Building the Picture: An inspection of police information management

Humberside Police

July 2015

ISBN: 978-1-78246-802-8

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 information14 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 System15). 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 12.

Inspection findings in Humberside

In the rest of this report, we describe our findings for the Humberside Police inspection which we undertook between the 14 and 16 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 Humberside Police

General

An assistant chief officer is responsible for information management, information communication technology (ICT) and information security across the force. We found information management structures in place that had clear leadership and decision making structures to support local requirements.

The head of information compliance has day to day responsibility for information management arrangements.

There was no information management board to consider areas such as data protection, freedom of information and records management. These were dealt with as they arose, and escalated when necessary to senior level. At the time of inspection, the force acknowledged this as a gap and had begun to establish an information management board.

A risk manager oversees the force risk register which is reviewed regularly at senior level. Each unit has its own risk register and feeds into the force risk register. At the time of our inspection, there were no specific information management risks recorded. An information management board would be beneficial in highlighting and managing information management risks.

Collection and recording

Intelligence records were entered directly by operational staff onto CIS4 – the primary intelligence system used by the force – with the option of grading records as high, medium or low risk. The force relies on the professionalism and experience of its staff to grade intelligence correctly.

All intelligence submissions were reviewed by staff within the force intelligence bureau (FIB) or divisional intelligence units. Intelligence staff then prioritise their reviews by the grade selected by the officer making the intelligence submission. All reviews were conducted within a 24-hour period but this process was not covered by a policy.

However, intelligence submissions do not trigger reviews of the recent related information or an assessment of it. There may therefore be a risk that intelligence records held about those who pose a high a risk were not identified as quickly as they could otherwise have been (see national recommendations 4 and 5).

Evaluation

Police information within the five core business areas[16] is held on a series of separate, unlinked systems. This frustrates the ease with which records can be readily identified, connected and the associations between them linked.

Managing police information – common process

The local Management of Police Information (MoPI) action plan was used to identify details of how the force meets the Management of Police Information Code of Practice and associated national guidance. Areas where the force diverged from the guidance were documented and explained. The document was reviewed over a three-year cycle with different sections being reviewed each year by the records manager.

An information management strategy (IMS) was in place which works to the principles of the Code of Practice and associated national guidance.

The IMS is supplemented by a set of local policy and practice documents about the retention, review and deletion of police information. These policies detailed local decisions to deviate from the national guidance as well as the direction in which the force is developing its information management work.

There are strong governance arrangements in place for the development of new ICT initiatives with regular meetings to review milestones and identify priorities.

Sharing police information

CIS4 is the primary intelligence system used by the force to manage and contain intelligence records. It is a computer system that holds information on crime, intelligence and domestic abuse but does not allow for the merging or transfer of records with other information communication computer systems used by the force for areas such as child protection and custody. The system can restrict access to records to certain users according to the sensitivity of the information contained. Information graded for sharing only within the police service was routinely entered on the CIS4 intelligence system, which made it searchable and available for upload to the PND. Records considered sensitive triggered a system alert to inform staff of their existence. There is a formal process of review to ensure that intelligence marked initially as sensitive was transferred quickly to CIS4 where appropriate.

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

As the Home Office Major Enquiry system (HOLMES) does not have a direct link or facility to transfer information onto CIS4, the force relies on operational staff to do this manually. There are no agreed processes to ensure this takes place.

The professional standards branch (PSB) has a comprehensive policy which covers all aspects of information and intelligence handled within the department. This is a department-specific policy. We found that assessment of information generated and held within the PSB was taking place and, where appropriate, information was transferred to make it more widely available through CIS4.

The current National Special Branch Intelligence System is being replaced as part of a national programme known as Apollo. Migration to the new system is governed by data rules about existing force information. The replacement programme has driven the review of special branch[17] information and the deletion of records where appropriate.

Information from the five core business areas was uploaded automatically to the PND each day.

Retention, review and disposal

There is a review team that assesses records to meet requirements and also actively reviews old paper crime records when capacity allows. We found the team worked closely with operational staff, highlighting where potential crime reduction or safeguarding action might be necessary.

The review, retention and disposal team collated success stories about its work where this had directly contributed to the reduction of risk or prevention of harm to vulnerable people. This was a good example of illustrating the importance of good information management.

Information management reviews take place routinely and issues about the duplication of records and the poor quality of information provided were addressed. However, triggered reviews did not consider information held in HOLMES, professional standards or the counter-terrorism area.

Police information on force systems was retained indefinitely due to the limitations of the CIS4 system. There was no consistent process for deleting information once it ceased to meet a policing purpose. This situation raises the risk of duplication and compromises investigation and analysis (see national recommendations 1 and 8).

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

There were monthly audits covering data quality, duplicate records and the failure to create records; summary reports of these were placed on the force intranet and more detailed reports were sent to relevant units for remedial action.

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.