempt to send via SMS, email and through SystmOnline. You will be presented with a dialog showing how the verification/security code has been sent for that particular patient, for example, if it has sent via email but not via SMS.

If the organisation is unable to send an SMS, the patient will still be sent the code via email, and will also be able to approve the request through SystmOnline.

If this fails, you can also contact the patient's registered GP to discuss allowing your organisation to record a share-in for this patient, with consent, without the extra verification/security process.

Once a patient gives an organisation the verification code, does that just apply for that episode of care or can that organisation then see that patient record forever?

Currently, once the patient has shared in to an organisation, the organisation will continue to be able to see their record, even if that organisation is subsequently placed on the Verification or Prohibited list.

TPP are investigating the possibility of applying the verification/security code episodically. This means that the verification/security code will last for one episode of care (e.g. referral, OOH contact). For example, if the organisation was previously on the 'Allowed' list, and subsequently moves to the 'Verification' list between periods of care, the organisation will be prompted to verify when they attempt to re-register the patient for another period of care. TPP will keep customers updated on the progress of this investigation.

What happens with a child's patient record where the parent's mobile is recorded but the parent is not present?

The parent can provide the verification code via phone to the SystmOne user, alternatively the verification is also sent to the email address recorded on the patient's record and through SystmOnline. Parents with proxy access to

the child's SystmOnline account will also be able to access the Sharing Requests and customise the Child's sharing rules.

Most patients won't think about their record status until they need it e.g. turning up at A&E in a place remote from their home surgery – how will they give on the spot access in these situations?

Patients can remove organisations from the Prohibited list on SystmOnline, and add organisations to the Allowed list or approve requests through SystmOnline. In addition, GPs will hopefully have had a conversation with the patient as part of fair processing about the choices available to them.

Pilot and rollout

Where's the pilot site?

We are currently piloting with a number of GP Practices in Wakefield, and a nearby Community unit who have been put in the Verification list for the purposes of the pilot to test the verification/security process. The functionality will be expanded across Wakefield CCG over the coming weeks.

When will this be released?

The pilot of the new functionality began on 19th September 2017. We will be phasing the roll out of the functionality by area in the coming weeks and months.

What should I do to prepare for these changes?

You should familiarise yourself with the new changes, as outlined in the supporting documentation. Please note that any organisations that are not GP surgeries (with full GMS registration of the patient) may be required to go through the verification/security process for patients registered at their organisation.

As a GP, if you decide that some organisations require the extra verification/security process to record a share-in, you should make sure that patients have as many of the following set up as possible:

- Mobile number
- Email address
- SystmOnline account

CCG / CSU leads may want to review current local sharing configurations and agreements and consolidate the extensive work some have undertaken to correlate with the Allowed list. Creating a pre-agreed list of organisations and organisation types that can be uploaded to the Allowed list will facilitate the process. To help organisations improve and encourage the recording of the communication methods within SystmOne, TPP will be providing useful system wide tools such as patient status alerts and reports.

Does the organisation configuration have to be executed at individual GP practice level or is there an area wide control for a CCG to implement?

It is appropriate that the organisational preferences are determined at that practice. To minimise the administrative burden for our users, a bulk upload tool will be able to be utilised by practices to add organisations easily and en-masse to the *Allowed* list. Therefore, if a CCG wishes to manage sharing organisations centrally and provide a consolidated list for all practices in the locality this still can be achieved by creating an *Allowed* list within SystmOne and uploading this at each practice.

What happens if a patient from the pilot area moves into our area and registers at a new SystmOne GP practice; will the new functionality be enabled in their record as it was during the initial eDSM rollout?

Yes, the new functionality will remain enabled for pilot patients who move GP practice. This will mean that:

- If a patient is using the 'Practice Default' sharing setting at their old practice and then move to your practice, they will inherit your organisation's Practice Default. Until your practice is enabled for the functionality, your practice default will be 'No Organisations Require Verification' i.e. normal eDSM. You will be able to amend this patient's share-in settings on a patient-by-patient basis within their record from the 'Share In Rules' node on the Clinical Tree, but you will not be able to amend your organisation-wide settings until your practice has been enabled during roll-out.

- If a patient is using their own 'Custom' list at their old practice, they will keep their Custom list when they transfer to your GP practice. You will be able to amend this on a patient-by-patient basis within the patient record from the 'Share In Rules' node on the Clinical Tree, but you will not be able to amend your organisation-wide settings until your practice has been enabled during roll-out.

Impact on current sharing

How will my current patients be affected?

Any current registered patients at your organisation receiving care, and have a consent to share-in recorded, will not be affected. The existing shares of this patient's record will continue. The changes will only affect patients where the registered GP or the patient have decided that your organisation is required to complete an extra verification process and the following conditions are met:

- You are recording a share-in consent for the patient ; and

- The patient does not have a previous consent to share in the record at your organisation or the patient previously had a dissent to share in the record.

The Verification/security process is triggered when recording a consent to access the shared record. It **will not** be triggered when setting a dissent to share in or not setting a consent to share in.

Will this affect how I view my patients' data? Will GPs also have to ask for consent in order to view the shared record?

For your GMS-registered patients, the changes will only affect the ability for external organisations to record a share-in, so these changes will not affect how you view your GMS-registered patients' records.

If you are attempting to view patients' records for which you are not the GMS registered practice, you will be subject to these new changes and may be required to complete the extra verification/security process, or be prevented from recording a share-in, by the patient's GMS record owner.

Regardless of what list your organisation is on, you will still be required to record the patient's consent to share out and share in, as per current eDSM rules.

Will safeguarding continue to work in the same way?

Data recorded under the *Safeguarding Information* node will continue to be shared outside of eDSM sharing consents. Information marked as *Safeguarding Relevant* will continue to be affected by sharing consents and so in order to view the information organisations may need to complete the verification process should the patients sharing rules require this. Safeguarding organisations should work closely with GP organisations and CCGs/CSUs to ensure that the correct information is still available to allow them to effectively provide patients with care.

How is sharing between Community units affected?

If your patient's Registered GP is not on SystmOne, sharing will continue under normal eDSM rules.

If your patient's Registered GP is on SystmOne, the patient and/or their Registered GP will have the option to choose that a Community unit:

- Can view the shared out medical record, providing they gain consent; or

- Must go through the extra Verification/security Process, controlled by the patient, in order to view the medical record; or

- Is prevented from recording a share-in preference for the patient.

These settings will affect how organisations can access the entire SystmOne shared record for a patient. For example, if an organisation has been denied access to the SystmOne EHR, (either by the patient's requesting this from the GP, or the patient's GP taking the decision), the Community unit will not be able to access the shared record of any SystmOne organisation caring for that patient.

What is the impact on MIG sharing?

There are no changes to MIG sharing. The eDSM sharing out consent at the patient's GMS practice, and the patient's sharing in consent at the receiving organisation, will govern whether a patient's GP record is shared to the MIG.

Is there any impact on sharing of vaccination data between GP and Child Health units?

No, vaccination information will continue to share outside of eDSM sharing rules for the purposes of Child Health scheduling.

Will special notes still sit outside of eDSM sharing rules as they currently do?

Yes.

How will electronic referrals work? Will the referrer still be prompted to set sharing preferences?

Yes, when creating an electronic referral, you will still be prompted to set the patient's sharing consents for that period of care. Note: that you will be required to verify this patient's consent if the organisation you are referring to is in the patient's Verification list.

What about Consent Override?

The Information Commissioner considers that data recorded on SystmOne has the potential to be made available to all SystmOne organisations and users (subject to N3 and access controls) and therefore it could be disclosed too broadly and beyond the reasonable expectation of patients, because of the widespread user access to the consent override functionality. Therefore, the retention of the override functionality may lead to breaches of the Data Protection Act. As part of the improvements to the sharing controls in SystmOne, the Consent Override functionality will be disabled across all organisations. This is necessary to ensure that the new controls cannot be undermined by the use of the override. The removal has been agreed in collaboration with NHS England and NHS Digital. Users will be notified via a status message when the date of the removal has been agreed.

Are there any plans to reintroduce a break glass function in the future?

NHS England and NHS Digital are currently undertaking a National Strategic Framework review of data sharing for direct care, which is to be system agnostic and working towards future compliance with GDPR. Part of this work includes investigating the use cases for 'Break Glass' functions to meet the needs of safeguarding teams and unconscious patients. This 'Break Glass' function will be made available in SystmOne when the national strategy and implementation is agreed.

If a consultation is marked as private will it not be shared?

Any events marked as 'Private' will only be visible to the organisation who recorded the data as is the case with current eDSM functionality. These consultations will not be shared under any circumstances following the removal of the Consent Override functionality.

What about Organisation Groups and Shared Admin groups?

All forms of Organisation Groups will remain unaffected, meaning if you have access to a patient record through an Organisation Group, this will stay the same.

What happens if a patient's GP practice doesn't use SystmOne?

If a patient does not have a fully GMS record on SystmOne, their record sharing will be controlled by normal eDSM controls, i.e. they will require a consent to share out from the providing organisation and a consent to share in at the receiving organisation.

What happens if a patient shares information with a clinician in a community unit but states that they do not want the GP to know?

Patients can use the normal eDSM controls to determine whether or not to share out their record from the Community unit, and share in at the GP unit.

What about consent override to view the SCR?

Consent Override to view the Summary Care Record (SCR) will not be changing.

Will our organisation still be able to set consent preferences of 'implied' in organisation preferences?

There are no changes to the recording of consent options. The functionality only introduces an additional control of who to share to for GPs. Organisations need to ensure they are complying with other legislation and good industry practice such as the Common Law Duty of Confidentiality and any other obligations surrounding gaining patient consent.

Miscellaneous

Is it available in Mobile Working?

The new sharing functionality is not currently available in Mobile Working. All configuration of the lists must be completed using the full SystmOne client.

For EPR Core units that have an ADT feed, can they be registered without consent?

Units using EPR Core will still have to go through the verification process when attempting to access the shared SystmOne record if they are on the patient's *Verification* list. Information that is shared between other systems using an ADT feed will be unaffected, as this does not rely on eDSM sharing consents.

Have any Out of Hours providers been consulted or involved in this process? Are A & E departments included in guidance for GPs on the allowed list?

TPP have collaborated with many stakeholders including emergency and urgent care representatives from NHS England, NHS Digital, the BMA, the SystmOne National User Group (SNUG) as well as the Royal College of Emergency Medicine and Royal College of Physicians. Individual organisations determine who they are happy to share data to, however we hope that CCGs and emergency and urgent care services will cooperate to ensure there is minimal disruption to patient care.

How do the changes fit with the introduction of GDPR?

The changes have been developed in consideration of the current guidance surrounding the revised data protection legislation. All documentation will be updated to align with the introduction in April 2018 of the General Data Protection Regulation and associated Data Protection Bill.