Health Research Authority

A Review of Adverse Events in Research, Evidenced from Breach Notifications

CONFIDENTIAL

Catherine Blewett - HRA Improvement & Liaison Manager

catherineblewett@nhs.net

Table of Contents

1. Introduction

The REC (Research Ethics Committee) is notified when any breach of the study protocol or the principles of Good Clinical Practice (GCP) in research has been identified and information pertaining to breaches is retained by HRA (Health Research Authority) for the purpose of monitoring the management of individual breaches.

The REC relies on breaches being reported or identified through audit and the majority are self-reported by sponsors/Chief Investigators, the REC does not have a role to audit and inspect. The information relating to individual breaches is also reviewed to identify any non- study specific issues which may require action, such as repeat problems with processes at an individual site. It is recognised that more generalizable information in terms of research governance can be extrapolated from the information provided via the breach reporting process.

For research involving investigational medicinal products, the study sponsor is legally required to notify the Medicines and Healthcare products Regulatory Authority when there is a departure from the approved protocol which is deemed to be a serious breach (please see section 3). However, all serious breaches of the protocol should be reported to the Research Ethics Committee so that the validity of the favourable ethical opinion can be kept under review.

The information which is provided when reporting a breach is valuable information but it must also be noted that this relies on robust audit and monitoring processes as well as the integrity of the individuals and organisations responsible for reporting, including all individuals involved in research processes. That is to say, high reporting by one organisation compared to another organisation does not necessarily indicate a high level of non-compliance but could in fact be indicative of exceptional monitoring and reporting processes. Moreover, it cannot therefore be said that the information provided via breach reporting is the whole picture of GCP and protocol non-compliance. The numbers reported here should therefore be seen as an indication of the type of issues which occur and not the total picture.

This project has focused on actual evidence of non-compliance to the principles of good clinical practice and the study protocol, as reported through the standard breach reporting processes, and the adverse effects which such breaches have had. The reporting period was 1 April 2013 to 31 March 2014. Such adverse consequences may have been for the participant, the research team, the sponsor or the hosting organisation etc.. The purpose of undertaking this project and producing this report is to highlight the types of issues which do occur, look at the common themes and trends which have been identified and to share learning more widely.

2. Aims

The aims of this project were as follows:

- To identify commonly occurring breaches of good clinical practice in research and protocol breaches.
- To look at the root cause, consequence and impact of breaches, including the impact on research participants, researchers, research sponsors and wider.
- To identify risk controls and assess their effectiveness including current governance practices.
- To establish how actual risks in research relate to the principles set out in the Research Governance Framework, particularly in regard to ensuring proportionality.
- To develop a framework for the communication of learning points
- To report to the project steering group and share learning as appropriate.

3. Background Information

3.1 Breach register

Information regarding all breach notifications, which include protocol violations, serious breaches and alleged incidents of fraud or misconduct, are recorded on a Breach Register. For the purpose of this document, the term 'breach' refers to all protocol violations, serious breaches and incidents of fraud or misconduct. Breaches are classified in accordance with the following descriptions:

Serious breach

A serious breach of the protocol or of the conditions or principles of Good Clinical Practice (or equivalent standards for the conduct of non Clinical Trials of Investigational Medicinal Products CTIMPs) which is likely to affect to a significant degree the safety or physical or mental integrity of the trial subjects, or the scientific value of the research. For the purpose of this procedure, this includes current and future participants.

Protocol Violation

Deviations from the protocol which are not agreed in advance and are the result of error but do not constitute a serious breach.

Fraud or Misconduct

Intentional behaviour by a researcher, both alleged and proven, that falls short of good ethical and scientific standards or the generation of false data with the intent to deceive.

The Breach Register includes the 'breach category'. The breach categories and sub categories have been developed over the last 18 months by the HRA for the purpose of identifying commonly occurring themes and trends. Data sorting of the 2013/14 breach register was undertaken to identify the frequency of occurrence of each breach category.

3.2 NHS and University R&D Survey

A survey monkey questionnaire was sent out to sponsor contacts with 97 responses being received. The survey was anonymous to encourage open and honest responses. The survey was for the purpose of better understanding the breach reporting culture and processes within different organisations. The information which was gained through this process was very useful and often confirmed conclusions drawn from reviewing the breach notification data.

Almost half of the responses received were from organisations which sponsored CTIMPs. The majority of organisations stated that they do have standard operating procedures in place for the management of serious breaches of the principles of GCP in research or of the study protocol and also for the management of alleged fraud or misconduct in research. However, a number of comments were received which suggested that there was an understanding that such standard operating procedures are not required for organisation who do not sponsor CTIMPs.

"No CTIMPs so no systems re breach"

"All individuals in CTIMPs are aware" (of breach reporting processes)

"SOPs are designed for CTIMPs and for those staff involved in managing CTIMPs"

Where standard operating procedures are in place, responders were asked to state the frequency with which they are followed. Just over 45% of the responses stated that they were always followed with 40% stating that they were very often followed. Due to the robust inspection process by the MHRA for organisations who sponsor CTIMPs, the expectation would be that organisations who do sponsor CTIMPs would have standard operating procedures which are always, or very often, followed as this is something that would be identified by the GCP Inspectorate during their inspection process.

Whilst having standard operating procedures in place is important, they will only be effective if these documents are accessible and members of the research team are made aware of them, particularly in relation to their own roles and responsibilities. Almost 70% of responders indicated that the documents were shared with all those involved in research. However, 10% of responders indicated that the documents were either not shared at all or were only shared with the Chief or Principle Investigators; 4% of responders indicated that they were not kept in a place which was freely accessible. For standard operating procedures to be effective, it is important that all members of the research team are aware of processes and responsibilities. Furthermore, it is important to determine understanding of and compliance with standard operating procedures. 34% of responders indicated that their organisation had no process in place to monitor understanding and compliance.

The full results of the survey are included in Appendix A

4. Analysis of the HRA Breach Register

Each breach notification received from 1 April 2013 to 31 March 2014 was reviewed in relation to a number of criteria. This included the type of individual breaches (breach category) which were reported within the notification and also the overall breach classification. This therefore means that whilst the individual breach category may not in itself constitute a serious breach, it may have been part of a wider breach which, when considered in its entirety, would be classified as a serious breach.

Data sorting was undertaken to identify the frequency of occurrence of breach types and the most commonly occurring breach types were reviewed individually for the purpose of better understanding the root causes and the impact of the breach. The impact of the breach was considered in regard to participants, researchers, sponsors and host organisations etc. A total of 157 breach notifications were received within the reporting period. Of these 157 notifications, 34 notifications were reporting multiple breaches within the same notification (table 4.1).

Table 4.1

Multiple issues in one report	
Yes	34
No	123

Each breach notification was classified as a serious breach, a protocol violation or alleged fraud or misconduct. Table 4.2 sets out the breakdown of all breach notifications by classification and table 4.3 further breaks this down by study type. The decision regarding whether a breach was considered to be a serious breach was primarily made based on the categorisation given by the MHRA for CTIMPs (Clinical Trials of Medicinal Products) but additionally, if not categorised as a serious breach by the MHRA, the HRA took into consideration whether there was *potential* for impact on the safety or mental or physical integrity of participants or the data integrity. This is broader than the MHRA definition but from an ethical perspective, this ensures consideration is given to future and other participants as well as those who are more directly affected by the breach itself.

Table 4.2

Breach classification		
Violation	85	54%
Serious breach	70	45%
Fraud or Misconduct	2	1%

Table 4.3

	Serious Breach		Violation		F o M	
CTIMP	59	84%	51	60%	1	50%
Healthy Volunteer	6	9%	2	2%	1	50%
Other	5	7%	32	36%	0	

It is reassuring to note that when put into context of approximately 6000 studies being approved by RECs in the UK per year, a reporting of 70 serious breaches in one year is a low number. Whilst there is still a question regarding whether low reporting is due to a low number of breaches or insufficient breach reporting processes, some assurance in this regard can be drawn, particularly for CTIMPs, from the clear requirements for breach reporting set out by the MHRA and the monitoring of adherence within the inspection process.

4.1 Breach categories.

This section looks at the breakdown of breaches on the HRA breach register by category. All breaches reported within one notification are recorded under categories and sub categories.

4.1.1 Investigational Medicinal Product (IMP)

This category includes all breaches which relate to a study drug. Table 4.1.1 indicates that the highest occurring breaches in relation to the study drug relate to dispensing, dosing and prescribing. These three areas are often linked and due to poor oral or written communication or processes. Errors with dispensing included more than one IMP being dispensed at the same time and becoming mixed up. One example was where two IMP packs were made up at the same time and the active drug pack and placebo pack became mixed up. The corrective actions for this breach were to update the study specific dispensing procedure and to re-train all technical services staff. This would suggest that adequate prior consideration was not given to ensuring that making up and dispensing of multiple IMP packs did not lead to them becoming mixed up. The impact of this error for the participants was that they may have received an incorrect IMP pack. The participants were informed that this had happened which has the potential for undue distress and the potential that their time had been wasted if the data was un-useable. The impact for the study was the potential that the data may not be included in the final analysis as well as a time and resource implication due to the investigation and actions to rectify the error.

Examples of IMP dosing breaches, the most commonly occurring IMP breach sub-category, include misunderstanding regarding the term ‘dummy titration’ which was not clearly defined by the sponsor to the laboratory. The outcome of this was that participants who were in the placebo arm of the trial were taking an unexpectedly large number of tablets which effectively led to indirect un-blinding; as it was apparent which arm of the trial they were in. This was confirmed only after suspending the use of the trial medication and un-blinding to the non-direct research team, who were able to check the medication and dose given to each participants. The impact of this for the trial participants was that some were taking twice the required number of tablets per day and the potential for distress during the period of uncertainty. The impact for the study was to the integrity of the data due to the indirect un-blinding (in regard to the placebo and IMP not being identical) which had occurred. There would also have been a time and resource implication to investigate and rectify the error.

> Titration involves increasing the dose of a drug until the side effects outweigh any benefit. For a trial to be blinded, the same titration process must be followed by all participants.

Another example of an IMP dosing error was in a Phase 1 oncology trial where a registration fax was received with the correct dose recorded but the incorrect dose was then written on the internal prescription. The Pharmacy did not pick up the error as they used the internal prescription only for verification. The participant was noted to experience adverse events after taking the IMP and it took a full 3 week cycle before it was possible to assess whether the participant would experience any serious adverse events(s). The participant was subsequently admitted to hospital with grade 4 neutropenia which was considered to possibly be related to the dosing error. The corrective action for this breach was to change the process to ensure that the registration fax is also used to verify the dose, not just the internal prescription. Further training was also undertaken with all relevant staff. This is a good example of where additional safety nets, such as only ever using two sources for verification, would have been simple and beneficial to prevent actual participant harm.

There were also IMP dosing breaches due to confusion about dosing calculations based on weight. One involved participants' weight being written next to the incorrect participants' record which led to two participants being under dosed and two participants being over dosed. One breach was due to a misunderstanding that the dose should not be calculated by weight, as would happen in clinical practice, rather than a set dose which was required for the study.

Whilst human error and misunderstanding or misinterpretation do, somewhat inevitably, occur, they can be mitigated by undertaking a robust risk assessment during the planning stages and ensuring that there are clear processes which include 'safety nets' to identify errors before they have an impact, particularly on research participants.

These breaches need to be considered within the context of the large number of studies conducted in the UK, 6000 per year approved by RECs of which around 1000 will be drug trials.

Table 4.1.1

IMP	Serious breach	Violation
Dispensing error	6	0
IMP accountability (issues with delegation log)	1	0
IMP dosing	7	5
IMP records	0	1
IMP storage	1	1
IMP temperature	1	1
Prescribing error	4	1

4.1.2 Consent / PIS / recruitment

As indicated in table 4.1.2, the most commonly occurring themes in this category were consent not being obtained, in CTIMPs this was commonly in relation to re-consenting in light of further safety information being available during the trial, and recruitment outside the inclusion criteria.

Examples of breaches of the informed consent procedure included a member of the research team having awareness of the procedure but choosing to deviate from the protocol and take informed consent at a different part in the process, as they believed that this would be more convenient and

prevent undue waiting at the Pharmacy. This is an example of where training in the protocol procedures was not sufficient in itself but rather ensuring an understanding of the importance of following the protocol and encouraging communication within the research team to highlight concerns regarding process which could be formally reviewed and amended if appropriate to do so. The majority of consent issues were protocol violations which involved a small number of participants (<5) and were a genuine oversight on behalf of an individual person. There was a significant impact for the research itself because tissue samples or data could not be used due to informed consent procedures not having been followed correctly. Informed consent is a fundamental ethical principle in research and the requirement to adhere to ethically approved informed consent processes should not be underestimated.

The issues in relation to not re-consenting participants in light of further safety information becoming available were of greater concern and hence were considered to be a serious breach for 6 out of 9 notifications. There were examples of members of the research team not following direct instructions to re-consent participants at the next scheduled visit, a delay in the sponsor providing the revised Investigators Brochure, misunderstanding of processes and confusion regarding the correct version of documentation. One notification indicated that there had been previous problems with the individual site in regard to re-consenting due to new safety information.

The Investigators Brochure is a document which is prepared from all available information and evidence that supports the rationale for the proposed clinical trial and the safe use of the IMP in the trial.

One breach notification received which involved not re-consenting in light of new safety information stated that the study team had been confused between the previous and revised versions of the participant information sheet and informed consent form. As a result of this, none of the 7 participants had been re-consented at this site, despite having been informed of this requirement and subsequently being followed up to monitor compliance with this requirement. It was noted that this was the only site involved with this particular study where this had occurred. This would imply local processes had failed. Another example of not re-consenting in light of new safety information involved 3 superseded versions of the participant information sheet and consent form for which participants had not been re-consented. A number of other protocol violations were also reported for this study. All participants were subsequently re-consented and all relevant staff underwent further training. These examples demonstrate the potential for actual participant harm where there is no valid informed consent in place which could have been prevented by improved version control and document management systems to ensure that there is clarity regarding current versions of important documents.

Recruitment outside of the inclusion criteria was the most commonly occurring breach and 13 of the 20 breach notifications were considered to be a serious breach. In some cases, this was considered to be a serious breach due to this compromising data integrity as well as some examples of where this caused actual or potential harm to the safety or physical or mental integrity of participants.

An example of where this had the potential to have a serious impact was a clinical trial with the inclusion criteria being post-menopausal women. Two participants (two different studies with the

same Contract Research Organisation) were enrolled without clinically confirming menopause and one of the participants subsequently became pregnant. A blood test had confirmed that she did not meet the inclusion criteria for the study but this was overlooked at the point of screening. The importance of contraception had not been included in the participant information as the assumption was that this would not be relevant. The impact of recruiting pre-menopausal women into this study and the possible adverse outcome was significant. This was compounded by the usual 'safety net', in terms of the requirement for robust contraceptive arrangements, not being in place.

In the significant majority of breaches which included recruitment outside of the inclusion criteria, information confirming that the participant was available and was either over looked accidentally or deliberately ignored. In some cases, the breach notification was followed by a substantial amendment to change the inclusion criteria. In cases such as this, the root cause may have been insufficient pre study planning or protocol design.

For breaches which fell into the consent/IMP/recruitment category, there were few corrective actions put in place which were not to some degree foreseeable. This would suggest that by building in simple safety nets to well thought through processes and protocols, such protocol breaches could be greatly reduced.

Again, these breaches should be considered in the context of the large number of studies being conducted in the UK. 6000 applications approved by RECs per year of which around 1000 will be drug trials.

Table 4.1.2

Consent/PIS/Recruitment	Serious breach	Violation
CF error	1	1
CF not approved	0	1
CF not completed	1	1
Consent not obtained	1	8
Consented by inappropriate person	1	1
Incorrect PIS / CF being used	0	3
Non approved study docs	0	1
PIS / CF not updated	0	1
PIS error	1	1
Protocol error	0	1
Re-consent not obtained	6	3
Recruited from site not listed on app	1	1
Recruitment outside inclusion criteria	13	7
Signed CF misplaced	0	1

4.1.3 Record Keeping

Table 4.1.3 sets out the breaches which relate to record keeping. Good record keeping is essential to be able to ensure that the study is being conducted accurately, consistently and according to the protocol, legislation and good clinical practice.[1] Schedule 1, Part 2, paragraph 10 of the Medicines for Human Use (Clinical Trials) Regulations states that all clinical trial information shall be recorded, handled, and stored in a way that allows its accurate reporting, interpretation and verification. For CTIMPs, the essential study documents are the ones which are usually audited by the sponsor's independent audit function and inspected by the regulatory authorities as part of the process to confirm the validity of the trial conduct and the integrity of data collected.[2]

The most commonly reported breaches in regard to record keeping were record keeping not being complete, not being accurate and problems verifying source data. Commonly cited reasons were staff pressures and changeover in staff. In most cases, problems with record keeping was only one of a number of issues reported as part of the breach notification, further issues often being highlighted as part of the investigation process. There was one example of a serious breach for poor record keeping which led to an inspection by the MHRA GCP Inspectorate during which it was identified that there were systemic problems with internal processes and staff following standard operating procedures. The impact was that the site ultimately closed.

There were also reports of inability to verify source data. This was particularly an issue where this related to verifying whether participants met the inclusion criteria for the study. In one example it was not possible for monitors to confirm that four out of eight participants enrolled into a clinical trial met the inclusion criteria as test results required to confirm this could not be located. The Chief Investigator was informed that no further protocol procedures should be undertaken until compliance with the inclusion criteria could be confirmed. One participant was subsequently found not to meet the inclusion criteria and withdrawn from the study. This also impacted on the study overall due to the time required to investigate and rectify the situation.

Table 4.1.3

Record keeping	Serious breach	Violation
Inconsistent with source doc	1	0
Record Keeping Not accurate	4	2
Record keeping Not complete	9	1
Records completed retrospectively	1	0
Investigator completing study docs	0	1
Not kept	0	1
Source data missing	1	0
Unable to verify source docs	2	1

[1] Good Clinical Practice Guide pg 177
[2] NIHR Guide to Good Clinical Practice

4.1.4 Safety Reporting

The requirements for safety reporting and the definitions of adverse events, serious adverse events and sudden unexpected serious adverse reaction should be clearly defined, including who is responsible for what. The breaches which occurred in relation to safety reporting were largely due to the process itself not being clearly defined or people not knowing or fully appreciating their responsibilities within the process. Some breach notifications received were study specific and some were in relation to the organisation more generally, with a large number of studies affected or potentially affected. In almost all cases, the proposed preventative action was re-training of the relevant people and improving processes.

Whilst none of the breaches reported in regard to safety reporting indicated that there had been any harm to participants as a result of the breach, there is potential for this to occur if processes are not clear or not followed. There is also a potential risk to a CTIMP sponsor organisation that should failings be identified as part of an MHRA inspection.

Table 4.1.4

Safety reporting	Serious breach	Violation
Delayed safety reporting	2	5
SAE(s) not reported	3	3

4.1.5 Appropriate approvals not being in place

Table 4.1.5 sets out the reported incidents of research proceeding without the appropriate approvals being in place. The majority of incidents were in regard to R&D approvals not being confirmed prior to the research commencing and substantial amendments being implemented prior to the appropriate REC approval being confirmed. The root causes of these incidents in all cases were either misunderstanding of the correct process or miscommunication between the R&D office and the Chief Investigator which led to a misunderstanding that approvals were in place. It was usually the case that there had been a deviation from the standard process in the form of further information having been requested by the R&D office prior to confirming approval; such as a requirement to confirm funding after the favourable ethical opinion was in place for a CTIMP but prior to the study commencing. In this case, funding was subsequently confirmed and the study started but formal R&D permission had not been confirmed by the R&D office. As the R&D approval was not formally in place, the study commenced without the conditions of the favourable ethical opinion having been fully met. The study was suspended to recruitment whilst a full investigation was undertaken to ensure that no other GCP breaches had occurred and to ensure that the correct approvals were in place. This impacted the study and the sponsor in terms of time and resources.

Issues with substantial amendments being implemented prior to formal approval from the REC included incorrect classification of amendments, misunderstanding regarding the requirements of the process and requested changes by the MHRA for a substantial amendment in the protocol leading to a new version which was not sent to the REC for review as they had approved the version submitted with the initial substantial amendment. This particular example highlights the issue of version control of documents, which is a theme evident in a number of breach notifications, and is a

problem which is often identified as part of the audit process which takes place when other issues have been identified. The requirement to update documents on the request of differing organisations at differing stages throughout the life of the research project can be problematic and requires good document control management systems.

One breach notification was received in regard to a study taking place without an active Clinical Trial Agreement from the Competent Authority (the MHRA being the Competent Authority in the UK) or a favourable ethical opinion being in place. This was in relation to a study which was in a follow up phase and the understanding was that a CTA was no longer required and the study was therefore declared as ended to the MHRA. An end of study declaration was also sent to the REC, stating that follow up would continue for a further 10 years. It has since come to light that the follow up phase would still be classified as a clinical trial requiring a CTA. The root cause of this issue appears to be misunderstanding regarding the classification of a clinical trial requiring a CTA and the requirements for end of study reporting. The implication for the study and researchers however is high due to an active CTA being a legal requirement.

Table 4.1.5

No approval	Serious breach	Violation
No R&D approval	1	3
Amendment implemented without approval	3	2
No CTA	1	0
No REC approval	2	2

4.1.6 Tissue

Table 4.1.6 demonstrates the breaches notifications received in regard to tissue. All notifications received related to samples being used other than as described in the study protocol. Examples include undertaking tests which were not consented for due to differing requirements in different countries and samples being taken for optional testing which was either not included in the consenting process or explicitly not consented to. In one case, samples were taken from seven participants who had not consented to additional genetic testing at screening and then at each 8 week follow up until the error was identified as part of an audit.

The consequence in some cases was that the samples were destroyed and not used and in some cases participants were contacted to request consent. This had an impact on participants in terms of extra samples having been taken which were destroyed and therefore served no purpose. There was also an impact on the study, research team and sponsor in terms of time and resource.

Table 4.1.6

Tissue	Serious breach	Violation
Samples used outside protocol	1	2

4.1.7 Data Protection

Table 4.1.7 sets out the breach notifications which have been received in regard to breaches of the Data Protection Act. The majority of breaches were considered to be a violation and were not intentional. This included confidential information being transferred electronically to an incorrect destination, paper records and lap tops containing personal information being stolen and study documentation containing personal information being kept at the home of a member of the research team. The requirements to adhere to the Data Protection Act extend beyond research and the expectation would be that organisations should have mechanisms in place to prevent breaches of the Data Protection Act and manage breaches when they do occur, including informing the Information Commissioners Office and those affected when appropriate to do so.

Table 4.1.7

Data Protection	Serious breach	Violation
Data Protection breach	3	11
Patient notes accessed outside clinical care team	0	1

4.1.8 Other

Table 4.1.8 sets out some other issues which were identified through the breach notification process which may impact the outcome of the study and were not covered by the other breach categories. Only breaches which fell into the 'other' category on the Breach Register and had occurred more than twice are included in this section.

There were 6 incidents which included either accidental un-blinding, and therefore had the potential to affect the study outcomes, or a delay to un-blinding, and therefore had the potential to harm the participant. Incidents of accidental un-blinding were most often due to not following the approved protocol, inadequacies with the protocol or ineffective electronic systems.

There was no indication of actual participant harm occurring in either of the breaches where un-blinding was delayed but potential for this to occur was identified in one breach notification. One incident involved the investigator having to contact the medical monitor who can authorise un-blinding. Concern was expressed in regard to accessing the named individuals out of standard working hours. In the other incident, the participant had been admitted to ICU with pneumonia which was thought to be potentially related to the study drug and un-blinding was therefore requested to confirm the initial treatment assigned during the blinded phase of study (the study was now in the open label phase). The Participant died five days after being admitted to ICU. There was a three day delay before un-blinding took place which involved a number of people trying and unsuccessfully un-blinding using a web based electronic system. The root cause of this incident was noted to be problems with the functionality of the system and also clarity in regard to use of the system. Whilst the delay in un-blinding was not considered to have caused direct harm to the

participant as such, there may be a psychological impact on the participant or family members during the three day period it took find confirm the initial treatment, which should be given consideration. There was also a further impact on the study team and sponsor in terms of time and resources to rectify the problem which may have been preventable with clearer written processes and better training of the research team in regard to using the web based electronic system.

Reasons for randomisation not being correctly implemented were not adhering to the protocol, including members of the research team pre-selecting the randomisation for some participants, inadequacies with the protocol, implementing randomisation prior to a substantial amendment having been approved which resulted in one arm not being randomised to, an error with IMP packaging which meant participants did not receive the IMP for the arm they had been randomised to and human error with researchers ticking an incorrect box on a form. In all cases the study data was deemed to have either been confirmed as impacted or potentially impacted. In two cases, recruitment was temporarily halted until the matter was investigated and rectified which would have impacted on the study and sponsor in terms of time and resources.

Table 4.1.8

Other	Serious breach	Violation
Accidental un-blinding	2	2
Delayed un-blinding	1	1
Randomisation incorrectly implemented	5	4
Test results missing	1	2
Tests not undertaken	6	1

5 Impact of breaches

5.1 Participant

An adverse impact on study participants identified through breach reporting was relatively low. The themes and trends which were identified in regard to adverse impact on participants were as follows;

i. The potential for mental or emotional impact on participants or their family whilst awaiting confirmation of whether the breach had led to harm.
ii. Procedures being undertaken without consent which goes against the fundamental principle of informed consent and compromises the rights of participants.
iii. Recruitment outside of the inclusion criteria. This can lead to actual harm and also compromise the rights of participants who are unable to give fully informed consent when recruited to a trial for which they do not meet the inclusion criteria.
iv. Time wasted due to undergoing study procedures where the participant was subsequently withdrawn from the study or tissue or data could not be used. This would also include participants who are recruited when they do not meet the inclusion criteria.
v. Delayed un-blinding.

5.2. Other than participant

Other than participant harm, there were notable impacts in relation to the study itself, the study team and the sponsor or host organisation. Table 5.2.2.1 shows the number and percentage of serious breaches and violations which resulted in recruitment being halted for a period of time. Whilst in the wider context this would be considered to be a low number of studies, the requirement to halt recruitment can have a significant impact in a number of ways and is often avoidable.

Table 5.2.1

	Serious breach	Violation
Recruitment halted	15 (21%)	4 (5%)

All breach notifications were reviewed for evidence of inspection by the MHRA being required. Breaches were also checked on the MHRA breach tracking document which is shared with the HRA on a quarterly basis. This indicated that in total, 10% of serious breaches are flagged as requiring some level of MHRA inspection. 6% of studies required a triggered inspection whilst 4% were reviewed as part of the standard routine inspection programme. Only one serious breach in 2013/14 requiring a triggered inspection identified a critical finding. The outcome of this was that the commercial unit voluntarily suspended all clinical procedures and after further investigation, the site subsequently closed. The critical findings were not in relation to participant harm.

Table 5.2.2

MHRA Inspection	Serious breach	Violation
Routine	3 (4%)	0
Triggered	4 (6%)	0

A more significant number of serious breaches resulted in either a 'for cause' audit or additional monitoring as a direct result of the breach. The consequence of this is that further time and resources are required which has an impact on the sponsor.

Table 5.2.3

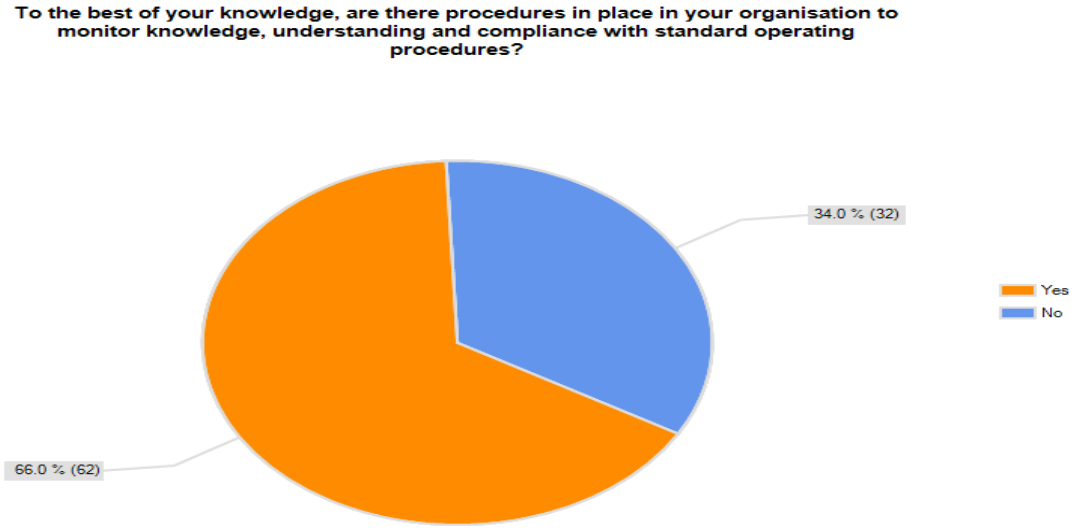
	Serious breach	Violation
For cause audit / monitoring	20 (29%)	4 (5%)

Table 5.2.2.4 sets out the route by which the breach was initially identified. It is reassuring to note that a significant percentage of breaches were reported by the study team. This is supported by feedback from the R&D survey, although it was also evident that improvements could be made.

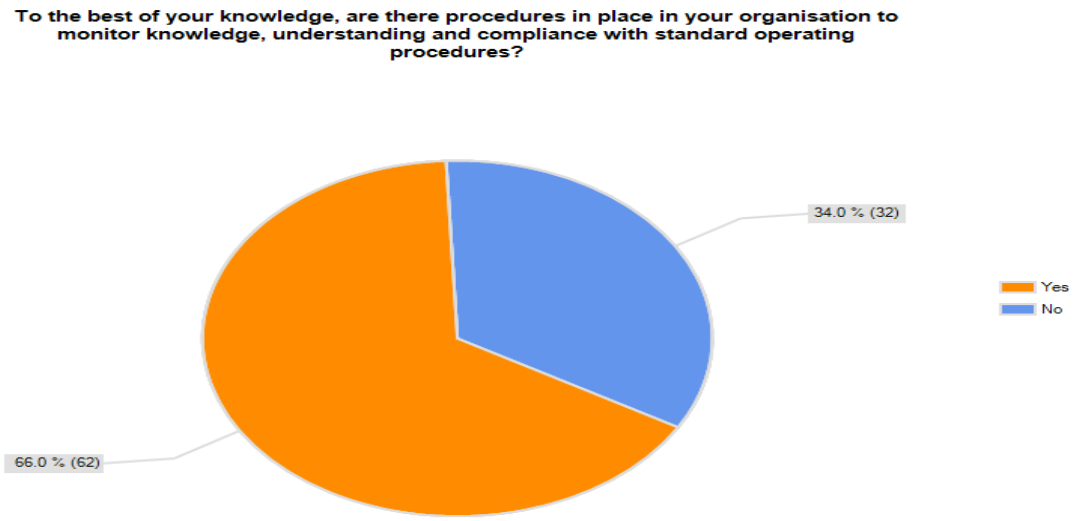
"Breaches are generally detected by staff who report them spontaneously. Their knowledge of breaches and breach reporting is good but could always be improved"

"All our CTIMPs are coordinated by experienced research nurses so in these cases any breach is identified and acted upon immediately. Non CTIMP studies, well, I am sure breaches can occur and we may miss them, but generally our study leads / coordinators are 'up front' and report them to us."

In response to the question "To the best of your knowledge, are all individuals involved in research in your organisation made aware of the standard operating procedures regarding breach and fraud or misconduct reporting?" The response was as follows:



In response to the question "To the best of your knowledge, are there procedures in place in your organisation to monitor knowledge, understanding and compliance with standard operating procedures?", the response was as follows:



This would suggest that there may be improvements to be made in regard to ensuring that all staff involved with research are aware of the procedures and that there are mechanisms in place to monitor understanding and compliance. It is important to acknowledge that just having a standard operating procedure is not in itself always effective. It is essential that staff are aware of the procedures, have a good understanding of the procedures and feel empowered to report breaches in accordance with such procedures by encouraging an open and honest reporting culture. The primary aim of breach reporting and investigation should be to ensure that errors are corrected to prevent adverse impacts.

Comments from the R&D survey suggested that there may be a misunderstanding that reporting a breach may lead to an MHRA inspection and have a negative consequence.

> *"There is perhaps a perception that reporting a breach will result in an unplanned visit from the regulatory authorities (MHRA) and that there will be a reputational risk to the researcher and the organisation. …There does need to be an increased awareness that there is not a blame culture"*

The importance of reporting breaches so that prompt action to resolve the issue should be made clear as this is the best way to reduce the overall impact and reduce the risk of wasted resources, such as data not being credible and therefore unusable.

Identification of breaches through standard processes such as routine audit is also important to note and clear requirements and processes would assist with this.

> *"We back up our SOPs with training sessions which are mandatory for all research staff, and are available to all clinical staff. It would be useful to know what other organisations are doing, or obtain a national standard for breach reporting to ensure that we are on the right track."*

Table 5.2.4

How identified	Serious breach	Violation
Audit	2 (3%)	4 (5%)
MHRA inspection preparation	2 (3%)	3 (4%)
Monitoring	25 (36%)	24 (28%)
R&D	4 (6%)	5 (6%)
REC	1 (1%)	2 (2%)
Research team	24 (34%)	26 (31%)
Sponsor	9 (13%)	4 (5%)
Unknown	3 (4%)	16 (19%)

Table 5.2.2.5 sets out the study type and breach classification for all breaches received during the reporting period. It is of note that 76% of all reported breaches are for CTIMPs (including healthy volunteer studies) yet this type of study make up only approximately 20% of the total number of applications which receive a favourable ethical opinion per year, which is disproportionately high. One possible explanation for this is that audit and monitoring arrangements are more robust for CTIMP studies. Another explanation is a perception that breach reporting is not a requirement for non-CTIMP studies. This perception was evident from some responses received to the questionnaire, as referenced above in section 4.

Table 5.2.2.5

Study type		
CTIMP	111	70%
Healthy Volunteer	9	6%
Other	37	24%

6. Conclusions

6.1. It should be noted that approximately 6000 studies were approved in the year 1 April 2013 to 31 March 2014 and only 70 breaches were reported which were considered to be a serious breach of the principles of GCP or the approved study protocol. Whilst there is an indication that breach reporting processes could be improved, particularly for non CTIMPs, this number is low in the overall context and suggests that research is well managed and should not be considered to be a risky activity.

6.2. Whilst the outcome of this work indicates that research should not be considered to be a risky activity, the potential impact on individual patients and participants and the potential to undermine the integrity and value of the research, as well as the potential for valuable resources to be wasted, should not be underestimated. Further work should therefore be undertaken to ensure proportionate and effective mechanisms are in place to monitor compliance with principles of GCP and approved study protocols.

7. Recommendations.

i. The importance of well planned and written protocols and internal processes.

Protocols and internal procedures should be clear, comprehensive and easily accessible by the relevant people. A number of breaches were identified as part of this project which were solely or partly due to poorly planned, unclear or non-existent protocols or procedures. There is a potential adverse impact on all parties involved as a result of inadequate protocols and procedures which can be significant and could be avoided.

ii. The importance of protocols and internal processes being followed.

Well planned and written protocols and procedures are only effective if they are followed. Within this review there was evidence of individuals purposefully not following the protocol or directions from the study sponsor for varying reasons. It is important to understand the root cause of non-compliance, this may be that the individual believed that the process was more efficient in another way or it may have been wilful defiance. Not adhering to the protocol has the potential for adverse impact in a number of ways and to all parties involved. For study participants, this compromises any informed consent given, for the researcher there is a potential for the credibility of study data to be compromised as well as a reputational risk and for sponsors there is often a financial and resource implication, particularly where a suspension to recruitment or extensive investigation or monitoring is required.

iii. The importance of good communication processes and lines of responsibility.

A number of breaches were identified as having occurred due to communication not happening or from being ineffective and from a lack of clarity regarding responsibility. There should be clear designation of responsibility and accountability with clear lines of communication between all those involved in research. Communication pathways should be clear in terms of what, how, who, when and why with documented roles and responsibilities.

iv. The importance of document management systems or good version control

There is often a requirement for documents to be revised and updated during the lifespan of studies and these requirements are often initiated by varying organisations. It is therefore important to ensure that the competent authority and ethics committee have reviewed and approved the most current version and that all those involved in undertaking research procedures are aware of the most current and approved version. Good document control for all is essential and needs improvement.

v. The need to ensure learning rather than just delivering training

Corrective and preventative action plans commonly cited training and re-training of members of the research time. This was often in relation to standard study procedures. It is however important to understand the root cause of non-compliance and having a more targeted approach rather than defaulting to providing training. Non-compliance may be due to not knowing the correct procedure, misunderstanding the correct procedure or wilful deviation, which may be due to poorly planned or unrealistic procedures. The targeted approach would differ depending on the root cause. It is

important to ensure that members of the research team are aware of the correct procedure but also that they fully understand what this requires and the importance of following it and that understanding and compliance is confirmed. It is also important to understand the wider context of error. If an individual makes an error due to insufficient time to complete a number of tasks, providing training will not in itself solve the problem or reduce the risk of the error being repeated.[3]

vi. The importance of encouraging open and honest reporting

It is widely recognised in healthcare that a culture of openness and honesty promotes safety. In clinical practice, incident reporting is strongly encouraged so that lessons can be learnt and improvements made. This principle is equally as valid in research both clinical and non-clinical. Errors can only be rectified and improvements made to reduce adverse impacts and increase the quality of research outcomes if they are reported in a timely way. For this to be truly effective, a culture of openness and honesty is essential with a focus on improvement rather than consequence.

8. Sharing of outcomes

One of the aims of this project is to ensure that learning which is derived from breach reporting can be shared more widely. The intention is for the findings from this project to be shared with relevant stakeholders in the interest of transparency and shared learning.

Communication Plan
1. What are we communicating and what do we want to achieve?
- The type of breaches which are most commonly reported - The consequences and impact of breaches - The importance of breach reporting to promote a culture of safety and improvement - Encourage shared learning - Promote a quality approach
2. Who do we want to communicate with?
- Research sponsors - Researchers - Research funding organisations - Patients and public involvement groups - Other regulators
3. What is their current understanding of the area?
- Current understanding of reported breaches is likely to be limited to individual experience of breach reporting and corrective actions rather than the wider view point - Requirements for the reporting of breaches
4. What outcome do we want in terms of what the communication recipient will know, think and do as a result of the communication?
- **Know**

[3] Clinical Risk Management, Charles Vincent.

- ✓ The types of breach which occur
- ✓ The consequence of breaches occurring
- ✓ The impact of breaches occurring

- **Think**
  - ✓ How can they use this information to improve breach reporting processes in their organisation?
  - ✓ How can they use this information to improve research processes in their organisation?
- **Do**
  - ✓ Share the information with colleagues
  - ✓ Implement the recommendation made into their organisation, as appropriate

5. What are the key messages for each communication recipient group, taking current understanding and intended outcome into consideration?

- **Research sponsors**
  - ✓ Breaches have an impact on studies and organisations in terms of time, finances, resources and also reputation
  - ✓ Many breaches can be avoided by good planning, learning from previous errors and having good systems and processes in place
  - ✓ Being proactive early on can reduce the consequence and impact of breaches
  - ✓ Breach reporting is important to promote shared learning and a culture of improvement

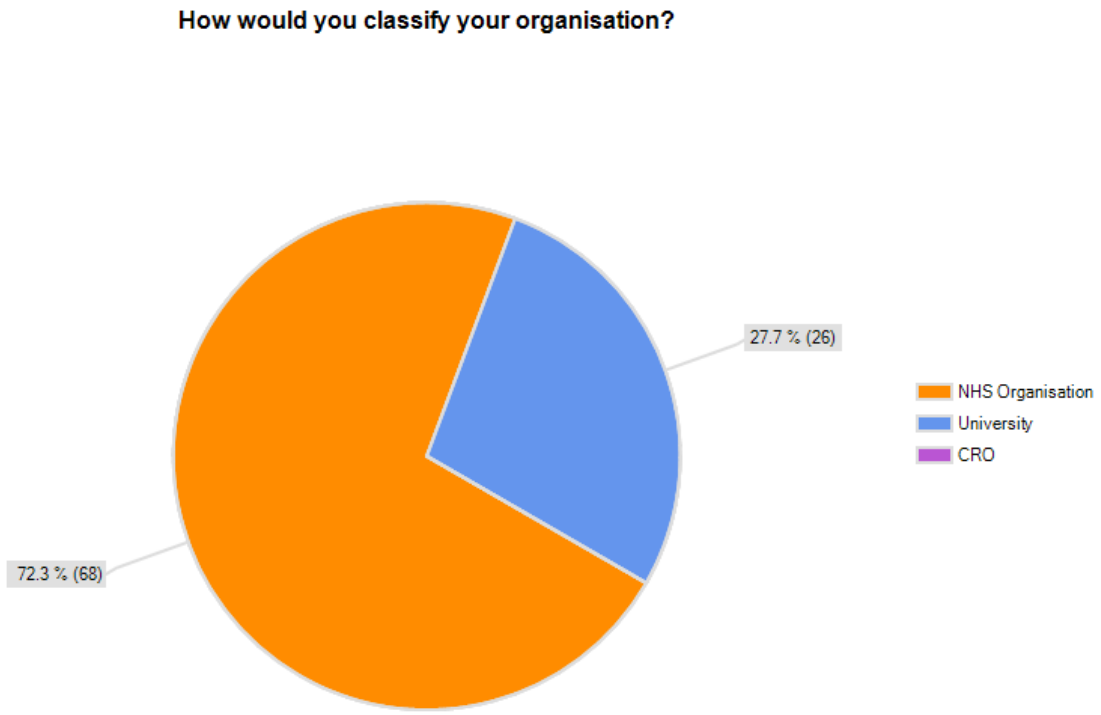
- **Researchers**
  - ✓ Breaches have an impact on studies and organisations in terms of time, finances, resources and also reputation
  - ✓ Many breaches can be avoided by good planning, learning from previous errors and having good systems and processes in place
  - ✓ Being proactive early on can reduce the consequence and impact of breaches
  - ✓ The importance of adhering to study protocols
  - ✓ Breach reporting is important to promote shared learning and a culture of improvement
- **Research funding organisations**
  - ✓ Breaches have an impact on studies and organisations in terms of time, finances, resources and also reputation
  - ✓ Many breaches can be avoided by good planning, learning from previous errors and having good systems and processes in place
  - ✓ Being proactive early on can reduce the consequence and impact of breaches
  - ✓ A quality approach is resource efficient
- Patient and public involvement groups
  - ✓ Research is largely well managed and closely monitored
  - ✓ The importance of undertaking research, some of which may be innovative and pioneering, to further healthcare and medical science
  - ✓ The HRA and other regulatory bodies strive to improve the quality of research for the benefit of all

6. Methods of communication delivery

- Presentations
- Articles
- External HRA communications

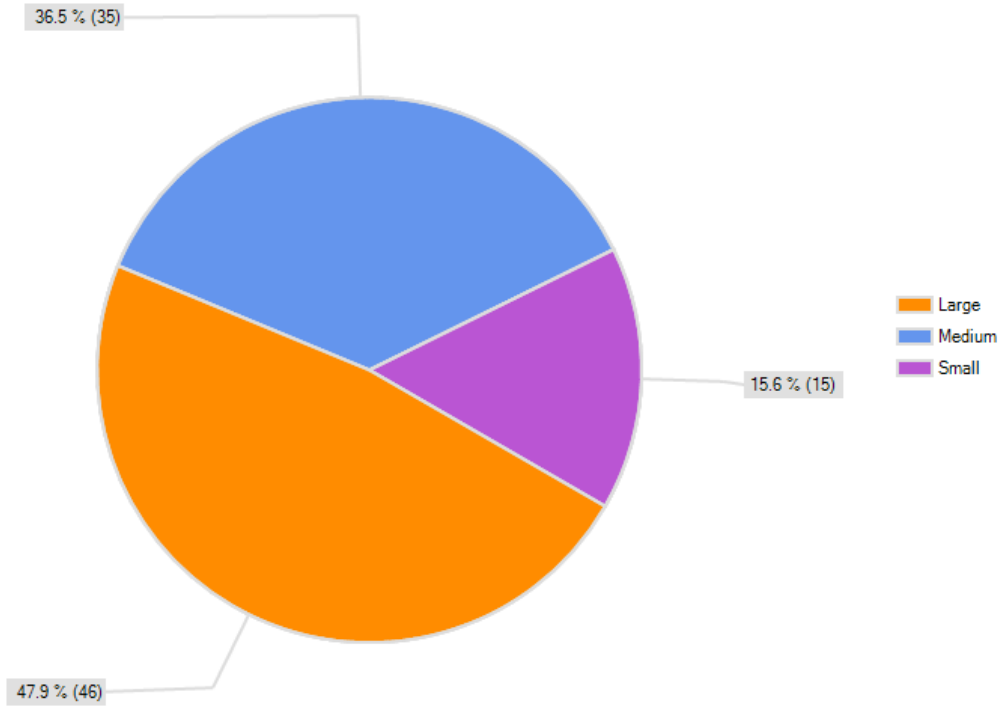
9. Appendix A

9.1 All responses

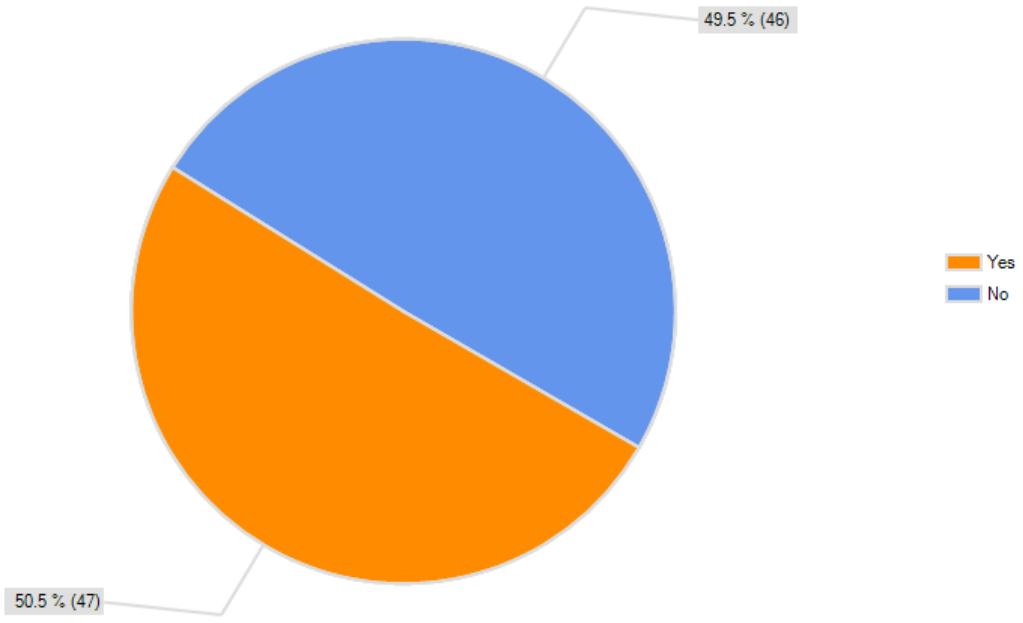


3 responses stated that they were a joint NHS Trust & University organisation.

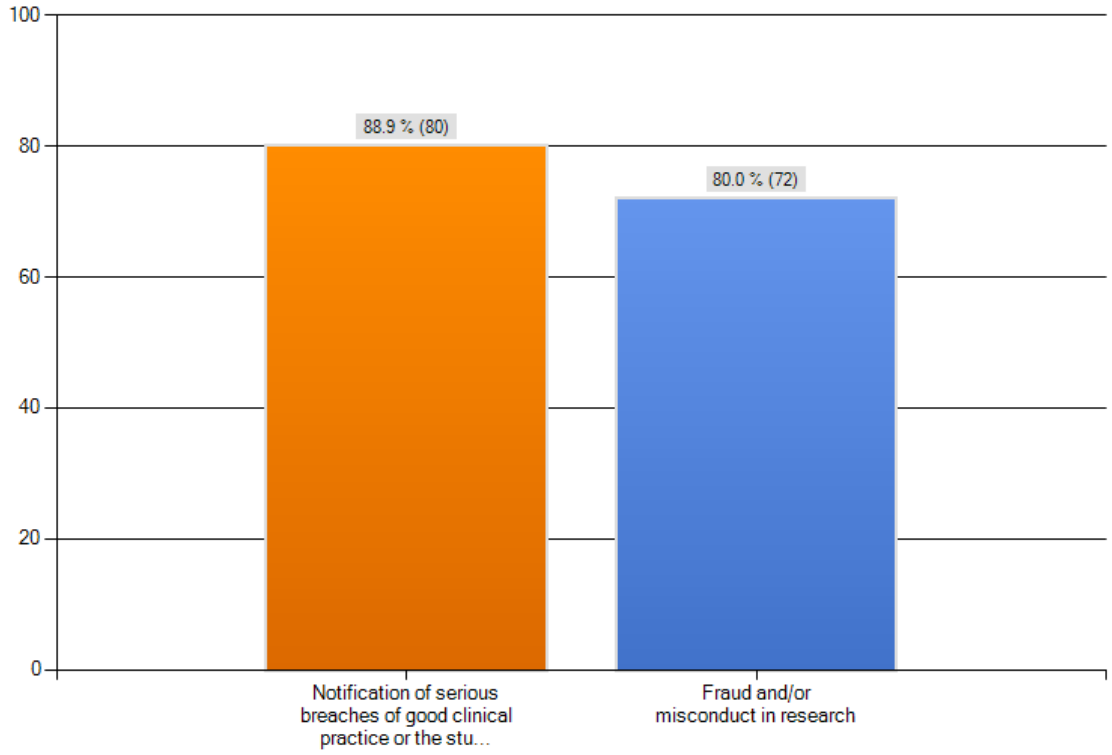
How would you classify the size of your organisation?



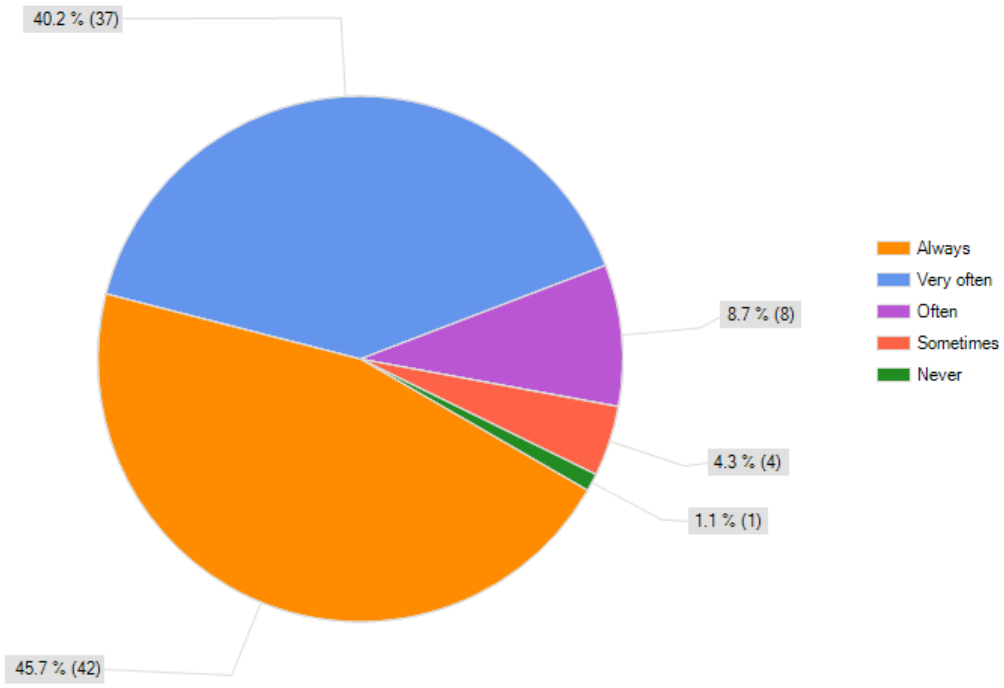
Does your organisation sponsor CTIMPs?



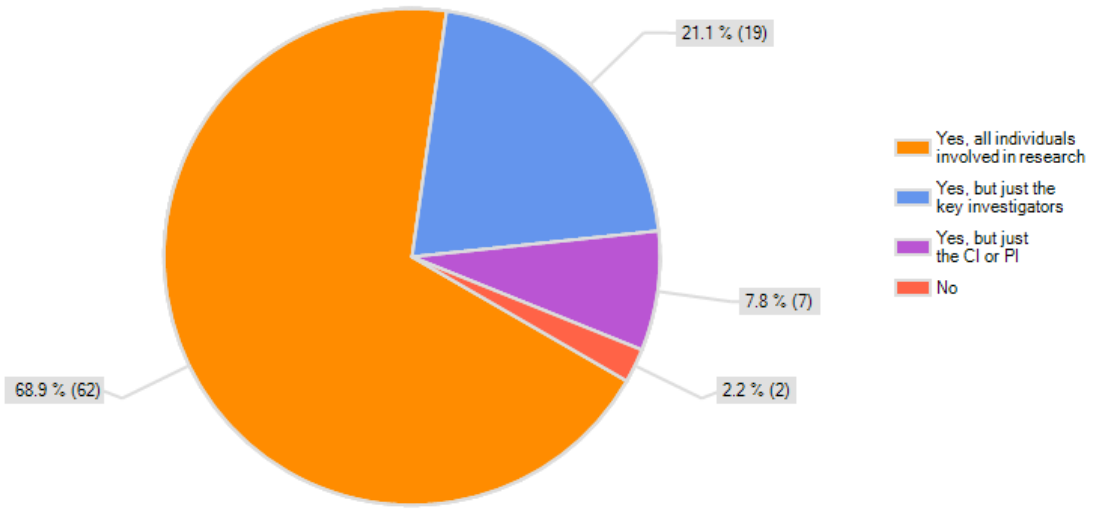
Does your organisation have stantard operating procedures for the following (please tick all that apply)



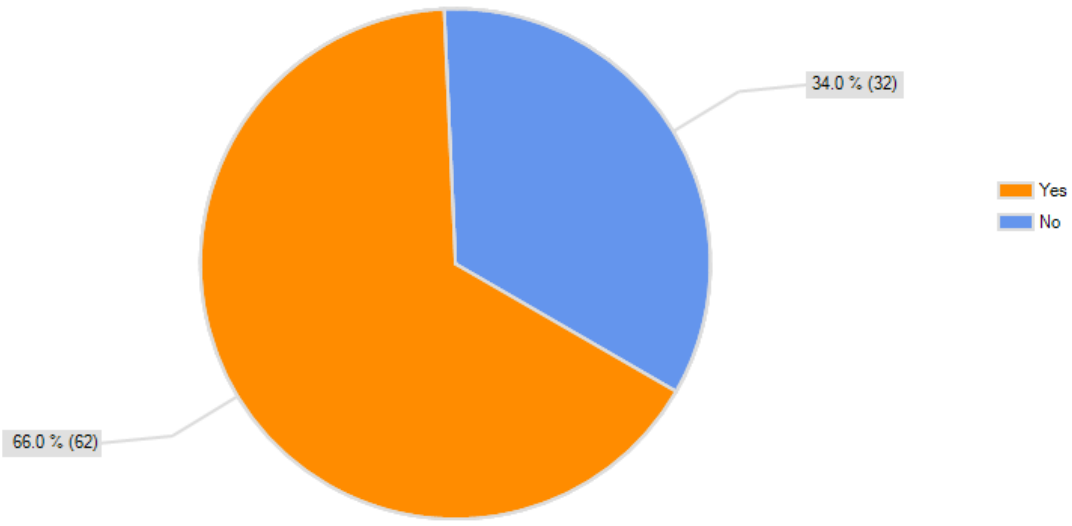
To the best of your knowledge, would you say that the standard operating procedures are followed...



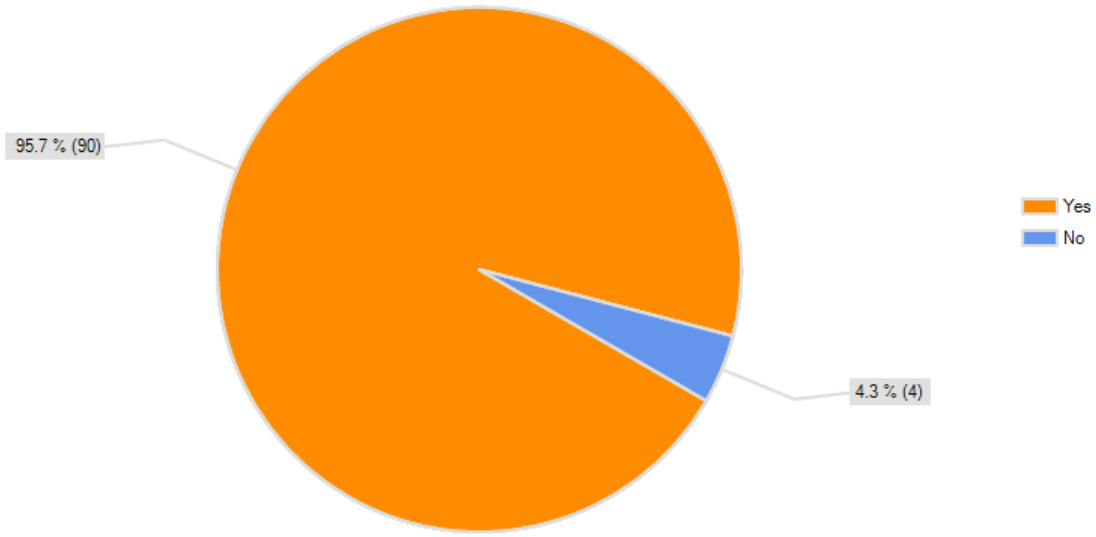
To the best of your knowledge, are all individuals involed in research in your organisation made aware of the standard operating procedures?

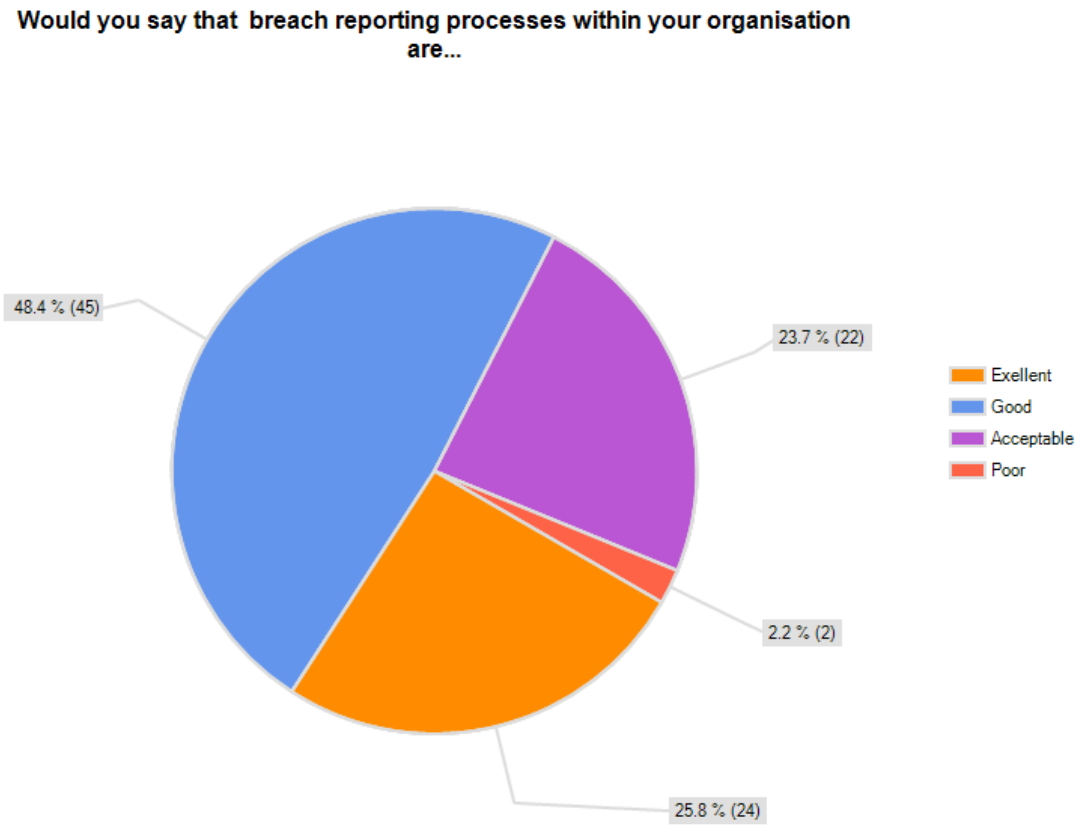


To the best of your knowledge, are there procedures in place in your organisation to monitor knowledge, understanding and compliance with standard operating procedures?

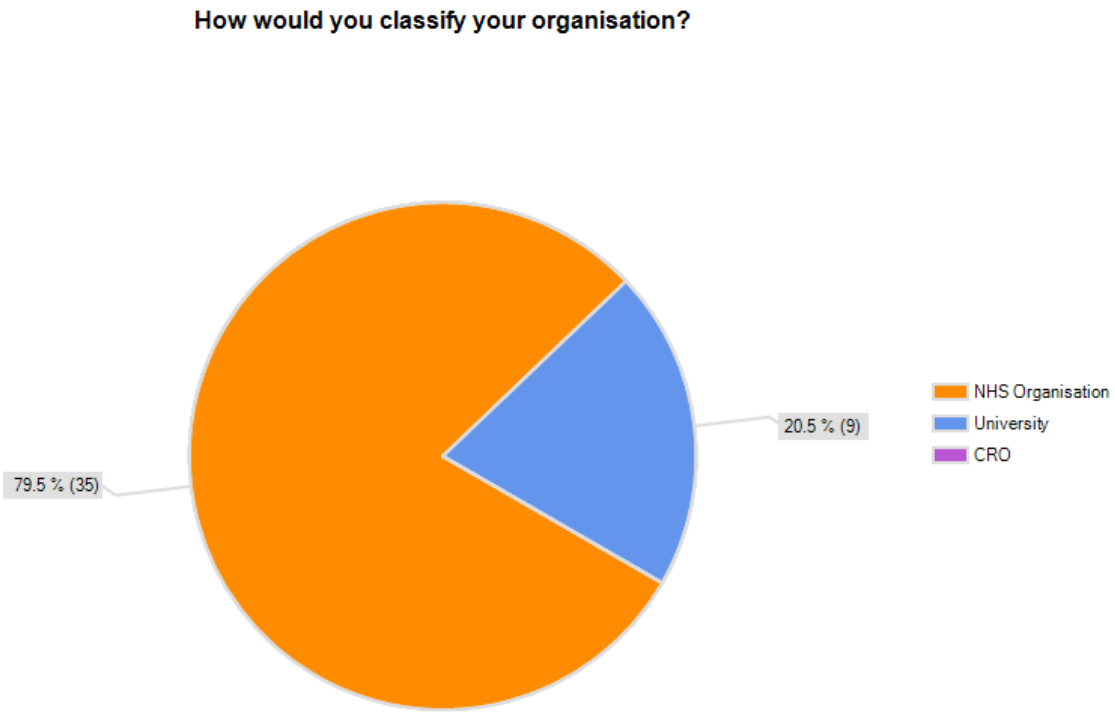


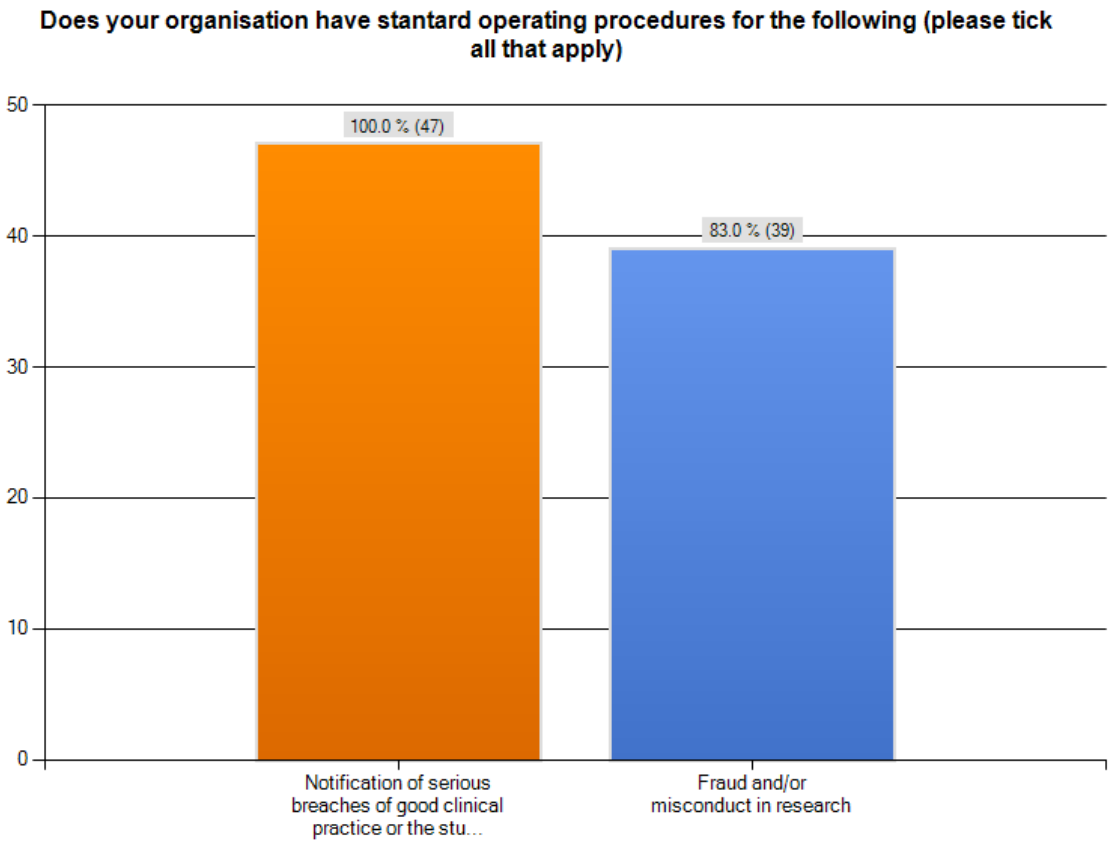
Are the standard operating procedures kept somewhere that is accesible to all appropriate staff?

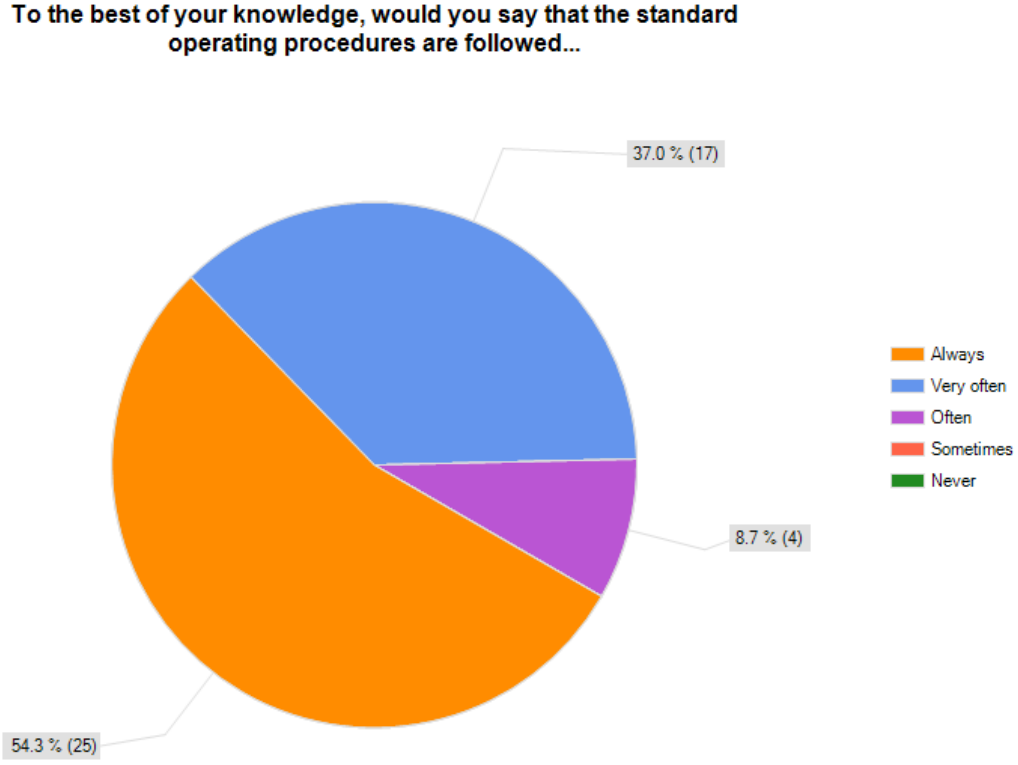



Would you say that breach reporting processes within your organisation are...
48.4 % (45)
23.7 % (22)
2.2 % (2)
25.8 % (24)
Exellent
Good
Acceptable
Poor

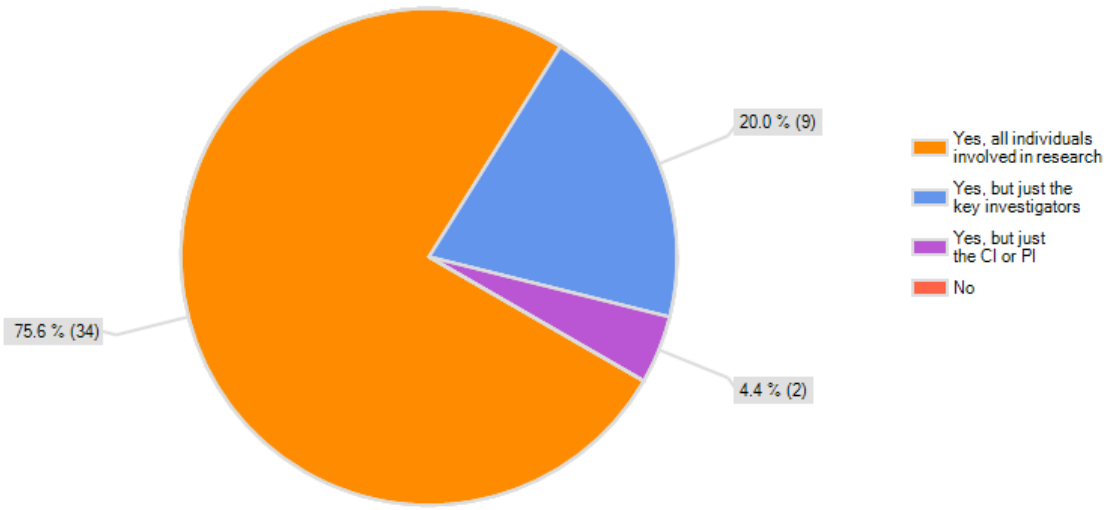
9.2 Organisations which sponsor CTIMPs only



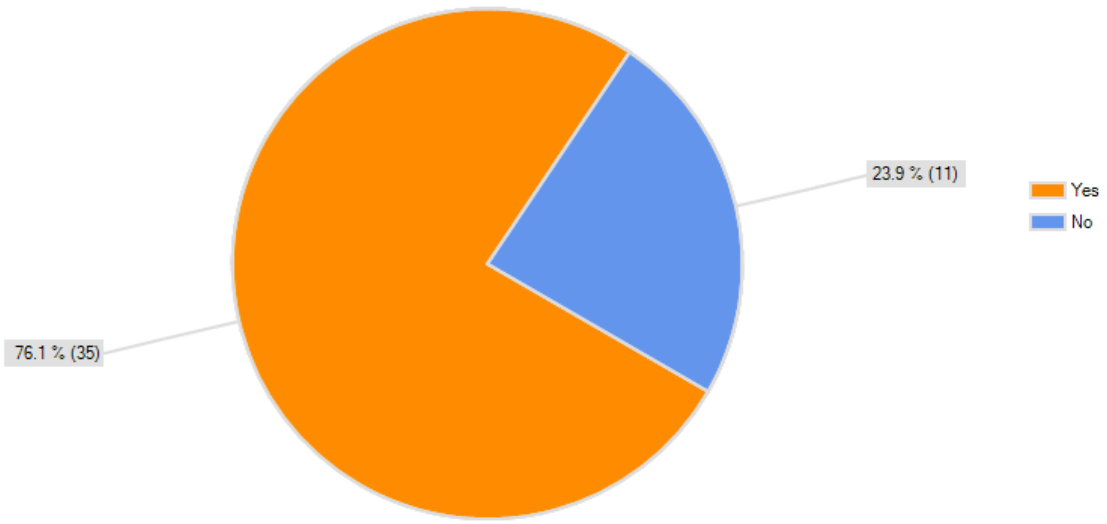

Does your organisation have stantard operating procedures for the following (please tick all that apply)
50
40
30
20
10
0
100.0 % (47)
83.0 % (39)
Notification of serious breaches of good clinical practice or the stu...
Fraud and/or misconduct in research


To the best of your knowledge, would you say that the standard operating procedures are followed...
37.0 % (17)
8.7 % (4)
54.3 % (25)
Always
Very often
Often
Sometimes
Never

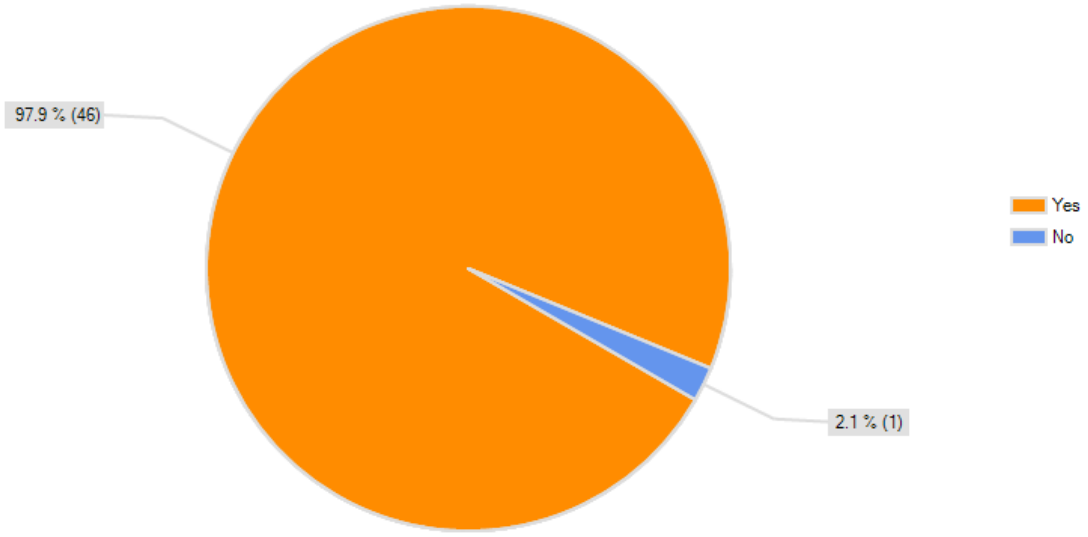
To the best of your knowledge, are all individuals involed in research in your organisation made aware of the standard operating procedures?



To the best of your knowledge, are there procedures in place in your organisation to monitor knowledge, understanding and compliance with standard operating procedures?



Are the standard operating procedures kept somewhere that is accesible to all appropriate staff?



Would you say that breach reporting processes within your organisation are...