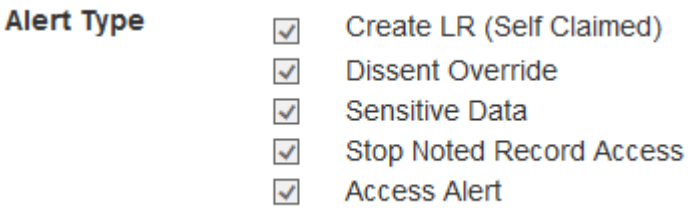
Your emergency care summary

Managing Alerts using the reconciliation tool – Spine 2

The following process is intended to guide privacy officers through the steps of reconciling any Transaction and Messaging Services (TMS) Event Service (TES) Alerts (from the Alert Viewer) using the tool provided on our website, the reconciliation tool.

Alert types

There are several different types of alert that are managed by the alert viewer;



Create LR (Self Claimed)

The alert is generated automatically when a user of the SCRa 2 uses their smartcard role to self claim access to the SCR.

Dissent Override

This Alert is triggered when a user activates the Emergency Access option ***in Non SCRa software***. As best practice the user(s) should have entered some supplementary justification text in the free text box.

Sensitive Data

The alert is generated when an attempt is made to access S-Flagged patient's demographics. S-flagged (or 'Sensitive flagged') records are records that have previously been marked to protect the patients location e.g. domestic abuse or looked after children.

Stop Noted Record Access

The alert is generated when an attempt is made to access S-Flagged patient's demographics. S-flagged (or 'Sensitive flagged') records are records that have previously been marked to protect the patient e.g. domestic abuse or looked after children. *Note that this alert is being removed from alert reporting due to incorrect terminology.

Summary Care Records

Your emergency care summary

NHS

Access Alert

This Alert is triggered when a user activates the Emergency Access option and also if Access for Other reasons is used. As best practice, user(s) should have entered some supplementary justification text in the free text box.

Local PMR data

Run or obtain an extract report from the patient recording system (e.g. Patient Admin System [PAS] or Patient Medication Record [PMR]) for the location you are analysing and for the dates required into Excel or CSV format.

- Run a report to extract patient attendances from the local system for a specific date range (daily, weekly or monthly).
- Save a copy of the data to a clearly labelled and accessible network folder with name identifying the date range. e.g. PAS or PMR 1-1-14 to 31-1-14.
- Delete all columns from the spreadsheet except NHS Number and the date of attendance. The date of attendance is not needed to make the tool work, but is useful when validating an alert.
- Filter NHS Number column to remove any blanks (sometimes blanks appear as the local PAS/PMR does not have the patients NHS Number stored).
    - CTRL F (find and replace) can be used for this.
- Save a local copy for audit purposes. This is the finished copy of admissions data you will use for the reconciliation process.

TES Alert Viewer data

Run the following reports from the alert viewer.

- Create LR (self claim).
- Access Alerts

Create LR (self claimed) Alerts

Create LR (self claimed) alerts are created when an individual accesses a SCR without the assistance of a colleague; because of this there is no role separation and no confirmation that the patient is actually there at this point in time, an alert is generated so the access can be validated later.

Create LR (self claimed) is by far the most populous alert type that most privacy officer will see. Whilst the reconciliation tool was designed to specifically manage these types of alerts it can also be used, with reduced efficacy to start an investigation process for the other alert types.

- Run TES extract report for the dates required ensuring they match the patient recording system report and export into excel.

- Carry out a search on the TES Alert Viewer using the same date range as the admissions data report ensuring that you *un-tick* all the alert type boxes except Create LR (self claimed) Alerts also ensure that Open (new) and Open (Under investigation) are selected.
- Once run, click on the tick box to select all the alerts
- Click the button "Extract All" to download the alerts. A warning message will appear click "OK". The next step will vary slightly depending on internet browser.
- The download/save dialogue box will appear. Click save and name the file using the same protocol used for the PAS/PMR etc report with a name identifying the date range and they are TES alerts. e.g. TES 1-1-14 to 31-1-14 SC. **Ensure you specify a secure location ideally the same network folder used for the PAS/PMR report.**
- Click on OK
- Delete the first 2 rows (these show the file name and column headings).
- Save. This is the finished copy of TES Alert data you will use for the reconciliation process. As a default the Alerts will be in the same order as they were on screen so if you have filtered them they will be in that order

Access Alerts (Emergency Access)

These alerts are activated when an authorised user decides that access to a patients' SCR is required, when a patient is incapable of giving permission. If the location is using the self claimed viewing model then these patients will have two alerts for each episode of care..

- Repeat the steps above but select the different alert type and change the file name

Reconciliation Tool

- Open your master copy of the reconciliation tool which can be found here.
  - Click *File* then *Save as* and rename using the existing protocol to the same network drive location. e.g. Master 1-1-13 to 31-1-13
  - Copy then paste the pas/PMR report NHS number list into the NHS column (cell A2) on the 'PAS or PMR information' tab, date of admission is optional.
  - Copy and paste the data from the TES extracts wholesale into the 'TES Information and Matching' tab within the Alerts Tool, starting from cell B2. Ensure that the NHS Number is within column D.
  - Use the sort on column D in the *TES Information and Matching* Tab to make the NHS number go in descending order

From here, within the 'TES Information and Matching' tab you will be able to see if any accesses have been made to SCRs which are not within the PMR extract and thus require further investigation.

NB: Multiple Alerts of the same type being raised is a known issue, and may be caused by moving backwards and forwards within the application including, using the back button on the browser or by changing Tabs.

Any red entries indicate that there are differences between the TES report and the local PAS/PMR report. This may indicate that an SCR had been accessed and that patient had not been present. These require more detailed investigation.

When running a Create LR (self claimed) match all the green ones displayed have been/were in the pharmacy at the time the two reports specified and can be closed without further investigation. Best practice recommends some entries are subjected to random sampling for verification.

Additional functions within the Alerts Tool

As well as comparing TES Alert extracts against PAS/PMR extracts, the Alerts Tool also performs a number of other functions:

- The 'No. accesses per patient' tab is a pivot table that will list all accesses and group any of the same NHS Number together. This allows for further investigation in cases where a single patient SCR is being accessed an unusual number of times.
- The 'No. accesses per user' tab is a pivot table that will list all accesses and group any of the same user together (using the ORIGINATOR_NAME column). This allows for further investigation in cases where a single user is accessing SCRs an unusual number of times.
- Column AM – 'TIME FILTER' – within the 'TES Information and Matching' tab filters the 'ALERT DATE AND TIME' column by time only. This allows for investigation into cases where SCRs are being accessed outside the normal hours of the pharmacy. The privacy officer will need to reconcile this against the opening hours of individual pharmacies, but by filtering column AM in ascending or descending order, any unusual accesses should become apparent.

Closing Alerts

- Open the TES alert viewer and rerun the original alert search, for the report in question. Select the tick box on the far left hand side of the screen for all the entries that were coloured green in the reconciliation tool. Once they are all selected then select bulk update. A new screen is displayed, from the 1st drop down select the option *Closed – no investigation required* and in the text box please enter the reason why. e.g. Access reconciled with local PAS/PMR.

  If the search is re-run again with the original criteria only the NHS Numbers marked as red in the reconciliation tool should now be visible.

- The NHS Numbers left should match to those listed as red in the reconciliation tool. They should be selected as per the step above, but the option *Open – Under investigation* should be selected from the drop down. The text box should also be filled in with any pertinent info to assist other members of your IG team. Over time as these alerts are investigated, in-line with the organisations existing IG policies then the status should be changed appropriately.

There are various different methods used by organisations across the NHS. What works for your organisation may not suit another. It is therefore left as a local decision what is considered an acceptable process to minimise/mitigate unauthorised access alerts. For example:

- Sorting Access Alerts in order of the individual who created the alert. Then check each user to ensure that additional information detailing the reason why 'emergency access was used' are being added and valid. Missing information is likely to indicate a knowledge gap that may lead to remedial training to ensure that all staff understand what constitutes the appropriate use of 'emergency access' and the importance of the explanation.

- A sample of Access Alerts could be investigated further to ensure that local records validate the explanation given for the use of emergency access.
  The privacy officer may want to look at trends, so creating a local tool that use the Access Alerts and create LR (Self Claim) alerts (which indicate how often an individual has accessed the SCR) to identify individuals who are using the 'emergency access' significantly more than the average for the organisation. This may not indicate misuse as some individuals will work with patient groups more likely to require the use of 'emergency access'.

Once the investigation for SCR dissent override alerts has been completed they can be closed in the same way as the LR (self claimed) alerts.

For further information see:

Process Map for Alert Investigation.pc

http://systems.hscic.gov.uk/scr/implement/ig