Service Model Policy and Guidance: general guidance

Version 8.0

Quality Directorate

Version: 8.0
Version Date: 1/8/2017

Contents

Introduction

1. The Parliamentary and Health Service Ombudsman's casework process is summarised in the Service Model. This guidance provides information about how our casework staff should operate in line with the Service Model.

2. The Service Charter contains 18 commitments about how we will deliver our service and what people can expect when they bring a complaint to us. The detailed information in the Service Model and this guidance helps us to deliver our service in line with the Charter commitments.

3. The intention of the guidance is to provide an additional layer of detail below the Service Model, with a particular focus on:

    - Requirements from the law (flagged as 'Legal requirement' in the text).
    - Requirements from our own policy (flagged as 'Policy requirement' in the text).

4. Those requirements set the framework within which our casework staff should operate. The guidance is not intended to prescribe the actions or process to be followed across all casework and in all circumstances. Many areas of casework require discretion and judgment and depend on the specific circumstances of the case. Any divergence from the stated requirements in the guidance should be recorded and explained on our case management system, Microsoft Dynamics (MSD).

5. This guidance document is a supplement to the main casework guidance and focuses on subject-specific or cross-cutting subjects. A casework reference library is also available which focuses on specific subject areas within our casework where separate guidance is required.

6. The guidance is a living document and will be updated on a regular basis.

7. The guidance is owned and maintained, on behalf of Operations, by the Quality Directorate.

8. If you have any feedback or questions about the guidance or related issues then please email: ++ServiceModelGuidance@ombudsman.org.uk

1. Assessing risk in casework

Introduction

1.1 We need to identify and manage risk continuously through the life of a case, in order to carry out casework effectively and safely. Everyone is responsible for ensuring that risk is managed appropriately.

1.2 Much of our work is not high risk – most identified risks have potentially low impact and are unlikely to occur. However, given that we cannot anticipate every eventuality, it is vital that we are diligent in our assessment of risk and can evidence a risk based consideration of the information of which we are aware. We need to mitigate any risk identified to the best of our ability.

Summary

1.3 There are eight risk categories (see 'risk category definition' below) to consider at key stages of the casework process in relation to likelihood and impact. The categories provide a broad framework for any particular risks identified. The Case Management System must be updated with the most current risk assessment. It is important to know when and how to escalate matters quickly if an immediate risk is identified.

When to do a risk assessment

1.4 Although risk management is a continuous process, a formal risk assessment is required at four points in the casework process (**policy requirement**):

- When we propose to investigate/decline to investigate (can we/should we look into your case)
- When we confirm the investigation (under investigation)
- When we share the draft decision
- When we decide to do further work following a complaint about our service or decision.

How to assess risk

1.5 The following questions must be considered in relation to the risk categories (defined below) (**policy requirement**):

- Is there a risk? (If so describe the risk in a short statement)
- What is the likelihood of the risk? (high/medium/low)
- What is the potential impact? (high/medium/low)
- How can we mitigate the risk?
- What do you expect the risk rating to be having taken mitigating action?
- What action do we take if the risk we have described happens?

1.6 A case assessed as being either high or medium risk must have a mitigation plan (**policy requirement**). Potential action to mitigate risk will significantly

vary from case to case (and a discussion with colleagues or a manager might help to clarify your thinking), however action in risk mitigation plans should aim to achieve one of two outcomes:

- Reduction (take action to decrease, or eliminate the likelihood or the impact).
- Retention (accept that the risk cannot be mitigated and is outside our control).

Responsibility for case risk and dealing with immediate risk

1.7 Case risk should be managed by the individual allocated ownership of the case.

1.8 If the caseworker identifies a high risk case, this must be discussed with their line manager as soon as possible. If the manager agrees with the risk rating then a mitigation plan should be completed and sent to an Assistant Director for review (**policy requirements**).

1.9 The caseworker should consider who else may need to be made aware of the case (and involved in mitigation planning), for instance colleagues in External Affairs (parliamentary/health policy staff, the press team) or the Quality Directorate (liaison manager).

1.10 If there is an immediate risk, particularly to the welfare of individuals, it must be considered quickly and a decision taken on what action to take (**policy requirement**). Please refer to our policies and guidance on unreasonable behaviour and risks to staff which are available:

- Unreasonable behaviour policy (includes information about risks to staff)
- Disclosing information about risk to a complainant or others

Conflicts of interest

1.11 Conflicts of interest are a relevant consideration in our risk assessment of a case as a conflict (if not identified or acted upon) could be a risk to our ability to carry out our function.

1.12 HR provide policy and guidance on identifying and declaring personal conflicts of interest. Where a conflict of interest exists in relation to the staff involved in a case then this must be reflected in the risk assessment and appropriate mitigation put in place.

1.13 Consideration of potential conflicts of interest should also take into account the declared interests of Board members and those of Directors and senior managers on the corporate register of interests (when available).[1]

[1] Note: The corporate register is in development as of October 2016.

1.14 Where a conflict of interest is identified on a case it must be documented on MSD, either as part of a mitigation plan or in a separate document if there is no mitigation plan (for example, if a conflict is identified but the case remains low risk).

1.15 The completion of a risk assessment means that the member of staff has considered all relevant risk factors, including conflicts of interest.

Risk category definitions

1.16 Assessing these categories should prompt us to consider some of the most common aspects of risk:

- **Risk to physical and/or mental well-being of staff**

This includes anything which could cause harm or unwarranted stress to our staff. For example:

- Explicit or indirect threat of injury or harm.
- History of threats to staff during this or previous complaints.
- Inappropriate or abusive use of social media.
- Unacceptable behaviour towards staff (such as abuse or verbal attacks).

Please refer to the unreasonable behaviour policy for further advice.

- **Risk to professional standing of staff**

For instance, the threat by a complainant or body to refer a person employed by or contracted to us to their professional regulator. This might apply to clinical or legal members of staff.

- **Risk to complainant, stakeholders and third parties**

Examples include:

- Explicit threat of suicide or self-harm.
- History of suicide attempts or self-harm made evident during this or previous complaints.
- Threat of harm to others (such as threats to staff at the body in jurisdiction).
- Potential harm to vulnerable people (such as children, people with disabilities, vulnerable adults or people who require/might require safeguarding).
- Potential impact of revealing previously unknown information (such as unexpected finding of avoidable death).
- A need to maintain complainant anonymity because of third party threats.
- Complainant is a whistle-blower.
- Personal impact on people or organisations who are not party to the complaint (such as the effect of disclosing the actions of an ex-partner

on a Child Support Agency or Cafcass case where there is evidence of an already difficult relationship).
- Potential harm to individual professionals (such as 'named' officers and clinicians) from our activities or findings.

Please refer to the policy on disclosing information about risk to a complainant or others for further advice.

- **Risks associated with the wider potential impact of our decision**

Please check resources such as Horizon Scanning and the Press Cuttings which can be found on Ombudsnet. Examples include:

- Complaint relates to issues which we have identified as strategic or systemic and so may have a significant impact externally.
- Complaint relates to previous publications where we have already publicly stated a view on an issue.
- The complaint is novel (and may be the first of many, and so set a precedent, such as the first complaint about universal credits).
- Casework themes and issues that have been flagged as being of interest or have a context that requires attention.
- The complaint has a finding of avoidable death.

- **Risks to our ability to carry out our function**

Examples include:
- Potential or actual publicity could impact on our ability to investigate in private
- We do not get the cooperation we need from a body or complainant.
- Significant challenge to draft report findings and/or recommendations.
- Required expertise is rare or unavailable – an example of this would be the Edwards Syndrome case where only two people in the country had knowledge and we could use neither.
- Investigating the complaint may pose significant challenges to our resources, capacity and/or costs – an example of this might be an enormous case like Equitable Life.
- Investigation requires sensitive documents to be sought or where we are unable to release information due to sensitive nature etc.
- We are required to change approach or process as a result of statutory change via JR/Litigation – an example of this might be Redmond.
- Conflict of interest of casework staff, senior staff or Board members.

- **Risks associated with customer experience**

For cases where there have been former or ongoing issues with the quality of our service or product. Examples include:

- An upheld review has recommended reopening the case.

- The robustness of a previous decision has been successfully challenged, which has undermined confidence in our process.
- Potential negative publicity is anticipated.
- Significant delays in progressing a case, causing negative impact for customer.

- **Other**

Please note that the categories are not a checklist; nor will they be comprehensive. A category of 'other' is therefore included for any risk factor not captured elsewhere. It is important that any risk is identified, and managed, regardless of category.

- **None identified**

If you have fully considered risk in relation to the information available and decide that no risk is currently present, please select this category.

2. Unreasonable behaviour policy

Policy statement[2]

2.1 We are committed to dealing with all people fairly and impartially and to providing a high-quality service. In order to do this it is important that we are able to communicate with someone bringing a complaint to us so we can make sure we fully understand it. We therefore do not normally limit the contact that people have with us.

2.2 We do not expect our staff to tolerate any form of behaviour that could be considered abusive, offensive or threatening, or that becomes so frequent it makes it more difficult for us to complete our work or help other people. We will take action under this policy to manage this type of behaviour and this applies to all contact with us including the use of social media.

2.3 We will make reasonable adjustments to ensure our service is accessible to everyone. It is important to us though, that we provide a safe environment for our staff to work in, which may mean we decide to restrict how someone can contact us.

2.4 If we consider a person's behaviour is unreasonable we will tell them why and will ask them to change it. If this behaviour continues, we will take action including deciding whether to restrict the person's contact with us. This decision will usually be taken by an Assistant Director[3].

2.5 We will usually only take action to restrict someone's contact with us after we have considered whether there are any other adjustments we could make to prevent unreasonable behaviour from occurring. Any restrictions imposed will be appropriate and proportionate. The options we are most likely to consider are:

- asking for contact in a particular form (for example, email only);
- only allowing contact with a specific member of staff or at specific times;
- asking the person to enter into an agreement about their future behaviour; and/or
- actions designed to specifically meet the needs of the person.

2.6 In all cases we will write to tell the person why we believe their behaviour is unreasonable, what action we are taking and how long that action will last. We will also tell them how they can challenge the decision if they disagree with it.

[2] Paragraphs 1-8 are the policy statement that should be sent to a person when a warning is applied. This text should also be used for the policy statement on the website.
[3] All decisions in this policy can also be agreed by members of staff who hold roles at a more senior level than referred to.

2.7 If, despite any adjustments we have made, a person continues to behave in a way which is unreasonable, we may decide to end contact with that person.

2.8 There will be occasions where we decide that a person's behaviour is so extreme that it threatens the immediate safety and welfare of our staff or others. In these instances we will consider stopping all contact immediately, reporting what has happened to the police or taking legal action. In such cases, we may not warn the person before we do this.

What is unreasonable behaviour?

2.9 Unreasonable behaviour is difficult to define and will usually depend on the situation of the individual concerned. It can occur in a variety of circumstances including in person, on the telephone, in written correspondence or on social media (see paragraph 2.71).

2.10 Any behaviour that makes someone feel uneasy, uncomfortable, distressed, anxious or unsafe is likely to be considered unreasonable and action can be considered under the policy in these instances. Examples include behaviour that a staff member considers abusive, offensive or threatening in nature.

2.11 We should also consider taking action under the policy where a high frequency of contact causes a disruption to the service we provide. For example, a series of disruptive calls which contain no abusive content may be suitable for action to be taken under this policy as much as a single call which contains a specific threat.

2.12 If at any stage we consider a person's behaviour poses an immediate threat to the health, welfare or safety of staff then we should decide whether more immediate action is required. Further information about what action to take is available at paragraph 57.

<u>Considering equality issues in deciding whether to take action under the policy</u>

2.13 The staff member must take into account any equality issues that may affect a person's behaviour before deciding whether to take action under the policy. This should include reviewing any adjustments currently in place and deciding whether any further steps could be taken to manage the person's behaviour. Any changes should be recorded on MSD.

2.14 If we decide to make further reasonable adjustments we should clearly record what we have agreed to do in the accessibility issues section on the complainant's MSD record as well as in the task section of the complainant's current case. **(Policy requirement)**

2.15 If the staff member considers further adjustments cannot be made to support the person, or their request for adjustment is unreasonable, then the reasons for this decision must be recorded on MSD and discussed with the Legal

Team. If the staff member has any concern about deciding that a requested adjustment is not reasonable, they must consult their manager, and also the Legal Team if appropriate. **(Policy requirements)**

2.16 A staff member can still take action under this policy even if a relevant equality or diversity issue is identified. They must take account of any reasonable adjustments agreed in deciding what action to take. **(Policy requirement)** For example, a dyslexic complainant may only want telephone contact. We may therefore decide to limit their contact to one person, rather than restrict all telephone calls to us.

Recording unreasonable behaviour

2.17 The staff member should log full details of any behaviour they consider to be unreasonable on the tasks section of MSD. This record should include details of why they consider the behaviour is unreasonable and details of, for example, any offensive terms used. **(Policy requirement)**

2.18 The staff member should record the exact language used in the contact and give as much information as possible about how and when it was used. This should not only include what someone said or did but the way they spoke and how they acted. They should also create a new record for each telephone call to capture the frequency of the contact. **(Policy requirement)**

The process

2.19 Staff members should complete each stage of the process below before moving to the next and should only take further action if the person's behaviour continues to be unreasonable. **(Policy requirement)** A diagram of the process is also available in annex A.

- Tell the person that we consider their behaviour to be unreasonable and why.
- Consider if a new or existing advocate can be used to communicate with the person as an alternative method of communication.
- Issue a warning with the agreement of a manager and provide details of our policy.
- Escalate to an Assistant Director to consider applying the policy.

Tell the person that we consider their behaviour to be unreasonable and why

2.20 The staff member who has experienced the unreasonable behaviour should usually be the one to challenge it. This is because they are in the best position to explain why the person's behaviour is unreasonable.

2.21 The staff member should tell the person involved that they consider their behaviour unreasonable, explain why, and give them the opportunity to stop. (This explanation can, if necessary, be given at the same time as a warning about the potential application of this policy.) They should also ask the person

at this time if there is a way we can adjust our service to help them. **(Policy requirements)**

2.22 If for any reason the staff member feels uncomfortable in challenging the person's behaviour at the time, or is concerned their personal safety is at risk (particularly if the behaviour is threatening or occurs in a face-to-face setting), they should record any details of the person's behaviour and discuss what happened with their manager as soon as possible. The staff member can still contact the complainant to discuss their behaviour after the telephone call if appropriate.

Examples of when and how to challenge unreasonable behaviour

2.23 If a person uses offensive language during a telephone call the staff member involved should explain to the person that their language is unreasonable and ask them to stop. If the person refuses to comply with that request the staff member should politely end the call. A record should be made on MSD of what has happened and the telephone call should be discussed with a manager.

2.24 If a person uses offensive language in letters or emails, the staff member should explain in their next written response to the person that the language they have used is unreasonable and ask them not to repeat this in future correspondence. Examples of sample letters are available in annex B.

2.25 If a person persistently makes repeated telephone calls without legitimate purpose (for example, to ask about progress on their case when they have recently been given that information) the staff member involved should explain to them that their behaviour is disruptive and is preventing work on their case and others. They should ask the person to stop doing this. If the person refuses to comply with the request then in the short term further calls can be terminated politely after a brief explanation (for example, that we have nothing further to add to the last update given on the case). If the behaviour continues the staff member must take action under the policy and should not continue to just terminate calls. **(Policy requirement)**

2.26 If a person sends repeated letters or emails without legitimate purpose (for example, if they send one letter each day that does not add anything to the evidence in support of their case) the staff member should ask, in their next contact with the person, that they limit the amount of correspondence sent to us.

Consider if a new or existing advocate can be used to communicate with the person

2.27 If a person displaying unreasonable behaviour has an advocate, the staff member should approach them as soon as possible to ask for assistance in understanding and managing the person's behaviour.

2.28 If the person does not have an advocate, the staff member should, if appropriate, suggest they get one and provide details of a suitable provider.

This may be particularly suitable in cases where there are equality considerations. **(Policy requirement)**

Issue a warning with the agreement of a manager[4] and provide details of our policy

2.29 A warning will normally be given before the policy is applied. This is different to telling the person their behaviour is unreasonable. The staff member will usually have already told the complainant why their behaviour was unreasonable and given them the opportunity to change.

2.30 The staff member should consider the most appropriate way of giving the warning, whether this is telephone, email or by post. The staff member should also record the warning on MSD. This must include a summary of the reasons for the warning, and the manager it was discussed with. **(Policy requirement)**

2.31 If the warning is communicated over the telephone the staff member should also send the person concerned either a copy or a link to the policy statement via email or writing (paragraphs 1-8 above are available on PHSO's website). This should be accompanied by a brief letter reiterating the warning and if appropriate a statement of our willingness to discuss a reasonable adjustment if helpful. **(Policy requirement)**

2.32 The staff member involved should usually deliver the warning as they are best placed to explain why the complainant's behaviour was unreasonable. Another staff member can do this though if appropriate. The warning should explain what the behaviour was, why we consider it to be unreasonable and the likely consequences of any continuation.

2.33 The staff member should usually discuss the decision to issue a warning in advance with a manager. There will be occasions when a person's behaviour (usually during a telephone call) requires a staff member to issue a warning without being able to discuss the case with a manager first. In these instances the staff member should inform their manager as soon as possible after the event. **(Policy requirement)**

2.34 If a Member of Parliament and/or representative have been involved in the case, the staff member should tell the person that, if the unreasonable behaviour continues and we decide to apply our policy, that we will tell the MP and/or the representative. **(Policy requirement)**

2.35 If the staff member considers the person's behaviour is particularly serious (for example, there has been a specific and immediate threat made) a decision may be taken by an Assistant Director to apply the policy without prior warning. In that event, the staff member who authorises the application of the policy should contact the person immediately explaining the reasons for doing this. **(Policy requirement)**

[4] If the member of staff dealing with the case is a manager at grade 2 or above, then they do not need the agreement of their manager before issuing a warning.

2.36 The staff member should also consider whether the Security Officer should be informed. This will mainly be relevant when the staff member feels threatened by the person's actions, for example a threat is made to come to our offices.

Recording a warning on Microsoft Dynamics

2.37 The staff member should record the warning on the 'alerts' section of the customer record. They should enter details of the warning and the manager who agreed it. This will appear on a banner at the top of the case screen and on the customer record. Restrictions applied will only normally apply to an individual and therefore to their contact on any cases they have with us. The staff member will therefore need to specify if the restrictions only apply to one case. **(Policy requirement)**

2.38 Information about how to record a warning, decision and review on Visualfiles is available in Annex D.

Escalate to consider application of the policy

2.39 If the person continues to behave in a way that is unreasonable, a request to apply the policy should be referred to an Assistant Director. The staff member should ensure the request provides relevant details (for example, steps taken so far, nature and frequency of the behaviour, information about the complainant's needs and circumstances (if known), and the type and duration of any proposed requirements or conditions). **(Policy requirement)**

2.40 In deciding whether to apply the policy the relevant manager should consider and record on the task section of MSD; **(Policy requirements)**

- The requirements/conditions for the person to follow in order to manage their behaviour.
- Whether there are any equality or diversity considerations that may impact on the requirements/conditions agreed.
- Advice and support to any staff members who receive contact from that person.
- Date for review of requirements/conditions.
- Responsibility for handling requests for review of requirements /conditions.

2.41 The staff member should record the outcome of the referral on MSD and detail the reasons why it has been agreed or not agreed that the policy should be applied. This should include whether restrictions need to apply to any other existing enquiries, reviews, investigations or information requests that the person has with us. **(Policy requirements)**

2.42 If it is decided that the policy should not be applied then the manager who considers the request should decide how to manage contact from the person in the future and record this on MSD. **(Policy requirement)**

2.43 If it is decided the policy should apply, the manager considering the request should agree how to restrict the person's contact with us. In doing this they

should balance the interests of the person with the duty to protect the health, safety and welfare of staff. **(Policy requirements)**

2.44 Possible actions include:

- requesting contact in a particular form (for example, emails only);
- requiring contact to take place with a named officer;
- restricting telephone calls to specified days and times;
- asking the person to enter into an agreement about their conduct; and/or
- actions designed specifically to meet the needs of the person.

2.45 When applying a restriction then the manager considering the request should set a date when it will be reviewed. This date should be recorded on MSD. This will not be more than 6 months after the restrictions are imposed. **(Policy requirement)**

2.46 The manager applying the restrictions should contact the person and explain:

- the reasons for the decision;
- the requirements/conditions the person must follow and any adjustments that can be made to assist with this;
- the date set for review;
- how the person can challenge the decision;
- a warning that continued unreasonable behaviour may lead to the case being closed; and
- where relevant, that the MP/representative has been told of the action.

2.47 The manager should preferably make this contact by telephone. If they are aware that the person has a preferred method of communication then contact should be made this way instead. This contact must be followed up in writing. **(Policy requirements)**

Recording the application of the policy and restrictions on Microsoft Dynamics

2.48 The staff member should record that the policy has been applied and the restrictions under the 'alerts' section of the customer record. They should also include details of the manager who approved the decision and the date the restrictions should be reviewed. **(Policy requirement)** This will now appear on a banner at the top of the case screen and on the customer record. The staff member will need to specify if only applying the policy to only one of multiple cases.

2.49 The staff member should set up a task to alert them when the policy is due for review. If they are no longer the staff member dealing with the person on this date then they should contact the staff member currently dealing with the person to inform them a review is due. **(Policy requirements)**

2.50 The staff member who is currently dealing with the person (or their case) is responsible for keeping the case record updated about the application of the policy. This includes where restrictions on contact are altered, varied or removed. **(Policy requirement)**

What if contact restrictions that have been applied are not complied with?

2.51 If a staff member receives a telephone call from a person who has been informed they cannot contact us this way, they should explain the restriction to the complainant. They should politely ask the person to contact us using an alternative method or via an advocate. The call can then be terminated. **(Policy requirement)**

2.52 If a staff member receives a letter or email from a person who has been informed they cannot contact us this way, then they should explain this restriction to the complainant (this can be in writing if appropriate). They should then ask the person to contact us using an alternative method or via an advocate.

What if unreasonable behaviour continues after the policy is applied?

2.53 If the person continues to behave unreasonably after the policy has been applied, then the manager of the staff member currently dealing with the person should decide whether further restrictions are required. They should ensure that any changes made are recorded on MSD as soon as possible. **(Policy requirement)**

2.54 An Operations Director can decide to terminate contact with a person completely if appropriate (which would also have the effect of closing or discontinuing any assessment, investigation or review consideration currently ongoing). The intention of this policy though is to manage challenging behaviour so we can continue to work on cases. This should therefore only be considered in rare circumstances. If the decision is made to do this then this should be recorded on MSD. **(Policy requirement)**

2.56 If the decision is made to terminate contact completely, then the manager of the staff member currently dealing with the person should decide whether to acknowledge or consider any further contact. This should be considered on a case by case basis and any action taken must be recorded on MSD.

Complaints about decisions to apply the policy

2.57 The Customer Care Team can consider complaints about whether the policy has been applied in line with this guidance. If the process has not been followed correctly, the Customer Care Team should pass the case back to the manager who applied the policy and ask for it to be reconsidered. The outcome should be recorded on MSD. **(Policy requirement)**

2.58 If the complaint concerns our decision to apply the policy, the complaint should be forwarded to the manager of the manager who agreed the

restrictions to review. The member of staff carrying out that review must issue a written decision to explain the outcome and record the decision on MSD. **(Policy requirement)**

Behaviour that poses an immediate risk

2.59 There will be exceptional cases where we consider a person's behaviour poses an immediate threat to the health, welfare or safety of staff members. In these cases an Assistant Director may decide to take action without prior warning, including terminating all contact. They may also consider other suitable action such as police involvement. **(Policy requirement)**

2.60 The staff member taking this action must clearly record what action has been taken on MSD and their manager and the security officer must be notified. **(Policy requirement)** A risk assessment template and guidance on completing a risk assessment are available (see Annex C for details).

Modification of behaviour

2.61 If a staff member considers the person has modified their behaviour before the review date to the extent that existing restrictions should not apply, a proposal to remove or modify the restrictions can be agreed by an Assistant Director.

2.62 If restrictions are removed on a person's contact with us before the review date set the staff member should contact the person to explain this. At this time they should also make it clear to the person that if their previous behaviour resumes this could lead to restrictions being imposed again or further restrictions imposed. **(Policy requirement)**

Deciding whether to continue applying the policy at the review date

2.63 The staff member who currently holds the case has the responsibility for ensuring a review is conducted (including cases that are held by the Customer Care Team).This is because they are best placed to comment on whether the person's behaviour has changed and restrictions should be lifted. **(Policy requirement)**

2.64 Before the review date the staff member should discuss the case with their manager and pass it to an Assistant Director to review. **(Policy requirement)**

2.65 The person reviewing the case should take into account the evidence and reasons for making the original decision, and any evidence of the person's subsequent behaviour. They should also seek comments from appropriate staff, including those affected by the behaviour, and consider the effectiveness of any adjustment already made. **(Policy requirement)**

2.66 If the person reviewing the case decides not to extend the original restrictions for a further period, the conditions imposed will lapse. This

decision should be recorded on MSD and the alert should be removed from the case.

2.67 If there is continuing contact with the person, the person reviewing the case should write to them explaining the decision. If the person is not in regular contact then contact does not need to be re-established to tell them about the decision. The decision should then be shared if and when they make contact again.

2.68 If the person reviewing the case does not extend the original decision and the unreasonable behaviour occurs again at a later point they can decide to enforce the previous restrictions again without going through the warning stage.

2.69 If the person reviewing the case decides to extend the original decision, they should set a further period during which restrictions should apply up to a maximum of twelve months. When this expires, a further review should be conducted. **(Policy requirement)**

2.70 The review of the application of this policy should be recorded fully on MSD by (or on behalf of) the person carrying out the review. The alerts box should then be updated to reflect any decisions made. **(Policy requirement)**

Social media

2.71 We generally consider unreasonable behaviour on social media (for example, Facebook or Twitter) to be when a person is abusive, makes personal threats or repeatedly references an individual member of staff. We should not usually take action under this part of the policy if the comment is a general criticism of our organisation or service.

2.72 If a person displays unreasonable behaviour on social media then this policy can be used to try to manage it. In these circumstances the staff member responsible for responding to the person should not continue to respond online, in order to prevent personal or confidential information (either about a case or about a member of staff) being disclosed or publicised further.

2.73 If a social media post about a specific member of staff is found online, then this should be referred to the relevant staff member's manager, human resources and the Digital Communications team. The manager should inform the staff member and take responsibility for agreeing what action to take, working with the Digital Communications team and, if appropriate, the Legal Team. **(Policy requirements)** The following options can be considered:

- support for the employee (including employee assistance programme);
- asking the person who made the post to remove it; (discuss this with the Digital Communications team first)
- asking the Digital Communications team to report the person to the social media platform (if the behaviour persists);
- seeking advice from the Legal Team.

Contact received on staff member's personal social media

2.74 Most comments we receive on social media will be made to our corporate accounts. Action can be taken under this policy though in relation to contact received from a person that is sent directly to a member of staff's personal social media account.

2.75 If a staff member receives contact through social media from a person who is currently, or has previously, used our service then they should raise this with their manager. The staff member should not respond to the contact or acknowledge the person has a case with us, as this may be considered a breach of data protection. **(Policy requirement)**

2.76 If this contact is threatening or abusive the staff member should report it to their manager as soon as possible. The manager should then consider whether action is required under this policy. **(Policy requirement)**

Further complaints and information requests

2.77 Restrictions under this policy should usually be applied to an individual. We can still decide to apply restrictions on a case-specific basis if appropriate. **(Policy requirement)** This should be considered on the individual circumstances of the case.

2.78 If a person who has had restrictions applied under this policy seeks to make a fresh complaint, the staff member should consult an Assistant Director for a decision on how to respond to that further contact.

2.79 If a person who has had restrictions applied under this policy makes a Freedom of Information request or Data Protection Act subject access request then an Assistant Director should be consulted for advice as well as our FOI and Legal Teams. **(Policy requirement)**

Variation of these procedures

2.80 These procedures may be varied in individual circumstances or on a specific issue by agreement with a member of staff at director level.

3. Disclosure of concerns about the health and safety of patients – section 15 Health Service Commissioner's Act 1993

Legislation

3.1 Section 15(1)(e) of our health legislation[5] gives us the power to disclose information to any person we consider relevant, if it is clear there is a likely threat to the health and safety of patients. (**Legal requirement**) Therefore if, during our consideration of a health case[6], we discover any information that would indicate a likely threat, we should consider whether disclosure of those concerns might be appropriate.

3.2 Once we have made the disclosure, the law[7] says we must ensure both the person supplying us with the information, and the subject of that information are told we have made a disclosure, and who we have made it to. **(Legal requirement)** The relevant section from the legislation is at Annex E.

Background

3.3 We should consider making a disclosure in any situation where we have reliable evidence that leads to us having concerns about the actions or behaviours of an individual or organisation. Before deciding to make a disclosure though we must ensure we have sufficient evidence to conclude there is a likely threat to the health and safety of patients. We must also make sure any disclosure we make is proportionate in relation to what has happened or might happen. **(Policy requirements)**

3.4 If we do decide to make a disclosure then this should always be to a relevant person or organisation that has the powers and responsibility to handle the information provided and take action. **(Policy requirement)**

3.5 We should also only disclose the minimum amount of information needed in order to respond to the threat and should not provide details of any case we are considering that is linked to the disclosure, unless directly relevant. **(Policy requirement)**

3.6 We should disclose information at any point we consider it necessary. We do not need to wait until the end of a case but should ensure we take a fair and reasonable approach. **(Policy requirement)**

3.7We do not have the same powers under our parliamentary legislation, and therefore any consideration of whether to disclose information for these cases

[5] Health Service Commissioners Act; 1993 section 15(1)(e)
[6] Note: This is not restricted to investigations only. The Act refers to information obtained 'in the course of or 'for the purposes of' the investigation. This therefore may include information obtained in Customer Services or review stage.
[7] 1993 Act, section 15 (1)(c)

must be considered under our disclosing information about risk policy[8]. **(Policy requirement)**

Disclosing information concerning the actions of a clinician

3.8 It is likely that most of the disclosures we make under section 15 will concern the actions of clinicians. This has potentially serious implications for the individual concerned and therefore it is important that we are fair and consistent in deciding whether to make a disclosure.

3.9 Before making a disclosure we should consider whether our concerns could instead be dealt with through discussions with the employing or supervising NHS organisation involved in the complaint as part of our usual casework process. We should also consider that findings and recommendations made during an investigation will already be shared with the responsible organisation. **(Policy requirements)** If we partly or fully uphold a complaint about a doctor, then an anonymised version of the final report will also be shared with their responsible officer[9].

3.10 There will be occasions when we decide information should be reported to a regulatory or other external organisation or to other individuals. For complaints about clinicians this is likely to be their regulatory organisation. (We do not refer individuals to their regulatory organisation or employer; we share information with them.)

3.11 In some instances, the threat to patients will relate more to their health than to their safety. For example, in dentistry, serious mistakes may not be life threatening, but may affect the oral health of patients. In these cases, we can still share information under section 15.

3.12 We can decide to make disclosures to the police, but should only consider doing so in the most serious of cases. This is likely to be where the incident concerned and the potential risk to patients is likely to amount to a criminal offence.

Disclosing information concerning the actions of others

3.13 Section 15 allows us to release information to **any persons** and there may be a number of circumstances in which we could release information lawfully to other bodies or individuals (for example, to a public inquiry). We can also disclose information about more than one individual to more than one organisation at the same time.

[8] Our Disclosing information where there is a risk to the health and safety of a complainant or others policy is available in section 4 of this guidance.
[9] An individual within a designated organisation (usually the doctor's employer) who is responsible for helping the doctor with their revalidation (affirming to the GMC that they are up to date with training and fit to practice).

3.14 If the Caseworker is unsure about whether information can be disclosed under section 15 then they should escalate their concerns to a Manager and the Legal Team before taking any action. In circumstances where a disclosure needs to be made urgently and a manager or the legal team is not available, the staff member can still make a disclosure. They must discuss the case with a manager as soon as possible though following the disclosure being made.**(Policy requirement)**

When a disclosure may be appropriate

3.15 The decision to make a disclosure will need to be determined by a balanced judgment taken in light of the circumstances of the individual case. We should not be making disclosures just because we are making an adverse finding.

3.16 We should also consider whether there are any wider systemic issues that need to be looked at before making a disclosure. **(Policy requirement)** For example; we receive several complaints in relation to a cancer unit at a particular hospital that may indicate a wider issue. This can be done by speaking to Managers and Assistant Directors and checking the Horizon Scanning Newsletter for any current and relevant systemic themes.

3.17 Below are some examples of the types of situations which we may decide are serious enough to warrant making a disclosure:

- the specific incident giving rise to the complaint is so serious that there are justifiable concerns about the potential risk to other patients if the matter is left 'unreported' (for example, issues of significant professional incompetence) – this could also relate to concerns about record keeping, such as inaccurate information in the medical records;

- the incident is not an isolated one (for example, if there have been other complaints against the practitioner concerned where we have identified similar service failings, perhaps on a related theme);

- an individual's ability, knowledge and experience in relation to the matter involved is significantly lacking or their attitude is inconsistent with relevant standards and established good practice – again this can relate to record keeping;

- the individual or organisation has not 'learnt lessons' from earlier complaints, is generally defensive (including failure to co-operate with the complaints procedure) and is likely to repeat similar serious failings;

- concerns relating to complaint handling and/or internal review/investigation of a specific incident – despite not being directly involved in care and treatment. (For example, we have disclosed information about clinicians under section 15 because of their failure to pick up on serious mistakes and/or take appropriate action as part of an internal review or investigation);

- the individual has failed to meet the relevant standards of conduct, for example in terms of honesty and integrity; for example, the falsifying of evidence;

- the individual has no on-going accountability to the NHS, so that the risk to patients from misconduct or poor practice is increased to an unacceptable level by a lack of suitable governance or supervisory arrangements, which may create a risk that further problems may not be identified; and

- if we find evidence to suggest that a practitioner has breached a conditional registration imposed by a professional organisation (for example, one of the sanctions available to both the GMC and GDC if they find that a practitioner's fitness to practise is impaired is to impose conditions on their registration for up to three years).

3.18 This list is not exclusive and it must be emphasised that a decision to disclose such information occurs only in a small number of cases.

The process

3.19 Where it is felt that a disclosure under section 15 might be appropriate, the following steps should be completed. **(Policy requirements)**

- The Caseworker should discuss the case with their Manager to decide whether a disclosure may be appropriate. They should then record this discussion in detail on MSD and cross-reference the relevant evidence and advice (including clinical).

- The Caseworker should review the case risk rating on MSD and ensure that any mitigation plan is up to date. Whether the risk rating needs to be changed will depend on the individual circumstances of the case, however both the risk rating and any mitigation plan should be regularly reviewed. (**Policy requirement**)[10].

- Details of the case should be escalated via line management to an Assistant Director to decide if a disclosure should be made (and simultaneously copied to the Legal Team who should be invited to comment) in line with the Delegation Scheme. The letters containing the information for disclosure should also be signed off at this level or above.

- The Caseworker should consider telling the subject of the disclosure that we are proposing to share information about them with a third party **before** doing so. There will be instances where this will not be appropriate, such as when a disclosure needs to be made urgently.

- This approval should be clearly recorded on MSD. We should disclose the minimum amount of factual information needed to mitigate the risk to the

[10] The guidance for risk ratings is available in section one of this document.

minimum number of organisations. This includes limiting any case specific information we provide to what is necessary to explain the reasons for the disclosure. If a disclosure is made to a professional organisation (for example, GMC, GDC, NMC) then this should also be recorded on MSD.

We can make the disclosure by telephone or in writing. If we use email, we should ensure that the person we are disclosing information to will read it promptly (for example, by asking them to confirm receipt or alerting them by phone to the information that we are sending). We should also follow the requirements of the protective marking scheme (for example, ensuring that documents are sent securely through Egress[11]).

- If we have not already done so, we must ensure we meet our legal obligations by informing the person involved that we have made a disclosure and who we have made it to. We must then inform the person who provided us with the information that we have shared it. **(Legal requirement)**

- The details of the disclosure, including the reasons why it was made, should be sent to the Operational Improvement Team to add to the Section 15 disclosure registry.

- The exact sequence of events will be determined by the nature of the case. The key requirement is that any case which has the potential to result in disclosure under section 15 is identified and escalated at an early stage.

When to disclose cases and how

- In investigation cases, we usually disclose the relevant information at the same time as we issue our final report by copying an anonymised final report to the regulatory organisation or other organisation/person. However, a disclosure of information can be made urgently if necessary before the investigation is completed.

- In investigation cases where the person we are disclosing information about would not normally receive a copy of the final report (for example, if they were not listed as a 'named person') we should still send them a copy of the final report[12] in order to meet the obligation to inform the subject of the information being disclosed. **(Legal requirement)**

- There will be occasions where we decide not to investigate a case, or are still considering what action to take, but still want to disclose information. The same process applies, but we should be careful to ensure we only share information about the complaint that is necessary in order to make the disclosure.

[11] Further information is available at the following link: How to send a secure email in outlook using Egress
[12] 1993 Act section15(1)(B)

- Disclosures should usually be made at the same time we issue our decision. A disclosure can be made before then though if necessary. We must ensure we meet our legal obligations by informing the person involved we have made a disclosure and who we made it to. As well as informing the person who provided us with the information that we have shared it. **(Legal requirement)**

Section 15 cases where there is an immediate risk to a patient

3.20 There will be circumstances where there is an immediate risk to the health and safety of a patient which requires us to disclose information straight away.

3.21 In instances where an Assistant Director or above is not available, an Operations Manager,[13] Head of Information Assurance or Head of Legal, can, exceptionally, approve the disclosure. This approval will include agreeing the organisation(s) to which we are disclosing the information (for example, the police, mental health crisis team, social/support worker, GP, other emergency services and so forth).

3.22 It is unlikely that a staff member will have to act alone when considering or making disclosures but, if there is a serious and immediate threat to an individual and an Assistant Director, Operations Manager, Head of Information Assurance or Legal cannot be contacted immediately, a staff member may make the disclosure without prior authorisation. **(Policy requirement)**

3.23 In any circumstance where an Assistant Director is unable to approve a disclosure before it is made, the staff member must notify them as soon as possible afterwards. They should record their discussion with the Assistant Director and relevant information about the disclosure on MSD.

3.24 If an immediate disclosure is approved, then we must inform the subject of the disclosure we have made it as soon as practically possible to meet our legal obligations. **(Legal requirement)** An Operations Director should also be informed that a disclosure has been made.

Compliance

3.25 The disclosure of concerns under section 15 is a process we follow when we consider it necessary. It is not a remedy for the complainant and there is no obligation on the organisation or person we have disclosed the information to, to tell us the outcome of our disclosure. Once we have made the disclosure, our involvement ceases. Therefore, there is no need to record the disclosure as a compliance item or create a compliance plan.

[13] An Operations Manager is any member of staff at grade 3 or above who manages a team within the operations directorate.

4 Disclosing information where there is a risk to the health and safety of a complainant or others

Introduction

4.1 This guidance explains what to do if you receive information that indicates there may be a risk (that is the probability of harm being caused) to a complainant or others (this includes children or vulnerable adults) and the situation may require us to disclose that information. The legal background contained in this policy is available in annex F and a process flow chart in annex G.

4.2 The guidance covers two main situations:

- We receive information which indicates that a complainant or someone else is at risk (or is likely to be put at risk) and we need to consider a prompt disclosure in reaction to this information. For example, a complainant threatening suicide or making a threat against others over the telephone.

- Our knowledge of the complainant's circumstances means that we make a proactive assessment that there may be a risk to a complainant or others. For example, a risk may arise when we send a decision not to investigate to a complainant with a history of self-harm, or a complainant might threaten to harm their GP if we do not investigate their complaint.

4.3 Section 14 (2I) allows us to share decision letters or investigation reports in health cases with any person we consider appropriate[14]. We would not generally use these powers to disclose information about risk. This is because we are unlikely to share whole decision letters or reports for the purposes of alerting others to risk. The specific type of information we want to release is also unlikely to be included in these documents.

4.4 We can disclose information under section 15 of the Health Service Commissioner's Act when it relates to a likely threat to the health and safety of a patient[15]. Section 15(1)(e) only deals with situations in which we have obtained information in the course of, or for the purposes of, a health investigation[16], and that information constitutes a threat to health and safety of patients. When we make disclosures this way, we are doing so lawfully and therefore should consider whether information can be shared using section 15[17].

4.5 There is no equivalent provision in the Parliamentary Commissioners Act 1967 that allows us to disclose information lawfully. This policy should therefore be

[14] 1993 Act, section 14 (2I).

[15] 1993 Act, section 15 (1)(e)

[16] Note: This is not restricted to investigations only and may include information obtained in Customer Services or review stage.

[17] The guidance for making these decisions is available in section 3 of this document.

used if we want to share information with others that is obtained for the purposes of a parliamentary investigation. **(Policy requirement)**

4.6 If a staff member is unsure under which policy to disclose information then they should discuss this further with a manager and the Legal Team before taking any action. In circumstances where a disclosure needs to be made urgently and a manager or the Legal Team is not available, the staff member can still make a disclosure. They must discuss the case with a manager as soon as possible though following the disclosure being made. **(Policy requirement)**

4.7 Any action taken under this policy should be fully recorded on MSD for our audit trail. **(Policy requirement)** The MSD entry should include the exact information we were given, the advice we followed when we decided how to act and the action we took as a consequence. It may be necessary to record these details after the event because of the immediate nature of some threats.

4.8 This policy does not cover the management of threats made to staff members. This is covered in the unreasonable behaviour policy[18].

Identifying risks

4.9 Information about risks may come from different sources, including telephone calls, emails, letters, social media and medical records. You should only consider disclosing information in the most serious circumstances. **(Policy requirement)** Some of the key points to think about[19] are:

- Is there a realistic risk to the individual or others? (It is not necessary to prove that the risk is valid, but we must be able to show that there are sufficient grounds for concern. A discussion with your manager may be helpful when you assess the risk.)

- Does the individual have past history which suggests that they are likely to be at risk or be a risk to others? (Although a past history of, for example, suicide attempts may put an individual at greater risk; the absence of past history does not mean that the risk is diminished.)

- Do we have clinical evidence which indicates that the complainant is likely to be at risk or be a risk to others?

- Can we identify an appropriate individual or organisation to disclose the information to in order to mitigate the risk? This must be considered case by case, but options might include disclosure to a GP or other health professional, social services or the emergency services.

[18] The unreasonable behaviour policy is in section 2 of this document.

[19] Note: these are only considerations, it is not a requirement to answer 'yes' to all of these to proceed with disclosure.

- Can we limit the disclosure of information to specific parties (and can we limit the amount of information we need to share)?

- Is the risk of disclosure outside our statutory powers outweighed by the risk to the complainant (or other individuals) and the risk to us if we do not act?

- Is the risk of disclosure in order to protect the vital interests (for example, a life or death situation) of the complainant or other persons? (Data Protection Act 1998, Schedule 3, Condition 3 (a), (b))

Telephone calls

4.10 All threats of harm must be taken seriously. If in conversation with a complainant or other person they suggest there is a risk they will self-harm, attempt suicide or endanger someone else, they should, if appropriate, first be encouraged to contact the emergency services or another suitable type of assistance themselves. **(Policy requirement)**

4.11 If the complainant is able to confirm in a calm and rational way that they will follow the agreed steps and maintain their own safety, then we may decide we do not need to take any further action. The staff member taking the call must ensure they record details of the call, including the plan agreed to ensure the complainant's safety.
(Policy requirement)

4.12 If we think that the risk is serious but not immediate, we should explain our concerns to the caller, try to obtain relevant information (for example, their location) and, if appropriate, seek their permission to disclose the information. Ideally, we will agree a course of action with the caller but there may be occasions where we are so concerned that we decide to act without the caller's agreement.[20]

4.13 If the caller reveals that they have already taken self-harm action, for example, they have taken an overdose or cut themselves badly, or if they are in a position of danger where self-harm could be take place or they may be about to harm others, we should consider an urgent disclosure. If appropriate, we should seek their permission to disclose the information and we should also, if it is safe to do so, tell them that we are going to disclose the information and why. If we do not have consent, or if the caller has refused consent for the disclosure, we may still take a reasonable decision to disclose the information in a potential 'life or death' situation.[21]

4.14 If a caller ends the call before we can get or give all the relevant information, then a judgment will have to be made, on the information available, about whether we need to take any action.

[20] DPA, Schedule 3, Condition 3 (a), (b) permits this.
[21] DPA, Schedule 3, Condition 3 (a), (b) permits the sharing of sensitive personal data without consent.

Process: making a disclosure following a reactive assessment of risk

4.15 This process should be followed when we receive information which shows that a complainant or others are at immediate risk (or are likely to be put at immediate risk) and we need to consider a prompt disclosure in reaction to that information. An example of this is if we receive a telephone call from a person who makes a credible threat against the doctor they are complaining about.

4.16 The staff member responsible should record all stages (including analysis, discussions, decisions and any disclosure) as fully as possible (on MSD if case related), however, this can be completed after the event. **(Policy requirement)**

- The staff member should discuss the case with a manager as soon as possible to assess the credibility of the threat and whether a disclosure may be appropriate. They do not have to seek legal or clinical advice to agree a disclosure, but if it is needed, it should be sought at this stage. Any threats to our staff, property or information must be reported to the Security Officer. **(Policy requirements)**

- If it is decided that a disclosure should be made, then details of the case should be escalated via line management to an Assistant Director or above for approval in line with the Delegation Scheme. If an Assistant Director cannot be contacted quickly, then an Operations Manager[22] or the Head of Information Assurance can, exceptionally, approve the disclosure. **(Policy requirement)**

- This approval should be clearly recorded on MSD. We can make a disclosure after a verbal authorisation. This must be confirmed later though, for example, by email or by a note on the case record. **(Policy requirement)**

- The approval decision must include agreeing the organisation(s) to which we are disclosing the information to. In the most urgent cases, the disclosure is likely to be to the emergency services. In appropriate cases we may additionally consider contacting other people or services, such as a mental health crisis team, social/support worker or GP. If the threat comes from an individual with a diagnosed mental health history, our normal approach should be to disclose information to their clinician (disclosure to other parties should be considered as appropriate).

- It is unlikely that a staff member will have to act alone when considering or making these disclosures but, if there is a serious and immediate threat to an individual (for example, a telephone call from a person saying that they have taken an overdose) and if an Assistant Director, Operations Manager or the Head of Information Assurance cannot be contacted immediately, a staff member may make the disclosure without prior authorisation. In these

[22] An Operations Manager is any member of staff at grade 3 or above who manages a team within the operations directorate.

circumstances, the staff member should notify an Assistant Director as soon as possible afterwards and record relevant information about the disclosure on MSD. **(Policy requirement)**

- A staff member who is working from home, or is a member of our associate team, should attempt to get approval before making a disclosure. There will be instances though when they may have to make a disclosure without prior authorisation. For example if a complainant is on the telephone and threatens self-harm, and the staff member cannot get in contact another way. **(Policy requirement)**

- The staff member should consider telling the subject of the disclosure that we are proposing to share information about them with a third party **before** doing so. There will be occasions when this will not be appropriate, for example, a complainant tells us if we speak to their GP about their suicidal thoughts then they will self-harm.

- We should ensure we disclose the minimum amount of factual information needed to mitigate the risk to the minimum number of organisations. This includes not providing information about any case we are considering or investigating, unless absolutely necessary in order to explain why we are making the disclosure. **(Policy requirement)**

- If possible, the staff member who identified the risk will make the disclosure by telephone. They should be prepared to answer detailed questions about, for example, the complainant's emotional state or tone of voice.

- When the staff member speaks to the person they are disclosing information to, they should tell them they are giving confidential information for the sole purpose of mitigating the risk in question. If possible/appropriate, they should:

    - ask them to keep the information secure and only use it for the intended purpose.
    - ask the organisation to let us know if it tells the subject of the disclosure that the information that initiated its action came from us.

  (These additional steps may not always be appropriate. For example, we might not mention the security of the information if we speak to the emergency services.)

- Making a telephone disclosure can take some time. If we get authorisation to disclose the information late in the working day, the staff member concerned may need to stay in the office beyond their usual office hours. If they are unable to remain at work to complete an urgent disclosure, the manager should make the disclosure on their behalf or ensure that another staff member has all the information necessary to do so. Managers should,

as far as is possible, make sure that no one is left in the office by themselves while making the disclosure.

After making the disclosure

- If not already completed, the staff member should ensure each stage of the process and the relevant approvals have been recorded on MSD. This should include explaining the reasons why the disclosure was required and cross-referencing to relevant evidence and advice (including clinical). **(Policy requirement)**

- If the disclosure relates to a specific case, the staff member should review the risk rating on MSD and ensure that any mitigation plan is up to date. (Further information about accessing the risk rating in cases is available in section 2 of the general guidance. Whether the risk rating needs to be changed will depend on the individual circumstances of the case, however both the risk rating and any mitigation plan should be regularly reviewed. **(Policy requirement)**

- If not already completed, we should inform the person involved that we have made a disclosure and who we have made it to. If applicable, we should also inform any person who provided us with the information that we have shared it. **(Policy requirements)**

Process: making a disclosure following a proactive assessment of risk

4.17 This process should be followed when we take a view that we need to disclose information because we consider our actions (or casework decisions) may lead to a risk to the health and safety of a complainant or others. This is likely to be linked to the content or outcome of a decision, investigation report (draft or final), or review request, or could be in response to an information request that we think might put the complainant or others at risk. Risk may arise, for example, when we send a decision to a vulnerable complainant explaining we will not take further action on their case or if a complainant has threatened self-harm if we do not uphold our investigation into their complaint.

4.18 The staff member should record all stages (including analysis, discussions, decisions and any disclosure) as fully as possible on MSD.

- The staff member should discuss the case with a manager as soon as possible to decide whether a disclosure may be appropriate. This will include considering how credible the threat is. We do not have to seek legal or clinical advice, but if it is needed, it should be sought at this stage. They should also inform the Security Officer of any threats to our staff, property or information. **(Policy requirement)**

- The relevant staff member (usually the case owner) should review the case risk rating on MSD and ensure that any mitigation plan is up to date.

Whether the risk rating needs to be changed will depend on the individual circumstances of the case, however both the risk rating and any mitigation plan should be regularly reviewed[23]. **(Policy requirement)**

- If we are to go ahead with the proposed disclosure, an Assistant Director (or above) should be contacted to approve the disclosure in line with the Delegation Scheme. If an Assistant Director cannot be contacted quickly, then an Operations Manager or the Head of Information Assurance can, exceptionally, approve the disclosure. **(Policy requirement)**

- This approval should be clearly recorded on MSD. We can make a disclosure after a verbal authorisation. This must be confirmed later though, for example, by email or by a note on the case record. **(Policy requirement)**

- This approval must include agreeing the organisation(s) to which we are disclosing the information to. But in appropriate cases we may additionally consider contacting other people/services, such as a mental health crisis team, social/support worker, GP and so forth. If the threat comes from an individual with a diagnosed mental health history, our normal approach should be to disclose information to their clinician (disclosure to other parties should be considered as appropriate).**(Policy requirement)**

- The staff member should consider telling the subject of the disclosure that we are proposing to share information about them with a third party **before** doing so. There will be instances though when this is not appropriate, for example, a complainant tells us if we decide not to investigate their case they will harm themselves.

- We should disclose the minimum amount of factual information needed to mitigate the risk to the minimum number of organisations. This includes not providing information about any case we are considering or investigating, unless absolutely necessary in order to explain why we are making the disclosure. **(Policy requirement)**

- We can make the disclosure by telephone or in writing. If we use email, we should take steps to ensure that the person we are disclosing information to will read it promptly (for example, by asking them to confirm receipt or alerting them by phone to the information that we are sending). We should also follow the requirements of the protective marking scheme (for example, ensuring that documents are sent securely through Egress[24]).

- The staff member making the disclosure should tell the person we are disclosing information to that we are giving confidential information for the sole purpose of mitigating the risk in question. If possible/appropriate, we should:

[23] Further information on assessing risk in casework is available in section one of this document.
[24] Further information is available at the following link: How to send a secure email in outlook using Egress

- ask the person we are disclosing information to, to keep it secure and only use it for the intended purpose; and
- ask the organisation to let us know if it tells the complainant that the information that initiated its action came from us.

- It can take time to make a telephone disclosure. If we get authorisation to disclose the information late in the working day, the employee concerned may need to stay in the office beyond their usual office hours. If the employee is unable to remain at work to make an urgent disclosure, the manager should ensure that they, or another staff member, have all the information necessary to make the disclosure. Managers should ensure that no one is left in the office by themselves while making the disclosure. **(Policy requirement)**

- If the case also contains a Duty of Candour issue, we should we should contact the CQC's Safety Escalation Team at their National Customer Service Centre on 0300 0616161 to inform them of the Duty of Candour issue. See Section 6 for more detail.

After making the disclosure

- If not already completed, the staff member should ensure each stage of the process and the relevant approvals have been recorded on MSD. This should include explaining the reasons why the disclosure was required and cross-referencing to relevant evidence and advice (including clinical). **(Policy requirement)**

- If the disclosure relates to a specific case, then the staff member should review the case risk rating on MSD and ensure that the mitigation plan is up to date. Whether the risk rating needs to be changed will depend on the individual circumstances of the case, however both the risk rating and mitigation plans should be regularly reviewed. **(Policy requirement)**

- If not already completed, we should inform the person involved that we have made a disclosure and who we have made it to. If applicable, we should also then inform the person who provided us with the information that we have shared it. **(Policy requirement)**

Support for staff

4.19 As soon as possible after the disclosure, the manager of the staff member (the person who received the information and/or made the disclosure) should meet with them to discuss the incident, talk through their feelings and to raise any concerns or anxieties. Managers and staff involved in these disclosures should also consider whether using the counselling and support services available from the employee assistance programme would be of benefit. **(Policy requirement)**

4.20 The staff member and manager should also use this meeting to identify any learning about how we handled the disclosure and to decide if there are any lessons to be learnt for the future. If the manager identifies wider learning, they should inform Q&SI. The manager should also agree an action plan for how staff should deal with further contact with the complainant concerned (For example; reconsidering the risk rating on the case, or having correspondence go through a specific staff member). **(Policy requirement)**

4.21 We will fully support staff members who make authorised disclosures in line with this guidance if there is a subsequent complaint about a breach of data protection, or our own, legislation.

5 Casework categories and themes

What are casework categories?

5.1 Casework categories have two important functions. Firstly, they help capture insight by providing high level information on the content of our casework. This then helps us to identify systemic issues, collect meaningful insight and achieve improvements in public services. Secondly, we record our decisions for each part of the complaint under these categories. They therefore provide a clear audit trail of our decision making process that can then be reported upon.

5.2 The categories we use set out common ways we describe the content of our casework and are applied to organisations to reflect the complaint as put to us. There are three types of categories in use; category (including sub-categories), complaint type and professional group[25].

- A category and sub-category are general descriptors of the type of service provided and in what setting, for example 'Hospital Services - Inpatient'.
- A complaint type describes the content of a case in more detail, such as 'communications' or 'arrears'.
- A 'profession group' covers different clinical specialities such as orthopaedics and is only applicable in health cases.

The process of adding categories

5.3 A category, complaint type, and profession group should be added under the 'principle category' section of the Case Management System (CMS) record by the Customer Services Officer considering the case before passing it for assessment. (Categories cannot be added on the CMS if a case is declined before it is passed for assessment). The principle category information is then used by the CMS to assign the case to an appropriate Assessor and Investigator.

5.4 At this stage the Customer Services Officer should pick a principle category that gives an overall view of the case being considered. If the case concerns more than one area, then the Customer Services Officer should pick the category that reflects the majority of the complaint. **(Policy requirements)**

5.5 The Assessor must review these categories when they receive the case to check their accuracy. They should also add any further complaint type or profession groups reflected in the complaint. These will need to be added separately as 'complaint parts'. **(Policy requirements)**

[25] A full list of categories, sub-categories, complaint types, and profession groups are available at the following links: Categories Sub Categories Profession Groups Complaint Types

5.6 Categories should capture key parts of the complaint. If it is not clear which category should be used, then the Customer Services Officer or Assessor should add the closest one available.

5.7 Categories should also be recorded to reflect complaints about complaint handling. These should be specifically about the way a complaint was handled, for example the time it took for a response to be provided, not that the complaint has not been resolved. **(Policy requirements)**

5.8 If the case is passed for investigation and the Assessor is unsure which category to use then they should record why it has been selected on CMS to ensure the case is allocated to a suitable investigator.**(Policy requirement)**

5.9 Once work has been completed on a case, the staff member working on the case should check the categories selected and confirm they accurately reflect the complaint as put, amending them if necessary. **(Policy requirement)**

5.10 A decision should be recorded against each category. If the case is being assessed this should include what we have decided to decline to investigate, as well as what sits in the scope of our investigation. If the case is being investigated this should include whether we decide to uphold that aspect of the complaint. **(Policy requirements)**

5.11 If a staff member wants to request a new casework category, sub-category, profession group or complaint type is added, then they should contact the Microsoft Dynamics Pilot Team who will be able to provide advice.

5.12 For a step by step guide of how to add categories and complaint parts, please see the CMS manual.

What are casework themes?

5.13 Themes[26] enable us to group cases together that have an issue in common, whether related to case content or our provision for managing them (for example 'Access to work' or 'Weekend/Bank Holiday healthcare provision'.) Themes are different from categories in that they are often attached to cases as a whole, rather than specific organisations. They help us identify any systemic trends and provide possible themes for future publications.

The process of adding themes

5.14 A theme cannot be added to a case until it is passed on for an Assessor to consider. The Assessor will therefore need to decide whether to add a theme once they have received the case.

[26] A full list of themes is available: Casework Themes

5.15 A decision should be taken on a case by case basis as to which theme, if any, is relevant and should therefore be recorded. More than one theme can be added to a case.

5.16 If a staff member wants to request a new theme is added, then approval should be obtained from an Operations Director. This should include agreeing a description of the theme and explaining when it can be used. **(Policy requirement)** This can then be added by the Microsoft Dynamics Pilot Team.

5.17 The Operational Improvement Team should also be contacted when a new theme is agreed so that the guidance can be updated. **(Policy requirement)**

6. Duty of Candour

Introduction

6.1 As the final stage in the NHS complaints process we may receive complaints about the Duty of Candour or we may discover a lack of adherence with the Duty of Candour requirements as part of our casework. It is important that staff are clear on how to consider the Duty of Candour as part of our casework process.

What is the Duty of Candour?

Professional

6.2 Individual members of staff who are professionally registered with the CQC are subject to the Professional Duty of candour. This says that every healthcare professional must be open and honest with patients when something goes wrong with their treatment or care which causes, or has the potential to cause, harm or distress. The Professional Duty of Candour is overseen by the General Medical Council, Nursing and Midwifery Council and General Dental Council.

Contractual

6.3 There is also a contractual duty of candour imposed on all NHS and non-NHS providers of services to NHS patients in the UK to *'provide to the service user and any other relevant person all necessary support and all relevant information'* in the event that a *'reportable patient safety incident'* occurs. A 'reportable patient safety incident' is one which could have or did result in moderate or severe harm or death.

Statutory

6.4 On 27 November 2014 a new statutory Duty of Candour was introduced under Regulation 20 of the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 for all health service bodies, such as hospital and NHS trusts. On 1 April 2015, the duty was expanded to include all independent providers of NHS services, including primary care providers such as GPs and dentists. The Duty also applies to private healthcare organisations registered with the CQC who provide publically funded care and treatment.

6.5 The statutory Duty of Candour requires that 'Registered persons must act in an open and transparent way with relevant persons in relation to care and treatment provided to service users in carrying on a regulated activity'.

Regulation 20

6.6 Regulation 20 says that the Duty of Candour is triggered by a 'notifiable safety incident' which is defined as *'any unintended or unexpected incident that occurred in respect of a service user*

Notifiable Safety Incident

6.7 Health service bodies are subject to a wider definition of a 'notifiable safety incident' than independent providers. For a health service body, it is enough to trigger the Duty if the 'notifiable safety incident' could have resulted in harm, whilst for independent providers the 'notifiable safety incident' has to have resulted in harm.

6.8 The definitions in full are set out in Annex H. The definitions for the types of harm the 'notifiable safety incident' may cause are detailed in Annex I.

Duty of Candour requirements

6.9 For both health service bodies and independent providers; once a 'notifiable safety incident' has been identified, a registered person has to carry out a number of actions to meet the Duty of Candour requirements:

- Telling the relevant person (the service user or a person acting on their behalf), in person, as soon as reasonably practicable after becoming aware that a notifiable safety incident has occurred.
- Offering reasonable support to the relevant person.
- Providing an account of the incident which, to the best of the provider's knowledge, is true of all the facts the registered person knows about the incident as at the date of the notification.
- Offering an apology.
- Following up the apology by giving the same information in writing, and providing an update on any further enquiries made.

Contractual Arrangements

6.10 It is important when we are looking at a Duty of Candour complaint, that we are aware of the contractual arrangements for the organisation involved so that we can consider the correct definition. For example, we may receive a complaint about a GP service which relates to the Duty of Candour, however, the GP services are contracted out by a Trust. In this situation the relevant definition for a 'notifiable safety incident' would be the other health service body definition not the independent provider definition.

6.11 Please contact the Jurisdiction Advice Team if you need any assistance identifying the correct type of organisation.

Role of the CQC

6.12 The CQC are responsible for regulating, monitoring and enforcing implementation of the Duty of Candour with registered providers. They meet their responsibilities through their registration and inspection processes and report on the Duty of Candour under the safety key questions in their inspection reports. The CQC can take action (including seeking criminal sanctions) if providers breach the duty.

Casework Considerations

6.13 In considering Duty of Candour complaints we should continue to follow the casework process set out in the Service Model main guidance. We do not need to conduct our casework differently just because a case raises a Duty of Candour issue. We just need to be aware of what the Duty is and how we consider it as part of our normal casework process.

Actions during Intake

6.14 If it is clearly identifiable to a Customer Services Officer that a complaint received is about the Duty of Candour, then this should be flagged on the electronic casefile by creating a 'pop up'.

Duty of Candour complaints that have not been through local resolution

6.15 In health cases, the law[27] prevents us from conducting an investigation unless we are satisfied the complaints process has been used and exhausted, or it was not reasonable to expect the complainant to have done so. **(Legal requirement).** There are some exceptional circumstances where we may decide to consider a premature complaint.

6.16 The NHS complaints procedure is the formal complaints process before coming to the Ombudsman, so even if complainants have had a Duty of Candour response, we still expect organisations to signpost the complainant to the formal complaints procedure. This is because patients and their families have a right to complain and they should be told what that process is as they may have other issues they want looked at that aren't covered by the Duty of Candour **(Policy Requirement)**.

6.17 However, we may still receive cases in which the complainant has received a Duty of Candour response but has not received a local resolution response. This may be because the organisation has not provided one or because the complainant has decided they do not wish to pursue a local resolution complaint.

6.18 If we do receive a complaint that hasn't been through local resolution, but has had a Duty of Candour response, we should not automatically close the case as being premature. Instead, we should consider whether there is any merit in looking further at the complaint. **(Policy Requirement)**.

6.19 Some of the points we might want to consider when determining whether to look at a complaint that has had a Duty of Candour response but no local resolution response are:

- Whether the organisation has carried out a Duty of Candour investigation and response that has been communicated to the complainant and how satisfactory that response is.

[27] Section 4(4) and (5) 1993 Act

- Whether the organisation considers there is anything further they can add to the Duty of Candour response already provided, through local resolution.
- Whether the complainant has raised any other concerns that have not been addressed by the Duty of Candour response.

6.20 This is not a definitive list of considerations. Each case should be judged on its own merits to determine the most appropriate way to proceed. If staff are unsure about how to proceed with a case, they should speak to their Line Manager in the first instance.

6.21 If we decide to close the case as premature to allow the local complaints process to be completed, we should clearly explain to the complainant why we are unable to proceed with their case using just the Duty of Candour response. **(Policy requirement)**

Actions during assessment

6.22 If it is clearly identifiable to an Assessor that a complaint received is about the Duty of Candour and this has not been noted on the file, then this should be flagged on the electronic casefile by creating a 'pop up'.

Contact with the complainant

6.23 If we are aware that the complainant has raised a Duty of Candour complaint, we should check what outcome they are seeking during our contact with them.

Alternative Legal Remedy & Another dispute resolution forum.

6.24 If the complainant is solely seeking regulatory action or a legal decision that the Duty of Candour was breached, then it might be more appropriate for the courts (as an Alternative Legal Remedy (ALR)) to deal with the complaint or the CQC (as an alternative dispute forum) to be made aware of the issues.

Actions during Investigation

Cases where the Duty of Candour has been addressed by the organisation

6.25 For the majority of cases we receive which relate to the Duty of Candour, it will be clear from the paperwork that the organisation has considered the complaint in line with the Duty of Candour and decided whether to provide a Duty of Candour response or not. The Duty of Candour should be referenced in the complaint papers we receive from the organisation.

6.26 When analysing the evidence in order to reach a decision on the case, as well as looking at the case papers, we should use Regulation 20 as one of the standards against which to measure what should have happened against what did happen for Duty of Candour complaints. The CQC has produced their own guidance on Duty of Candour complaints which is available here (**http://www.cqc.org.uk/content/regulation-20-duty-candour**) and can be used as a relevant standard. In addition, each organisation should have their

own internal policies on the Duty of Candour and both the GMC and NMC have produced guidance also. We should consider using these documents as relevant standards also.

Identifying maladministration or service failure in Duty of Candour complaints.

6.27 We must be careful that where we identify maladministration or service failure relating to the Duty of Candour issue, we do not make legal determinations, as it is not our role to adjudicate on matters of law. We could not therefore find that the Duty of Candour requirements have been breached by the organisation complained about. This is because it is a matter for the courts to say whether the law has been breached or not, it is not our role to do so.

6.28 Instead, we can reach a view on whether the organisation complained about, has paid appropriate attention to their obligations under the Duty of Candour set out in Regulation 20 and we can reach a view on the reasonableness of their Duty of Candour response.

Making recommendations

6.29 If we make recommendations in relation to the Duty of Candour then the recommendation should, in line with our normal approach, be relevant to the injustice found and the remedy is to put right that injustice.

6.30 If we find that the organisation did not have due regard to their obligations under the Duty of Candour when deciding whether or not to trigger the Duty, we can recommend that decision be taken again, this time without the failings we have identified. In exceptional cases, where there is sufficient evidence, we can recommend that the Duty of Candour is activated.

6.31 We could also recommend that the organisation apologise and provide a more satisfactory Duty of Candour response to the complainant, if appropriate. Similarly, we may also make recommendations for systemic remedy: to prevent a recurrence of the failings that we have found. If we are considering making systemic recommendations, we should check the outcome of any recent CQC inspections in the area of the organisation or aspect of care we are investigating.

Cases where the Duty of Candour has not previously been mentioned

6.32 Whilst in most cases, it should be clear from the case papers and organisational records whether the Duty of Candour is relevant to the complaint; there may be occasions where we receive a complaint in which the Duty of Candour has not previously been raised or considered. Instead, we may receive cases where, as part of our casework, we identify that there is a relevant Duty of Candour issue.

6.33 A relevant Duty of Candour issue may occur in any case we receive. This does not mean that staff should go looking for Duty of Candour issues in all health cases nor should we spend a disproportionate amount of time trying to decide if the Duty of Candour is relevant. However, staff should be aware that

the Duty of Candour may be relevant to a complaint even where it has not been raised earlier.

6.34 We cannot make findings and recommendations on complaints that are not within the scope of the investigation. Therefore, if we consider that there is a Duty of Candour complaint relevant to the case which has not been raised previously, then we will need to decide how best to proceed with the case. When considering how best to proceed we should consider the Service Model main guidance, paragraphs 5.9-5.10 - Expanding the scope.

6.35 In that situation, the caseworker should raise the issue with their line manager to determine what the next steps should be together. This could include:

- Considering how closely related the 'new' issue is to the complaint we are currently considering.
- Whether we should notify the complainant, and
- Whether the organisation may need to provide a response.

6.36 Similarly, if a Clinical Adviser considers that there is a relevant Duty of Candour issue to the case, then they should raise this with their Lead Clinician.

CQC

6.37 The Duty of Candour is one of the CQC's Fundamental Standards - the standards below which they consider care must never fall. For cases which relate to the Duty of Candour, we should continue to carry out the following activities:

- Publishing our case summaries which the CQC look at – we should ensure we reference the Duty of Candour in the case summary, and
- Checking the outcome of any recent CQC inspections in the area of the organisation or aspect of care we are investigating.

Sharing information with the CQC when there is a likely threat to the health and safety of patients

6.38 During our consideration of any health case we may discover information which indicates a threat to the health and safety of patients. We have a statutory power to disclose such information to any persons to whom we think the information should be disclosed to in the interests of the health and safety of patients[28].

6.39 When determining whether there is a potential risk to the health and safety of patients, staff should follow the process set out in the Disclosure of concerns about health and safety of patients under S.15 HSC guidance.

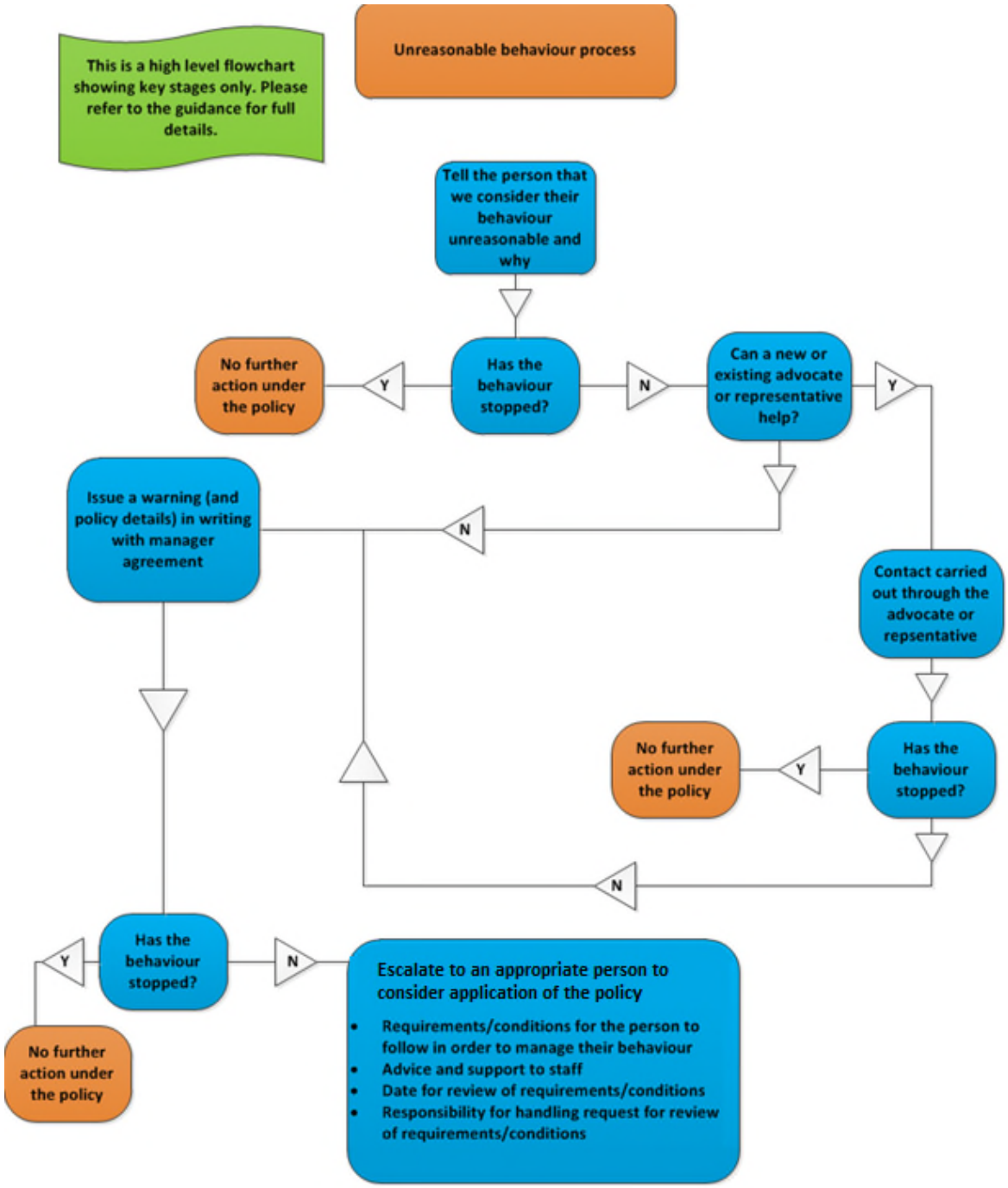
6.40 If the case also contains a Duty of Candour issue and, having followed the process set out in the Disclosure of concerns about health and safety of patients under S.15 HSC guidance, we decide that there is a potential risk to

[28] 1993 Act, section 15 (1) (e)

the health and safety of patients and we should disclose this – as part of that disclosure we should contact the CQC's Safety Escalation Team at their National Customer Service Centre on 0300 0616161 to inform them of the Duty of Candour issue.

6.41 It is important to note that disclosure would not be appropriate for cases where we just make an adverse finding of fault. Disclosure under Section 15 should only be considered where we have identified an additional potential risk to the health and safety of patients.

Annex A: Unreasonable behaviour process flow chart



Annex B: example letters

Warning letter

I write in response to your telephone calls to me and my colleague yesterday. During these telephone calls, you made numerous abusive comments to us which we found offensive. When speaking to staff at our Office it is unacceptable to swear or make racist comments or comments of a sexual nature.

Please stop making such comments or being at all rude to staff. If you continue to contact us in this way, we may unfortunately have to take steps to manage our communication with you which may include limiting your contact with us. I enclose a copy of our Unreasonable Behaviour Policy, which you can find on our website at…

That said, if you are prepared to have a polite and reasonable conversation about your complaints, we will be happy to discuss them with you.

Letter imposing restrictions

As you know, we warned you that if you continued to swear or use racist and/or sexual language when talking to our staff then we would consider taking action to limit your contact with us. Despite that letter and further reminders you have continued to use inappropriate and offensive language when talking to staff. As your offensive remarks have fallen within our definition of 'unreasonable behaviour' I have instructed my staff not to take telephone calls from you.

Consequently, you are now prohibited from making telephone calls to us but you may still communicate in writing. To be clear, you must not use the telephone to contact this office. If you do so, my staff will immediately terminate the call. However, we will review the position in six months.

If you have any representations then please send them to us in writing and we will consider your concerns.

I hope you understand that this action has become necessary because of the abusive nature of your telephone calls. We will continue to deal with written communication that is not of an abusive nature, in an appropriate manner.

Annex C: Employee risk assessment process

1. Security at PHSO is the collective responsibility of all staff and contractors. It is supported by a clear corporate accountability framework, designating specific roles and responsibilities as set out in the Security Policy.

2. The employee risk assessment form is intended to be used when a potential risk to the safety or wellbeing of a PHSO member of staff is identified from a complainant or another party to the complaint.

3. Any employee identifying a potential risk to themselves or another member of staff should talk immediately to their manager (or another manager if the manager is not available). The manager (talking to others as necessary) should decide whether the employee risk assessment form should be completed (as there may be circumstances in which no action or different action is required).

4. Examples of circumstances in which this form could be used:

    - Threats to members of staff (for example, in letters, emails, telephone calls or face-to-face).
    - Nuisance telephone calls or emails.
    - Members of staff being contacted or approached by a complainant outside of work.

5. These are only examples. The key factor in deciding whether to use the form should be the identification of the risk to the member of staff.

Completing the form

6. The manager of the member of staff at risk should complete the form.

7. The form is a living document and should be reviewed and revised when necessary. Additional sheets are available to record further actions and review dates.

8. The form should be saved on the relevant MSD case record.

9. If you need further advice please talk to your manager in the first instance.

    - Section 1: Complete the names of relevant staff, case reference number and date. The 'staff support' field is optional and is intended to record details of anyone who is supporting the staff member such as a trade union representative or other colleague.

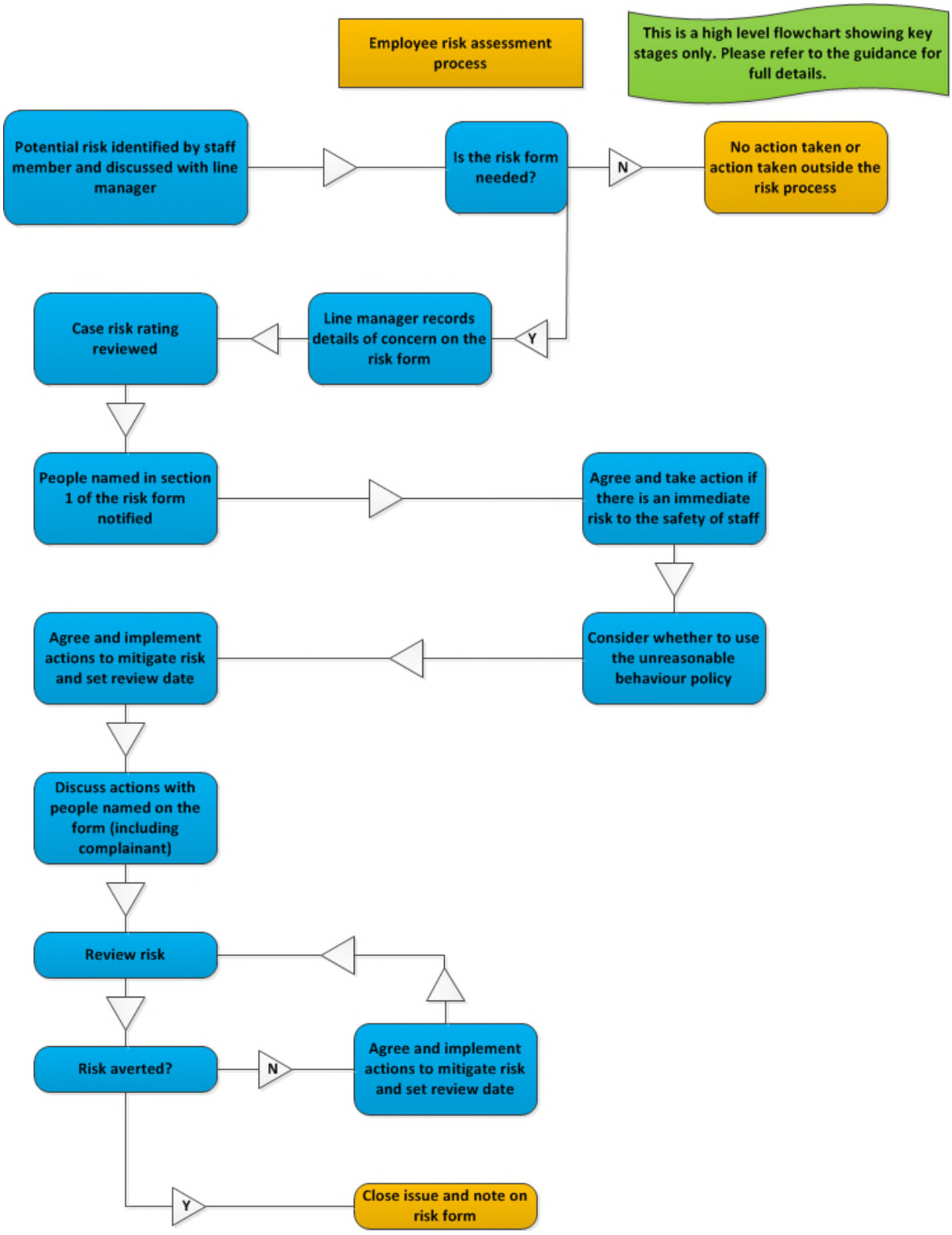
    - Section 2: A summary of the risk, how it was identified, relevant dates and any action taken so far. This must also say whether the relevant case is open or closed.

    - Section 3: This should be ticked when the case risk rating has been reviewed.

    - Section 4: This should be ticked when the security officer has been notified.

- Section 5: Answer yes or no to the three questions about immediate risk and reallocation of the case.
- Section 6: This should be ticked once application of the unreasonable behaviour policy has been considered.
- Section 7: A summary of the agreed actions, who will carry them out and by when. This will include internal actions (for example, issuing a warning or imposing a restriction under the unreasonable behaviour policy) and external actions (for example, contacting the police).
- Section 8: A date to review the risk again should be agreed and entered here. The timescale for this will depend on the circumstance of the case, but it should not be more than three months from the completion of the form. The risk can of course be reviewed prior to that date if circumstances change.
- Section 9: The manager should tell relevant people (both internally and externally) about the agreed actions (section 7) and tick to confirm it has been done. This will include telling those people named in section 1 of the form. It may also involve contacting the complainant or other parties to the complaint.
- Section 10: This should be used to record the outcome of the risk review (which should happen at the latest by the date set in section 8).
- Section 11: Record if the risk can now be closed. If not, the risk should be reviewed and further action agreed (as per section 7).
- Section 12: The form should be signed by the relevant members of staff after section 8 has been completed.

Employee risk assessment flowchart



Annex D: Recording information on Visualfiles

Recording a warning

1. The staff member should record the warning fully on the person's details screen on Visualfiles (this screen can be accessed by either searching for the person by name or by accessing their details from a case). **(Policy requirement)**

    - On the person's screen select '*Behaviour policies'* then '*Apply warning' (*if a previous warning exists, the option to '*View existing warnings*' or '*Create a new warning*' appears).
    - Complete the mandatory comments box. This should summarise the reasons for giving the warning and contain a brief note of the discussion with the manager.
    - Select the manager with whom the warning was discussed from the list of staff.

2. Existing (or previous) warnings are available by selecting '*View warnings'* from the *'Behaviour policies'* screen.

Recording the application of the policy and restrictions

- On the individual's screen select 'Behaviour policies' then 'Apply policy'.
- Select the manager who approved the decision to apply the policy.
- Select the date on which the application of the policy should be reviewed.

3. Add relevant details about the restrictions imposed.

    - Select 'Add/view restrictions' (if previous restrictions are recorded then the option to 'View existing restrictions' or 'Create a new restriction' appears).
    - Choose the restriction type from the list that appears.
    - Complete the mandatory comments box. This should summarise the restrictions imposed.
    - Select the manager with whom the application of the restriction was discussed (note: in many cases this will be the manager who authorised the application of the policy).

4. It is essential that the staff member dealing with the person at the time keeps Visualfiles up to date, particularly if the restrictions on contact are altered, varied or removed. **(Policy requirement)**

Recording a review of the policy

- On the individual's screen select 'Behaviour policies' then 'Policy review'.
- Select the manager who reviewed the application of the policy.
- Select the outcome of the policy review: 'Continue', 'Revised restrictions' or 'End application of policy'.
- If 'Continue' or 'Revised restrictions' are selected then a further review date must be entered.
- Before 'End application of policy' can be recorded there must be no current restrictions in place. To end a current restriction select 'Add/view restrictions' and then 'View existing restrictions'. Highlight the relevant restriction and press 'Select restriction'. You can then select 'End date' and will be prompted to enter the name of the manager who approved the ending of the restriction (which may also be the manager who reviewed the application of the policy).

Annex E: Extract from section 15 of the Health Service Commissioners Act 1993

15. Confidentiality of information

(1) Information obtained by the Commissioner or his officers in the course of or for the purposes of an investigation shall not be disclosed except -

(a) for the purposes of the investigation and any report to be made in respect of it,

(b) for the purposes of any proceedings for –

(i) an offence under the Official Secrets Acts 1911 to 1989 alleged to have been committed in respect of information obtained by virtue of this Act by the Commissioner or any of his officers, or

(ii) an offence of perjury alleged to have been committed in the course of the investigation,

(c) for the purposes of an inquiry with a view to the taking of such proceedings as are mentioned in paragraph (b),

(d) for the purposes of any proceedings under section 13 (offences of obstruction and contempt), or

(e) where the information is to the effect that any person is likely to constitute a threat to the health or safety of patients as permitted by subsection (1B).

(1A) …

(1B) In a case within subsection (1)(e) the Commissioner may disclose the information to any persons to whom he thinks it should be disclosed in the interests of the health and safety of patients.

(1C) If the Commissioner discloses information as permitted by subsection (1B) he shall -

(a) where he knows the identity of the person mentioned in subsection (1)(e), inform that person that he has disclosed the information and of the identity of any person to whom he has disclosed it, and

(b) inform the person from whom the information was obtained that he has disclosed it.

Annex F: Legal background: maintaining confidentiality in our casework

- We must act in accordance with the law relating to data protection[29] including maintaining confidentiality of the parties to the complaint and avoiding sharing any information at a time or in a way that may influence or prejudice our work.

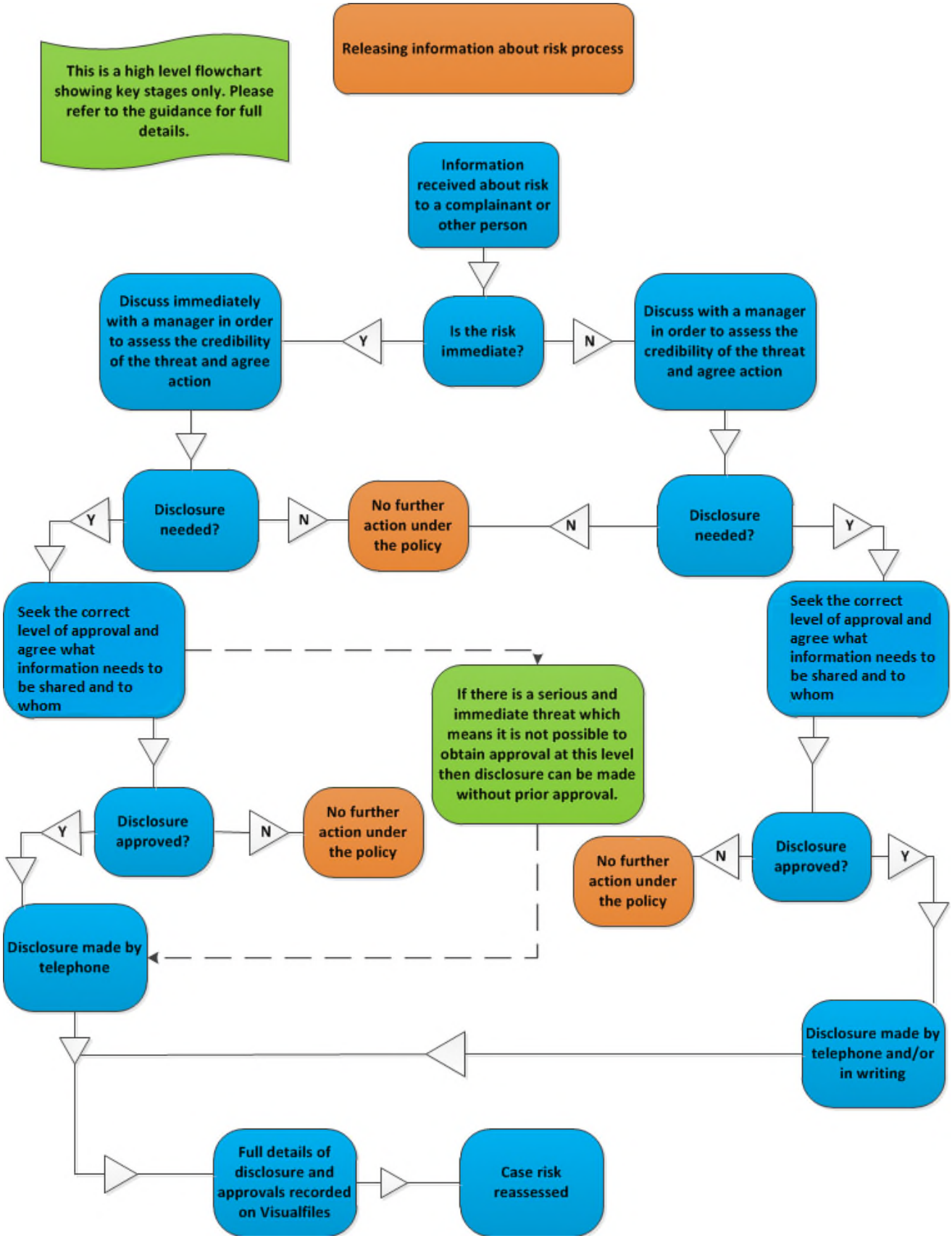
- Our legislation requires that we conduct investigations[30] in private.[31] We should make sure that we maintain confidentiality when we conduct an investigation and are aware of information that is, and is not, appropriate to share between the parties to the complaint. We may disclose information to the parties to the complaint or to third parties where doing so is for the purposes of the investigation or the report and for other limited reasons.[32]

- We should be aware of our responsibilities under the *Data Protection Act 1998* (the DPA) to process personal data lawfully and fairly. We should only share personal information if doing so is necessary for the exercise of our statutory functions. The DPA allows the release of information without the consent of the data subject where doing so is necessary to protect the vital (that is, life or death) interests of the data subject or others.[33]

- Although the release of information in the circumstances set out in this guidance is likely to be a fair and lawful disclosure under the DPA, it may fall outside the scope of our legislation and be a technical breach of our own statutory bar.

[29] *Data Protection Act 1998. Freedom of Information Act 2000.*
[30] Please note that these restrictions on the disclosure of information cover all of our casework, including assessment and review work.
[31] 1967 Act section 7(2). 1993 Act section 11(2).
[32] 1967 Act section 11. 1993 Act section 15.
[33] 1998 Act, Schedule 3, paragraph 3(a) (i)-(ii) and 3(b).

Annex G: Process flow chart



ANNEX H – Regulation 20 of the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014

20.—

1. Registered persons must act in an open and transparent way with relevant persons in relation to care and treatment provided to service users in carrying on a regulated activity.

2. As soon as reasonably practicable after becoming aware that a notifiable safety incident has occurred a registered person must—

a. notify the relevant person that the incident has occurred in accordance with paragraph (3), and
b. provide reasonable support to the relevant person in relation to the incident, including when giving such notification.

3. The notification to be given under paragraph (2)(a) must—

a. be given in person by one or more representatives of the registered person
b. provide an account, which to the best of the registered person's knowledge is true, of all the facts the registered person knows about the incident as at the date of the notification,
c. advise the relevant person what further enquiries into the incident the registered person believes are appropriate,
d. include an apology, and
e. be recorded in a written record which is kept securely by the registered person.

4. The notification given under paragraph (2)(a) must be followed by a written notification given or sent to the relevant person containing—

a. the information provided under paragraph (3)(b),
b. details of any enquiries to be undertaken in accordance with paragraph (3)(c),
c. the results of any further enquiries into the incident, and
d. an apology.

5. But if the relevant person cannot be contacted in person or declines to speak to the representative of the registered person —

a. paragraphs (2) to (4) are not to apply, and
b. a written record is to be kept of attempts to contact or to speak to the relevant person.

6. The registered provider must keep a copy of all correspondence with the relevant person under paragraph (4).

ANNEX I – Definitions

Notifiable Safety Incident – Paragraphs 8 (health service body) & 9 (other registered person) of Regulation 20

'8 - In relation to a health service body, "notifiable safety incident" means any unintended or unexpected incident that occurred in respect of a service user during the provision of a regulated activity that, in the reasonable opinion of a health care professional, could result in, or appears to have resulted in—

a. the death of the service user, where the death relates directly to the incident rather than to the natural course of the service user's illness or underlying condition, or

b. severe harm, moderate harm or prolonged psychological harm to the service user'.

9 - In relation to any other registered person, "notifiable safety incident" means any unintended or unexpected incident that occurred in respect of a service user during the provision of a regulated activity that, in the reasonable opinion of a health care professional—

a. appears to have resulted in—

i. the death of the service user, where the death relates directly to the incident rather than to the natural course of the service user's illness or underlying condition,

ii. an impairment of the sensory, motor or intellectual functions of the service user which has lasted, or is likely to last, for a continuous period of at least 28 days,

iii. changes to the structure of the service user's body,

iv. the service user experiencing prolonged pain or prolonged psychological harm, or

v. the shortening of the life expectancy of the service user; or

b. requires treatment by a health care professional in order to prevent—

vi. the death of the service user, or

vii. any injury to the service user which, if left untreated, would lead to one or more of the outcomes mentioned in sub-paragraph (a)'.

Definitions of Harm

Moderate harm – Paragraph 7 of Regulation 20

- *'"Moderate harm" means—*
  - *a. harm that requires a moderate increase in treatment, and*
  - *b. significant, but not permanent, harm;*

'harm that requires a moderate increase in treatment' (e.g. unplanned return to surgery, an unplanned re-admission, a prolonged episode of care, extra time in

hospital or as an outpatient, cancelling of treatment, or transfer to another treatment area (such as intensive care)'.

Severe harm – Paragraph 7 of Regulation 20

- *'"Severe harm" means a permanent lessening of bodily, sensory, motor, physiologic or intellectual functions, including removal of the wrong limb or organ or brain damage, that is related directly to the incident and not related to the natural course of the service user's illness or underlying condition'.*

Prolonged psychological harm – Paragraph 7 of Regulation 20

'"Prolonged pain" means pain which a service user has experienced, or is likely to experience, for a continuous period of at least 28 days'.

Other definitions

Relevant person – Paragraph 7 of Regulation 20

'"Relevant person" means the service user or, in the following circumstances, a person lawfully acting on their behalf—

a. *on the death of the service user,*
b. *where the service user is under 16 and not competent to make a decision in relation to their care or treatment, or*
c. *where the service user is 16 or over and lacks capacity in relation to the matter'.*

Apology – Paragraph 7 of Regulation 20

'"Apology" means an expression of sorrow or regret in respect of a notifiable safety incident'.