Inspecting policing
in the public interest

Building the Picture: An inspection of police information management

Lancashire Constabulary

July 2015

ISBN: 978-1-78246-805-9

www.justiceinspectorates.gov.uk/hmic

Contents

1. Introduction

Her Majesty's Inspectorate of Constabulary (HMIC) is an independent inspectorate with a statutory responsibility to "inspect, and report to the Home Secretary on the efficiency and effectiveness of every police force maintained for a police area" in England and Wales[1.]

This report sets out findings from our review of the way police forces in England and Wales collect, record, evaluate and share information.[2]

Why information management is important

Information[3] is the lifeblood of the police service. It leads to effective investigations, timely arrests and appropriate criminal justice outcomes. It also helps to prevent further crimes being committed. Information is vital in the fight against crime.

Seemingly one-off instances of suspicious or criminal behaviour assume a greater importance if it can be shown, by linking information, that they are not isolated, but form a pattern of behaviour that gives rise to concern. The whole picture may well be greater than the sum of its parts. This is why linking information and building the picture of the crime are so important – and why the consequences of failing to make the right links can have a significant adverse impact on the public; for example, the mistakes that were made during the police handling of allegations against Jimmy Savile. This is discussed in more detail below.

The recent decision of the Supreme Court in *R (Catt) v Association of Chief Police Officers* [2015][4] emphasises the pivotal importance of complying with the Code of Practice on the Management of Police Information 2005, the associated Authorised Professional Practice (APP) on information management[5] and the former editions of

[1] Section 54(2) of the Police Act 1996.

[2] The intelligence management section of Authorised Professional Practice defines intelligence as "collected information that has been delivered for action" (www.app.college.police.uk). Thus, in policing terms, not all information is classified as intelligence, but all intelligence is a form of information. In this report, the term information includes both information and intelligence unless otherwise stated.

[3] In this report, 'information' is used to refer to both information and intelligence. See page 20.

[4] *R (Catt) v Association of Chief Police Officers of England, Wales and Northern Ireland and another (Equality and Human Rights Commission and others intervening)* [2015] UKSC 9.

[5] *Authorised Professional Practice on information management*, College of Policing, 2013. Available from www.app.college.police.uk/app-content/information-management/management-of-police-information/ This is the body of guidance published by the College of Policing to provide the police service in England and Wales with policy and procedures to follow.

the national guidance.[6] In her judgment, Baroness Hale echoes one of the main themes of this report in stating: “We do not need any reminding, since the murder of two little girls by a school caretaker in Soham and the recommendations of the report of the Bichard Inquiry which followed (2004) (HC 653), of the crucial role which piecing together different items of police intelligence can play in preventing as well as detecting crime.”[7]

Background: Mistakes Were Made

On 12 March 2013, HMIC published the findings of a review into how the Metropolitan Police Service, Surrey Police and Sussex Police dealt with the information and allegations which they received between 1964 and 2008 regarding the criminal sexual conduct of the late Jimmy Savile.[8]

This review considered the way in which these forces applied the Code of Practice on the Management of Police Information 2005, the APP on information management[9] and the former editions of the national guidance[10] in dealing with the information and allegations. It also examined the extent to which those forces made effective use of the Police National Database[11] to aggregate discrete pieces of information (from within and across forces) and so build a picture of the extent and nature of the alleged offending.

[6] Code of Practice on the Management of Police Information issued under sections 39 and 39A, Police Act 1996 and sections 28, 28A, 73 and 73A of the Police Act 1997. Available from http://library.college.police.uk/docs/homeoffice/codeofpracticefinal12073.pdf

[7] *Ibid*, para 48.

[8] *"Mistakes Were Made" - HMIC's review into allegations and intelligence material concerning Jimmy Savile between 1964 and 2012,* HMIC, March 2013. Available from www.justiceinspectorates.gov.uk/hmic/media/review-into-allegations-and-intelligence-material-concerning-jimmy-savile.pdf

[9] *Authorised Professional Practice on information management*, College of Policing, 2013. Available from www.app.college.police.uk/app-content/information-management/management-of-police-information/ This is the body of guidance published by the College of Policing to provide the police service in England and Wales with policy and procedures to follow.

[10] *Guidance on the Management of Police Information*, 1st edition, Central Police Training and Development Authority, 2006, produced by the National Centre for Policing Excellence, and the second edition of the same, produced by the National Policing Improvement Agency in 2010. It is referred to in this report as ‘national guidance’.

[11] The Police National Database is a national information management system that improves the ability of the police service to manage and share information, to prevent and detect crime and make communities safer. It offers a capability for the police service to share, access and search local information electronically, overcoming artificial geographical and jurisdictional boundaries.

HMIC concluded that mistakes had been made in the handling of information and allegations and stated that we were “sufficiently concerned about information management" to conduct a further review in this area. This inspection fulfils this commitment and answers the question: could the same mistakes be made again?

Methodology

Our principal inspection objectives were to establish:

- if force strategies, policies and procedures for information management adhere to the principles of the APP on information management and former editions of the national guidance, are proportionate to risk and fit for purpose;
- if information and intelligence are captured, recorded, evaluated, acted upon, audited and retained by the police (including safeguarding interventions) in an effective way; and
- if the use of the Police National Database is effective and efficient.
- To answer these questions, HMIC analysed the results of a self-assessment survey[12] of information management practices which was completed by all 43 forces in England and Wales in 2013 (to give an indication of the national picture), and conducted three days of fieldwork in each of 13 forces.

National inspection findings

Given that chief constables are obliged to have regard to the Code of Practice on the Management of Police Information 2005, we expected that either:

- they would ensure that their forces complied with the Code, and with the relevant section of the APP on information management or former editions of the national guidance;[13] or
- if, because of their local context and operating environment, they decided not to comply with elements of the APP on information management or former editions of the national guidance, that proper records would be maintained about the extent of and rationale for any move away from the Code.

[12] This survey was commissioned by the ACPO Information Management Business Area Lead, and conducted on his behalf by the College of Policing. We are grateful for permission to use the results.

[13] *Authorised Professional Practice on information management*, College of Policing, 2013. Available from www.app.college.police.uk/app-content/information-management/management-of-police-information/ This is the body of guidance published by the College of Policing to provide the police service in England and Wales with policy and procedures to follow.

We were therefore disappointed to find that the reasons for decisions to depart from the APP on information management or former editions of the national guidance were only recorded in three of the 13 forces we inspected.

We also expected each force to have in place a current information management strategy – a requirement stipulated in the Code of Practice on the Management of Police Information 2005. Again, we were disappointed to find that this was not always the case.

In the light of case law and high-profile cases such as Jimmy Savile's long period of sex offending, we are materially concerned about the extent to which the police service is responding fully to the responsibilities inherent in a changing environment, where speedy access to up-to-date and relevant information is essential. For example, we found cases where forces had not revisited their position since the whole of the police service completed local information management implementation plans in 2010. In this regard, the absence of appropriate audit and assurance regimes (to check that information is being appropriately assessed, retained or disposed of) is especially worrying, and needs to be addressed swiftly.

HMIC found that forces which maintained a central information management team were better able to adopt the principles of the APP on information management and former editions of the national guidance. This was especially so when those teams had access to an integrated computer system that was able to reference and facilitate the assessment of all the information held on a named individual without the need to search separate computer systems.

It is a matter of serious concern that there is insufficient review taking place of the information that forces hold. Without these reviews – and the means to demonstrate that they have taken place properly or at all – the police service leaves itself vulnerable to challenge. The absence of sound and consistent reviews means that information might be destroyed when it should be kept, thus increasing the risk to public safety.

The volume of information acquired by the police means that not every piece of information can be evaluated and processed at the same time. The question then arises of how to identify those pieces of information which demand more immediate consideration than others. Clearly, the information which informs the police of a greater or more immediate risk to the public should be considered as soon as possible. We found that the extent to which information was reviewed, prioritised and indexed – and the capacity to undertake this exercise – varied between and within forces.

A significant strand of our inspection examined how sensitive information[14] is handled, particularly when it is acquired and held as a result of specialist policing activities such as major crime investigations, counter-terrorism investigations and internal investigations of police officers and staff for misconduct, or corruption or other criminal offences. We found that there is scope for better integration between the IT systems which house sensitive information and the mainstream databases available to the police (such as the Home Office Large Major Enquiry System[15]). There is also scope for more effective processes to transfer information between systems; while our inspection found some awareness of the problems caused by the lack of such processes (for instance, some forces are developing the means to identify, isolate and transfer appropriate records on a case-by-case basis), there is more to be done.

Where information is marked as sensitive, the police must undertake reviews from time to time to determine whether such a classification remains appropriate. The importance of information fluctuates with the passing of time, and the police service should do more to act on those fluctuations. We found evidence that different practices are being followed in the 43 police forces in England and Wales with regard to the handling of sensitive information.

We were also concerned to note that only four of the forces we visited had a force-wide policy setting out how sensitive information should be treated; and even in those four forces, we did not find any evidence to show that compliance with the policy was being monitored to ensure that it was being followed. The absence of consistent practice together with differences of approach in implementation results compromises the ability to manage information effectively.

As a result of these findings, we have made ten recommendations (for the Home Office; the national lead for information management business area; chief constables and the College of Policing). These are set out on page 11.

Inspection findings in Lancashire

In the rest of this report, we describe our findings for the Lancashire Constabulary inspection which we undertook between the 21 and 23 July 2014. These should be read alongside the thematic report, *Building the Picture: an inspection of police information management*, which is available from www.justiceinspectorates.gov.uk/hmic/wp-content/uploads/building-the-picture.pdf

[14] 'Sensitive information' is that which is contained in specialist business areas, and generally hosted and used outside mainstream policing intelligence systems and processes. It is therefore only available to specialist officers. Examples include information on current operations; major crime investigations or counter-terrorism information; and information held by professional standards directorates.

[15] An ICT system used for major crime investigations.

2. Findings for Lancashire Constabulary

General

An assistant chief officer is the senior information risk owner for Lancashire Constabulary with the deputy chief constable leading on information assurance and security.

The assistant chief officer chairs an information assurance board that provides overall governance. There had historically been issues of low attendance but, at the time of inspection, the situation had improved. The Office of the Police and Crime Commissioner was not represented at the board.

There has been a significant decrease in the number of staff working in the information management business area. At the time of inspection, there was no force information manager or records manager in post; these absences may be responsible for the lack of corporate information management processes. In addition, two senior information managers had left the organisation.

Collection and recording

Intel2, part of the force Sleuth system, is the primary intelligence system used by the force to store and manage intelligence records. It allows staff to search across and view records from multiple internal applications including the briefing and tasking pages, allowing staff access to intelligence records and targeting plans.

The force has a computer system known as CLUE for the management of sensitive information. This was used by specialist investigation departments, such as the one which deals with serious and organised crime syndicates, to protect the sensitive information they may generate. There was an expectation that sensitive information would be assessed at the conclusion of a serious crime operation and, where possible, made more widely available as general intelligence. Additionally, sensitive information would be assessed by staff from the sensitive intelligence unit when it is being entered on the system and should be transferred where appropriate to Intel2. Priority is given to records related to sexual offences, firearms and officer safety.

At the time of inspection, there had been a structural reduction, relocation and realignment of locally-based intelligence assistants to complement a force intelligence department central processing unit. Their role is to assess and distribute force intelligence. There was a backlog of approximately 1,500 records awaiting review. While this backlog does not necessarily result in delays to local action, records are not sent to the Police National Database (PND) until they have undergone a local assessment by the central processing unit.

Responsibility for the intelligence reviews required and described in the national guidance sits with the central intelligence processing unit and local intelligence units. This would ensure the review of intelligence and information records on Intel2 though, at the time of inspection, it was unclear if there were sufficient staff to do this.

Evaluation

Police information within the five core business areas[16] was held on a series of separate applications linked through the Sleuth data warehouse. Each is available as a single Sleuth search. The force was seeking to develop further a ‘primary nominal’ solution which would significantly enhance the ability of the force to meet the national requirements for the review and deletion of records until force systems have the technical ability to do this (see national recommendations 6, 7 and 10).

Managing police information – common process

We found no specific information management policy to outline the extent to which the force meets standards set out in the Information Code of Practice and associated national guidance, or which would identify any gaps in force practice (see national recommendations 1 and 2).

There had been no formal review of information management implementation and development since 2010. It is vital that the force has a full understanding of any gaps between local practice and national guidance and a clear understanding of any risks arising from that (see national recommendations 1 and 2).

At the time of inspection, an audit team had been recruited to review the quality of police information held on local computer systems.

Sharing police information

The current National Special Branch Intelligence System is being replaced as part of a national programme known as Apollo. This has driven the review of special branch information[17] and the deletion of records where appropriate.

[16] Child abuse, domestic violence, custody, crime and intelligence are known as the five core business areas for uploading onto the PND.

[17] Special branch is a police unit that deals with terrorism and domestic extremism threats; usually works closely with a counter-terrorism unit

Information within the professional standards department is managed as sensitive information on CLUE. The CLUE system does not directly supply information to PND. Departmental processes are being introduced to assess how new intelligence should be transferred from CLUE to Intel2, allowing it to be more widely available and shared.

The force relies on staff to transfer intelligence from the Home Office Large Major Enquiry System to Intel2. There is an expectation placed on officers that they will check intelligence before visiting potential witnesses during a major crime investigation, and a similar expectation that any new intelligence will be transferred to Intel2 where appropriate. The processes are supported by a requirement for officers to endorse enquiry logs accordingly; however there is no audit or dip-sampling to ensure compliance.

Information from the intelligence, crime and custody business areas are sent to PND each day. There had been issues uploading child abuse and domestic violence records to the PND but, at the time of inspection, measures had been put in place to remedy this situation.

Retention, review and disposal

There was a force policy for the retention, review and disposal of documents. However, the document we saw at the time of inspection was long out of date and in urgent need of review. At the time of inspection, proposals for review were due to be considered by the information assurance board (see national recommendation 1).

At the time of inspection, there had been significant structural change in the retention, review and disposal of records team with insufficient resources in place to undertake information management review work (see national recommendations 1 and 7).

There was no systematic deletion of police information on force systems and the effectiveness of Intel2 was compromised by the large number of records still held within it. This situation increases risk of duplication and compromises investigation and analysis (see national recommendations 1, 7 and 10).

There was no formal process in place to make sure that police information was regularly reviewed (see national recommendation 6, 7 and 10).

3. Thematic report – National recommendations

To the Home Office and the National Lead for Information Management Business Area

Recommendation 2

By May 2016, the Home Office and National Police Chiefs' Council's Information Management Business Area lead, should agree and implement common standards to be used by forces to identify and transfer information, no longer sensitive to an enquiry contained within HOLMES, to systems which are accessible and searchable by the police service generally.

To chief constables

Recommendation 1

By 30 November 2015, chief constables should ensure that a review is undertaken of the way in which their forces' information management policies and practice comply with the APP on information management so that they give effect to the national approach and minimise any divergence from that APP.

Recommendation 3

By 30 November 2015, chief constables should carry out systematic audits in their forces to identify the extent to which locally-adopted practices and procedures conform to the APP on information management.

Recommendation 4

By November 2015, chief constables should ensure that adequate local information management processes are in place to consider all available information in an efficient and systematic way so that the continuing levels of risk that individuals pose to communities are properly assessed and, where necessary, information is recategorised and linked.

Recommendation 5

By November 2015, chief constables should ensure that their local information management processes adequately identify and prioritise the records of those who pose the greatest risk, in order that they are properly monitored, and appropriate, timely action is taken.

Recommendation 6

By 30 November 2015, chief constables should put in place arrangements to scrutinise audits of compliance with the APP on information management through the force information management governance structure. This should include measures to ensure that categorisation of records are regularly adjusted.

Recommendation 8

Immediately, chief constables should make sure that their force information records are reviewed at the end of the review period set for each information grouping, and records created when decisions are made to retain information beyond the applicable period of retention.

To the College of Policing

Recommendation 7

By 30 November 2015, the College of Policing should amend its APP on information management so as to specify the minimum information management requirements for initial reviews in relation to the retention and disposal of information.

Recommendation 9

By 30 November 2015, the College of Policing should ensure that specific guidance about the handling and availability of sensitive information is included in the APP on information management, and by 30 June 2016, chief constables should ensure that the guidance set out concerning sensitive information, is implemented.

Recommendation 10

By 30 November 2015, the College of Policing should revise the current APP on information management and include a common review process in respect of sensitive information for adoption by all forces. This should include timescales for the review of sensitive information in order to ensure it remains appropriately categorised.