Building the Picture: An inspection of police information management

The Metropolitan Police Service

July 2015

ISBN: 978-1-78246-799-1

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 12.

Inspection findings in the Metropolitan Police

In the rest of this report, we describe our findings for the Metropolitan Police inspection which we undertook between the 4 and 6 August 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 the Metropolitan Police Service

General

An assistant commissioner has oversight and responsibility for information management across the organisation. At the time of the HMIC visit, the appointed assistant commissioner had only assumed this responsibility six weeks previously.

The responsibility for information management now sits under the management of corporate headquarters.

An information management governance board was in place up until the end of 2012. The board was disbanded and had only recently been reintroduced. As a consequence, staff interviewed during the inspection reported a sense of renewed focus on information management issues. There was now confidence in the revised management of the area and that the importance of information management was recognised at a senior level.

Collection and recording

A recent review of the force's structure has introduced a centralised 'record, evaluate and disseminate' (RED) team.

The RED team had responsibility for:

- supporting live time enquiries with particular focus on threats to life and safeguarding of vulnerable people;
- the development of slower time intelligence;
- information quality assurance of around 700 records per month; and
- reviewing the records created on the force primary intelligence system (CrimInt), including checking data standards and the appropriateness of the use of the handling code[16].

At the time of the inspection there was no backlog of intelligence records on CrimInt awaiting review.

[16] Introduced under the National Intelligence Model (see: *Introduction to Intelligence-led Policing*, produced on behalf of the Association of Chief Police Officers by the National Centre for Policing Excellence, 2007 www.acpo.police.uk/documents/crime/2007/200708-cba-intelligence-led-policing.pdf). The system evaluates the source for the intelligence, the validity of the data and the handling sensitivity of a piece of information. Each category has five possible gradings and hence the system is universally known within the police service as 5x5x5.

The main activities and responsibilities of all intelligence staff were outlined in a standard operating procedure.

Evaluation

Police information within the five core business areas[17] was held on a series of separate, unlinked systems. However there was some search capability across these systems and an ability to compare associated information held on each system.

The force had put in place a 'total technology' programme; this was overseeing the development and introduction of a fully linked information communications technology (ICT) system and was intended to provide a single search across all core business areas. The system is not likely to be complete until 2017.

Managing police information – common process

The force produced a records management manual in 2010; this detailed the force's response to the review, retention and deletion (RRD) standards which must be applied. The manual focused on measuring risk and maximum retention periods for police information held on unlinked systems. Due to ICT constraints, the processes described in the manual had not been put in place. We refer to this later in this report.

Assessment of how the force's RRD standards meet requirements of the APP (formally MoPI) had not been reviewed since 2010. However, the records management manual was due to be reviewed under the new structure although the process and timeframe for completion of the review were not given. The force should complete this work as soon as it can to ensure current practice is in accordance with expected professional practice.

A draft information management strategy (2012–2018) outlines information management risks and how these will be addressed; this had not formally been accepted.

Sharing police information

As the Home Office Large Major Enquiry System (HOLMES) does not have a direct link to CrimInt, the force relies on staff to enter intelligence manually from major enquiries onto CrimInt.

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

Senior managers within the major crime specialist area were expected to have an overview of intelligence obtained during major crime enquires and to ensure it is transferred to CrimInt where appropriate. A pop-up appears on screen when investigation logs are opened as a reminder to do this. However, there was no audit or dip-sampling process to make sure this takes place.

At the time of our inspection, a project was in place to develop automatic transfer of records about people from HOLMES to CrimInt. This was due to be in place by October 2014 but is yet to happen. The automatic transfer of records will ensure a significant amount of intelligence previously held only on HOLMES will be available through Crimint searches. Information will be transferred unless a marker has been applied to a record preventing its transfer. The key role of individual officers in transferring relevant intelligence to CrimInt will not be changed.

There were several thousand records held within the special branch specialist area[18][19] which had not been indexed. This prevents them being linked to related records on other systems or searching by category of information. The information can be accessed using free text search but this is imprecise and unreliable. This is of concern to us as storing this information in isolation may prevent connections being made with information in other records and so pose a significant risk to the public (see national recommendation 4).

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. Force migration has been delayed by about two years to allow for data cleansing. There is a risk that records yet to be indexed may not be moved across to the new national system. The force must have a full understanding of this risk and take proportionate measures where appropriate (see national recommendation 7).

Multi-agency safeguarding hubs (MASH)[20] have responsibility for dealing with cases in their area when they are referred by police officers and staff as well as other partner agencies. The MASH acts as a central point of co-ordination so relevant agencies have the information necessary to provide safeguarding services. However, the child abuse investigation teams also received referrals direct from

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

[19] The department that deals with terrorism and domestic extremism threats in the Metropolitan Police is called SO15 Counter Terrorism Command. For the sake of consistency between force reports featuring in this inspection we have used the Special Branch reference.

[20] An entity in which public sector organisations with common or aligned responsibilities for the safety of vulnerable people work. The hubs comprise staff from organisations such as the police and local authority social services; they work alongside one another, sharing information and co-ordinating activities to help protect the most vulnerable children and adults from harm, neglect and abuse

partner agencies. The risk that referrals may not always be shared with the MASH had been identified and a notification (pan-London referral) form had been introduced in 2014 to ensure that referrals were submitted and notified to partner agencies in all relevant cases. (see national recommendation 6).

When information held by the department of professional standards (DPS) ceased to be restricted, it was not transferred; this poses a risk that information that should be shared via the Police National Database (PND) is not (see national recommendation 4).

However, processes are in place within DPS so that records or allegations of sexual or violent offences are identified, and markers placed on PND to flag up that a record exists that may be relevant to other investigations.

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

Retention, review and disposal

The records management manual records how the force meets the retention, review and disposal elements of the APP guidance. The manual outlines that the force will provide a fully automated method of records management. The manual was signed off in 2010 and a revised manual was produced in 2012. The length of time that the force plans to keep information on systems was set out in the manual but the timescales were not consistent with either the previous Management of Police Information or current APP standards. A review of the manual was planned during which the force approach will be matched to developing ICT. All police information on force systems was retained indefinitely. There was no process of review and no consistent process for deleting information once it is no longer useful. This situation increases risk of duplication and compromises investigation and analysis (see national recommendations 1 and 7).

A recent review of intelligence records which had been restricted allowed a large number of these records held up to 2011 to be shared more widely. The information was therefore now available on CrimInt and is available for upload to the PND. The process for the ongoing and regular assessment of such records was unclear; however since our inspection, a policy has been put in place in an attempt to rectify this. Considerations concerning information that no longer needs to be protected as 'sensitive' and the wider sharing of it now rests with identified intelligence support functions[21]. (see national recommendation 4).

[21] SCO36 - 24/7 Intelligence Support now have on-going responsibility to consider the need of protected information within Crimint. The policy was approved 28th November 2014.

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.