360 ASSURANCE

Policy monitoring

Sharing best practice

Contents	

Introduction

In 2019/20, 360 Assurance conducted the Policy Monitoring core audit across our client base, focusing on complaints, mandatory training and temporary IT access. The review was carried out across 16 clients; 11 Trusts and five CCGs.

This benchmarking exercise summarises the themes and key findings of the audits to share best practice. Wherever the results were skewed for either Trusts or CCGs, we have made this clear in the narrative; otherwise the report refers to 'organisations'.

Complaints

The complaints process is a mechanism for patients and families if they would like to raise issues with the care they received. If an organisation has a healthy complaints culture where this direct line of feedback is valued, it is likely that lessons will be learnt, harm reduced and patient experience enhanced.

Complaints policy

It is a requirement that patients know how and where to complain and that organisations have a clear and adhered to complaints policy accessible to staff. All organisations had a policy which included information on how to handle complaints.

On average there was a three year review date for the complaints policy.

There was real variation in where the complaints policy was approved and ratified, varying across groups, committees and boards. There was only one policy that had input from a patient carer group; by doing this users can offer advice on how a complainant expects to be treated.

The key legislation we would expect a complaints policy to refer to is the Local Authority and Social Services and NHS Complaints (England) Regulations 2009 which were referred to in 14 of the 16 complaints policies.

Complaints policy – best practice

- Consider input into the complaints policy from a patient representative or focus group.
- Refer to the 2009 complaints regulations. Also consider referring to:
  - the Parliamentary and Health Service Ombudsman (PHSO) Principles for NHS Complaints Handling (2014)
  - the NHS Constitution 2015.

Complaints process

Of the 16 policies we reviewed, 13 did not state, or were not specific about, what training lead investigators were required to have. In one example it stipulated that the complaint investigator required training and the training compliance should be monitored.

A complaints policy needs to specify what the timeframes are for responses, these varied from 13 to 70 working days; the most commonly-used thresholds were 25-40 days. Timescales were often dependent on the risk rating of the complaint. Three policies did not refer to risk rating of complaints; of the 13 policies that did risk rate complaints, eight linked the response timeframes dependent on the risk rating.

In situations where the complainant is not the patient, obtaining consent may cause delays to the investigation. Only three policies stated that they would “stop the clock” on the response timeframe in this case; three different organisations would begin the investigation before receiving consent without reporting findings back to the complainant until consent was obtained. One policy stated that in cases of patient safety or staff conduct, investigations would take place, even when consent was never provided, for the benefit of learning from mistakes

and improving patient care.

Complaints process - best practice

- The policy should state what training investigators should have and the training compliance should be monitored.
- Consider risk rating complaints and whether the risk rating should impact the response time.
- Review whether a "high" risk rated complaint should be escalated within the organisation as soon as it's received.
- Be clear on how gaining consent impacts on the time to respond and when investigations should be started.

Reporting and monitoring

Most policies set out that complaints should be made to a designated team within the organisation and the total number of complaints received forms part of the monitoring arrangements (15 of the 16 policies).

The following reporting and monitoring arrangements were identified from our review of this section of the policy:

- five stated the time between receipt and acknowledgement should be monitored
- 13 stated achievement of target response times should be monitored
- nine stated the category of the complaints should be reported on
- three stated risk gradings should be reported on.

We noted that, in practice, organisations were generally monitoring and reporting more information than the monitoring requirements set out in the policy.

It would be considered best practice to outline the process for monitoring and reporting complaints within the policy itself, particularly against target timescales.

Across all policies there was no evidence that the monitoring of the data quality of complaints information had been considered.

Reporting and monitoring – best practice

- Incorporate monitoring of the achievement of timescales into the complaints policy.
- Consider monitoring of the data quality of complaints information.

Learning from complaints

All policies stated that action plans should be developed (wherever appropriate) following complaints.

Eight policies stipulated who was responsible for developing action plans; in most cases, this was the lead investigator.

Four policies explicitly stated that action plans following complaints would be tracked through software like Datix or Ulysses. In all other cases specific individuals/groups were named as

responsible for monitoring completion of actions.

Only five policies stipulated that completion of action plans would be monitored; only three of these named the committee/group this information would be reported to.

We identified one point of good practice where a policy stated that if, at any point in the complaints process, a potential risk was identified; it should be immediately added to the risk register for review.

Learning from complaints – best practice

- Clarify responsibilities for developing action plans.
- Specify how action plans will be tracked; consider using existing software to do this.
- Include monitoring of action plan completion.

Mandatory training

Providing statutory and mandatory training is a key investment made by NHS organisations and has an important role in ensuring a high level of safe and effective care to patients.

Mandatory training policy

It is essential for managers and staff in an NHS organisation to know what the mandatory training requirements are to ensure compliance. We found that a total of nine organisations did not use the term 'mandatory training' as the policy title; this is reasonable as long as staff can easily locate the relevant policy when searching for it.

13 policies defined a list of mandatory training courses:

- seven clearly listed the mandatory training courses within the policy, of which three included it as an appendix
- six referred to where a separate list of mandatory training could be located, often on the staff intranet
- the remaining three policies did not clearly refer to a list of mandatory training requirements.

For all policies the review term for the policy was between two and three years. There was less clarity around how frequently organisations review the content of their mandatory training programme:

- For the seven organisations with the list of mandatory training courses included within their policy, it could be implied that these have been reviewed and updated in line with the overall policy review.
- Of the six organisations who maintained a separate list of mandatory training courses, three of the policies explicitly stated this was because the list was frequently reviewed as legislation changed/annual training needs analyses evidenced that changes were needed.

It is best practice to review the content of the mandatory training programme at least as frequently as the policy itself, if not more frequently.

Eight organisations (all Trusts) had declared their alignment to the UK statutory/mandatory Core Skills Training Framework (CSTF) Aligned Healthcare providers and Verified Training Providers; one of these eight did not explicitly refer to this in their policy. However, we found that three out of these eight organisations' mandatory training lists did not agree to those mandated in practice (each was missing one course). Registration on the directory is useful to prevent unnecessary duplication of training as staff move between roles and organisations – those organisations who have submitted a Declaration of Alignment ensure compliance. It should be noted that it is less common but still possible for CCGs to appear on the CSTF directory.

Mandatory training policy – best practice
• If the policy doesn't include mandatory training in the title, ensure it can be easily located on the staff intranet. • Keep a defined list of those courses that are deemed mandatory and include it within, or clearly link it to, the central policy. • Review the mandatory training programme with at least the same frequency as the policy. • Organisations who have submitted a Declaration of Alignment with the CSTF should take steps to ensure their continued compliance with the mandated statutory/mandatory training directory.

Staff compliance

Wherever an employee's role changes, only six organisations defined who should authorise any changes to role training required. In two cases this was automatically completed by ESR, in three by the employee's new line manager, and in one case by the HR department.

Similarly, only two organisations define in their policy the body that can approve the addition or inclusion of mandatory training topics.

Our review found that five policies state compliance with mandatory training forms part of an individual's appraisal.

Wherever an individual has not completed their mandatory training (including essential to role training), organisations had varying consequences. Two organisations stated that pay progression would not be permitted in these cases. Other organisations detailed the following consequences in their policies:

- where an individual fails to submit assignments, complete, or withdraws from a course, the individual may be asked to make a repayment of the financial assistance provided, unless there are exceptional circumstances
- non-compliance with information governance results in IT access being removed
- the performance management policy is enacted
- staff that fail their mandatory training pre-course workbook more than three times will be referred to their line manager as this will be considered a capability issue.

The consequences imposed by organisations are not necessarily punitive but exist to protect the organisation and encourage completion of mandatory training.

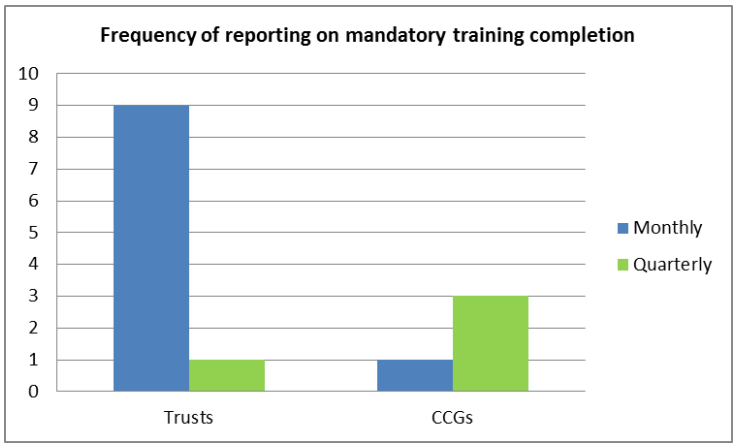
We identified where a Trust specified that formal training has to be completed once every three years, but some training can be completed by validation of learning in practice.

Staff compliance – best practice
• Inclusion of mandatory training within the employee appraisal framework. • The policy should stipulate who authorises/approves changes to employee training requirements whenever they change role. • Enforce appropriate consequences/restrictions in certain areas when mandatory training is not completed. • Consider the possibility of completing training by validation of learning in practice.

Reporting and monitoring

14 out of 16 organisations regularly monitor completion of their mandatory courses – with 10 reporting monthly (of which nine are Trusts) and four reporting quarterly (of which three are CCGs).

In four cases (three of which are CCGs) it was not clear to which committee/group the compliance level is reported.



Only three organisations stipulated their target completion rate for mandatory training within their policy. Six organisations report on the level of do not attends (DNAs) and only two report on the level of cancellations.

One Trust we reviewed had very detailed reports which are reviewed at directorate level looking at compliance against each mandatory training subject and the five compliance areas within each service. We also noted that one organisation monitored the effectiveness of their mandatory training by conducting a quarterly questionnaire on a random sample of staff to gauge their understanding.

Reporting and monitoring – best practice
• Establish a clear monitoring and reporting process, with appropriate frequency and to the appropriate committee/group level. • Monitor and report at divisional level as well as organisational level.

Temporary IT access

It is important that organisations have effective processes in place for controlling temporary IT access. Failure to remove access when an individual no longer needs it is not only poor practice, but could leave an organisation exposed to the risk of fines for failing to protect the data that it holds. The data protection act 2018 requires that data must be processed in a manner that ensures appropriate security, using appropriate technical measures. To comply, an organisation must ensure that only approved and appropriate staff have access to the information that they need (but no more than they require to do their job).

However, managing temporary access is not just about putting in place controls and barriers to getting access to systems and information. It is equally important to ensure that when individuals need access to information, and they have a right to it, that they are granted access accurately and efficiently. If temporary access is not granted (for example to bank staff, interim workers, inspectors etc.) this increases the likelihood of workarounds being used. Examples might be sharing user details or accessing information via another user. This is equally concerning, because the organisation has lost control of who has accessed what. A user allowing another person to share their credentials will almost certainly be in breach of their contract of employment, and potentially the Computer Misuse Act.

To ensure that these risks are understood and managed, organisations should have in place appropriate policies and procedures, setting out how access is granted, controlled and removed.

One Trust held two different temporary IT access policies at two different sites; therefore we undertook this comparison exercise across 12 temporary IT access policies from Trusts and five from CCGs.

Policy governance

There is a general lack of consistency regarding the policies that define IT access. The requirements were set out within Information Security or Network Access policies in just over half of cases. In three cases the organisation maintained a specific Access policy, and in a small number of cases there was no policy that seemed to cover user access requirements.

Ownership of policies varied; five policies approved at Executive/Governing Body level. Half of the policies sat with the Information Governance or Information Security groups, with the remainder approved by general policy and governance committees. Approval by any of these groups is appropriate, so long as steps are taken to ensure this remains an issue on the Executive's radar. The involvement of a Board/Governing Body member (usually the SIRO) within the approving group would be recommended.

Policy governance – best practice
• Organisations should have a policy that covers user access requirements, including detail of arrangements for temporary access. • The SIRO should take part in review of the policy to ensure Executive-level involvement.

Granting access

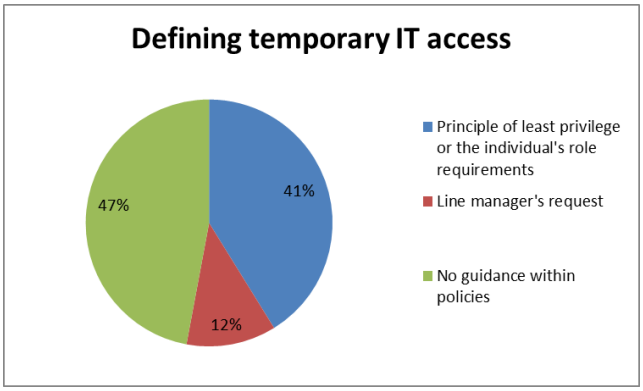
Policies varied in defining who could approve access. Half referred to an individual's line manager. This would seem appropriate, but it is unclear how the status of the line manager would be checked. In a quarter of cases, approval is required from the Information Asset Owner. This would seem appropriate in the context of granting access to a specific system, but is less clear who the Information Asset Owner would be in the context of authorising user access to a network. In two cases, the policy refers to access being approved by System Admin and IT Operations, which would seem to mix up the process of technically *granting access* with the officer *approving* that access.

Granting access – best practice

- The policy should describe how access is granted with a clear description of who can authorise access, including appropriate alternatives if those officers are unavailable.

Defining access

Seven policies referenced that access should be based on a principle of least privilege (ie minimum access required) or the individual's role requirements. In two instances the policy stated that access would be granted on the line manager's request. This would logically request access relevant to the user's role, but is not specified as such. In the remaining eight cases the policies did not provide any guidance or requirements around the access that should be granted.



Defining access – best practice

- The policy should describe how access is granted to ensure that users can quickly access what they need to (and only what they need to).

Removing access

We identified only one policy that we considered to represent good practice in defining the removal of access. This policy stated that any temporary users would be set up with an end date which automatically removed access on that date. There was clear reference to a monthly process of reviewing reports from HR to identify leavers, and a fall-back position of regular checks for any unused account, which would also be suspended and investigated.

Three policies made reference to checking for dormant accounts, but not on a regular basis. Half of the policies mentioned that 'regular reviews should take place' but were unclear regarding who was responsible for this, the precise frequency or how the checks should be

carried out. A quarter of policies did not appear to describe any processes or requirements for removing access.

Removing access – best practice

- The policy should describe the processes and controls to ensure that access is removed or amended promptly when a user leaves, changes role or their circumstances that require access to end.
- For temporary users, access should be set up with an end date so that access is automatically removed when it is no longer necessary.
- The policy should outline who is responsible, and the frequency, for reviewing leavers' reports, dormant accounts, etc. and removing their access.

Respective responsibilities

None of the policies we reviewed clearly identified the respective responsibilities of IT and the relevant department. There is a risk that this contributes to a situation where line managers assume that IT are monitoring user accounts, and IT departments adopt a position where they take minimal action unless requested by the employing department.

Respective responsibilities – best practice

- Roles and responsibilities are defined clearly, both within the employing department and also within the IT department.
- The defined roles and responsibilities should clarify how access is approved and applied, but also the ongoing respective responsibilities for ensuring that user access seems appropriate.