Building the Picture: An inspection of police information management

Sussex Police

July 2015

ISBN: 978-1-78246-798-4

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 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 business processes police forces in England and Wales use to collect, record, process, evaluate and share information.[2]

Why information management is important

Every year police forces in England and Wales receive millions of pieces of information. If this information is not handled correctly, opportunities for the police to build a picture of a criminal's pattern of offending may be missed. As a result, crimes which may have been prevented are committed, and criminals who may have been apprehended before causing any harm are allowed to carry on their unlawful enterprise, creating victims and anguish for those who suffer at their hands.

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.[3]

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 commit to a further review. This inspection fulfils this commitment.

---

[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] *Mistakes Were Made*, HMIC, March 2013.
See: www.justiceinspectorates.gov.uk/hmic/media/review-into-allegations-and-intelligence-material-concerning-jimmy-savile.pdf This review also examined whether West Yorkshire Police, as the force area in which Savile lived for most of his life, received details of this information and these allegations.

Methodology

HMIC analysed the results of a self-assessment survey on the management of information which all forces completed in 2013,[4] and conducted fieldwork in 13 police forces.

The selection of forces for the fieldwork phase was based on three criteria:

- involvement in cases reported by victims of Savile (Surrey Police, Sussex Police, the Metropolitan Police Service, and West Yorkshire Police);
- involvement in the Bichard Inquiry[5] (Cambridgeshire Constabulary and Humberside Police); or
- because there was a high, low or average (compared to other forces in England and Wales) level of risk regarding information management identified in the national self-assessment survey (Dyfed Powys Police, Hampshire Constabulary, Lancashire Constabulary, Lincolnshire Police, Merseyside Police, North Yorkshire Police and Nottinghamshire Police).

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;[6] 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.

We were therefore disappointed to find that decisions to depart from the guidance were only recorded in three of the 13 forces we inspected.

[4] This survey was commissioned by the ACPO national policing Information Management Business Area lead because of the failures in this area identified in *Mistakes Were Made.* It was conducted by the College of Policing.

[5] The Bichard Inquiry report, House of Commons, HC653, June 2004. http://dera.ioe.ac.uk/6394/1/report.pdf This inquiry was set up following the failure of local police forces to ensure that relevant information was exchanged regarding Ian Huntley who was convicted of the murders of Jessica Chapman and Holly Wells in December 2003.

[6] *Op cit*

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[7] 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 (HOLMES[8]). 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.

Inspection findings in Sussex

In the rest of this report, we describe our findings for the Sussex Police inspection which we undertook between the 19 and 21 May 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/publications/building-picture-an-inspection-of-police-information-management/

[7] '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.

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

2. Findings for Sussex Police

General

The deputy chief constable is the chief officer lead for information management across the force.

A head of information had been appointed to oversee information management; however this post did not have any staff specifically to support the role or to discharge information management responsibilities directly.

At the time of inspection, a new post of information manager had been identified and a candidate selected. A review and revision of force information management structures was therefore pending.

Again, at the time of inspection, a new business design group had been set up to provide links between areas such as information management, technical development and business change. The group had oversight of all change programmes. We found that the group was helping the force move away from a position where departments were working in isolation to one where work was better co-ordinated and prioritised.

The deputy chief constable chairs an information management strategy board (IMSB) that provides governance and high-level direction. At the time of our inspection, we found evidence of low attendance at quarterly meetings; indeed some recent meetings had been cancelled because of low numbers attending.

At the time of inspection, the IMSB's terms of reference were due to be reviewed; this included putting risks about information management on the force risk register.

Collection and recording

When an intelligence record is created by an officer, they add a handling code[9].The originating officer is also responsible for making an initial assessment of its priority and recording this on Niche, the force's records management system.

All intelligence records are reviewed by intelligence source co-ordinators (ISCs) within the intelligence units. The reviews include checking data standards, the handling code, and linking and indexing the record to those already in the Niche system. The handling code may be amended if it has not been correctly graded.

[9] The Handling Code was 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). It evaluates the source, 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.

Where the record is protected by an intelligence handling code it should be reviewed after a three month period. If it still needs to be protected at this point, this should be approved by a detective inspector. However no process was in place to make sure this happened.

Evaluation

The force introduced Niche in May 2013. This has brought all primary business areas on to a single information system with the necessary linking of information. This system is shared with Surrey.

Sussex reviewed data from a series of systems no longer in use and imported the records into Niche from the previous primary system (CIMS). Data from the CIMS predecessor (CIS) has not been transferred to Niche but is available separately on another force database. This therefore entailed a separate search to access CIS information (see national recommendations 4 and 5).

Managing police information – common process

At the time of inspection, the current information management strategy (IMS) was 16 months out of date and in need of review but there was no timeline in place for this.

We found no specific policy to cover the management of information across the force, or any policy statement describing how the force meets the Management of Police Information Code of Practice 2005 or the APP on information management and former editions of the national guidance, or the extent to which it fails to do so (see national recommendations 1, 3 and 6).

In addition, we found no clear process for the declassification of intelligence records, inconsistencies in the transfer of information from sensitive business areas to Niche and a lack of understanding of how effectively the major crime team staff are entering relevant intelligence on Niche.

Sharing police information

The force recognised that the transfer of intelligence from HOLMES to Niche was not specified in the crime and intelligence policy and this needed to be rectified.

The force was confident that child abuse and vulnerable adult-related intelligence was transferred from HOLMES to Niche and there was a memorandum of understanding to this effect; however there was no confirmation that transfer routinely takes place.

We found that Sussex was sharing information on the Police National Database from four primary business areas (crime, intelligence, child abuse and sexual violence). Custody records were not included. Certain fields were not always completed which could mean, for example, that a suspect in a child abuse case was not immediately identified (see national recommendations 4 and 5).

Sussex was developing an enhanced search tool (IBASE) which would allow cross-system searching of local databases. At the time of inspection, this had not been put in place because of IT constraints.

Retention, review and disposal

There was an early decision in the force information management implementation process to automate the retention, review and disposal of records.

At the time of inspection, we did find evidence of a backlog in the review of intelligence records.

Records on Niche are brought to the attention of the data compliance team when identified for deletion. We found no formal process in place to ensure retained information is reviewed regularly after the initial review by the ISCs (see national recommendations 4, 5 and 8).

The force needs to review its policy on the retention, review and disposal of records to eliminate risks to vulnerable groups and introduce appropriate auditing (see national recommendations 4, 5 and 6).

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 ongoing 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.