

Building the Picture: An inspection of police information management

Nottinghamshire Police

July 2015

© HMIC 2015

ISBN: 978-1-78246-809-7

www.justiceinspectorates.gov.uk/hmic

Contents

1. Introduction	3
Why information management is important	3
Background: Mistakes Were Made	4
Methodology	5
2. Findings for Nottinghamshire Police	8
General.....	8
Collection and recording.....	8
Evaluation.....	9
Managing police information – common process.....	9
Sharing police information	10
Retention, review and disposal.....	10
3. Thematic report – National recommendations	12
To the Home Office and the National Lead for Information Management Business Area.....	12
To chief constables.....	12
To the College of Policing.....	13

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 Wales¹.

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

Information³ 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 management⁵ 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 management⁹ and the former editions of the national guidance¹⁰ in dealing with the information and allegations. It also examined the extent to which those forces made effective use of the Police National Database¹¹ 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 survey¹² 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 Nottinghamshire

In the rest of this report, we describe our findings for the Nottinghamshire Police inspection which we undertook between the 23 and 25 June 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 Nottinghamshire Police

General

The deputy chief constable has oversight and responsibility for information management. Notable progress has been made around regional focus on information security. However, local focus, regional collaboration and networking about information management matters are not as well developed.

The force underwent significant restructure in 2011 when the data services department was disbanded. Information management became the responsibility of corporate development.

The deputy chief constable chairs a quarterly force information assurance board (FIAB). The terms of reference for the FIAB do not include information management as a specific area of responsibility.

There has been no concerted activity around information management development since the end of the national Management of Police Information (MoPI) introduction programme in 2010.

Collection and recording

PATRIARCH is the primary intelligence system used by the force to store and manage intelligence records. It is a separate, unlinked computer system that does not allow for the automatic transfer of records between other systems used by the force

Intelligence records are entered directly onto the PATRIARCH system by operational staff. There is an option to select the appropriate information management review group code when the record is created but many operational staff choose not to do so.

Force intelligence review officers (FIROs) and intelligence support clerks (ISCs) play a crucial role in assessing the quality of information on the PATRIARCH system. FIROs and ISCs will review the evaluation and handling codes as well as the management review category, and complete and amend them where necessary. However, there is no process in place to make sure intelligence is reviewed and the handling code kept up to date. At the time of our inspection, there was a backlog of approximately 500 records for intelligence review which meant processing delays of around 4 days.

Evaluation

Police information within the five core business areas¹⁶ is held on a series of separate, unlinked systems. However, a search engine called Genie is in place which provides some capacity to find information in these systems.

The GENIE search engine does not provide a complete method to search records of all information across the five core business areas. This means that separate searches need to be made – specifically for records of domestic abuse and child abuse.

The force was considering the adoption of an enhanced GENIE function from Leicestershire Police to improve functionality and allow a search across the command and control system and of some historic data.

Development of GENIE in line with the Leicestershire model was not due to begin until April 2016.

There were also plans to explore another records management system. Niche 5 is currently the preferred option. If introduced, Niche 5 will have full search capability and be integrated across the five East Midlands forces¹⁷.

The force will be unable to link information effectively until records held on all systems can be searched with greater ease. Similarly, it will be difficult to demonstrate how the force is meeting national requirements for the review and deletion of records until force systems have the technical capacity to do this (see national recommendations 6, 7 and 10).

Managing police information – common process

There was no force policy or statement which set out how the force delivers against the MoPI Code of Practice and associated guidance. How far the force diverges from the national guidance has not been recorded or risk assessed.

The information management strategy (IMS) expired in 2011 and is currently under review. There was a draft strategy which laid out aims and objectives for the force. The revised IMS did not specify how the force will match local review, retention and disposal processes to the national guidance. The force should complete this work as soon as possible so it meets the expected standards for professional practice (see national recommendation 1).

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).

¹⁷ The East Midlands region of police forces comprises Derbyshire Constabulary, Leicestershire Police, Lincolnshire Police; Northamptonshire Police and Nottinghamshire Police.

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 following on from that (see national recommendations 1 and 2).

Sharing police information

There was no force policy or statement laying out a process for the transfer of information from sensitive business areas into PATRIARCH, the force intelligence system. The same is true for records and intelligence reports restricted due to their sensitivity.

It has not been possible to transfer records of people coming to police notice from HOLMES to the force intelligence system since the introduction of PATRIARCH in March 2014.

Information about public protection is managed and held on the case administration tracking system; access to it is largely restricted to those working in public protection roles. There is no process to ensure that appropriate intelligence is migrated to PATRIARCH; nor is there any process to share appropriate information for wider assessment and consideration. The information management Authorised Professional Practice places particular emphasis on records of children and vulnerable adults to ensure that those who pose the greatest risk to them are appropriately monitored (see national recommendation 7).

Information from four out of the five core business areas is automatically uploaded to the Police National Database (PND) each day. Intelligence has not been provided to PND since PATRIARCH was introduced in March 2014 as it was not technically possible to do so. Work was underway to rectify this, but until a solution is in place it poses a risk.

Retention, review and disposal

All police information on force systems was retained indefinitely. There was no process of review and no consistent process for the deletion of information once it is no longer useful. This situation increases the risk of duplication and compromises investigation and analysis (see national recommendations 1 and 7).

A significant investment was made by the force between October 2012 and March 2013 to review around 14,000 records which were restricted as 'covert case incidents'. The review ensured that the records were correctly graded and reassessed to maximise the amount of intelligence available at force level. Undertaking this review ensured that appropriate intelligence was uploaded to PND.

The restricting of intelligence may only be applied to divisional-level intelligence records with approval of a detective inspector. Such intelligence should then be reviewed every three months to ensure that the restrictions which remain are necessary. However there was no automated flagging process to prompt reviews and we were unable to gain assurance that those necessary took place.

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.