INVESTIGATION · FOUNDATIONS

Documenting an Investigation: Notes, Records and Reports

An investigation that is not documented cannot be checked, defended or continued. This article sets out what investigators should record, how, and why, from contemporaneous notes and decision logs to the final report.

ModQu research article · 1,224 words · 12 references (APA 7th edition)

Investigators sometimes treat paperwork as the dull part of the job, something to be completed after the real work is done. In practice, documentation is part of the real work. It is how an investigator remembers what was found, how colleagues and supervisors know what has been done, and how courts, tribunals, regulators and readers can judge whether the conclusions are sound. An investigation with poor records may reach the right answer and still fail, because nobody can show how the answer was reached.

Why documentation matters

Good records serve four purposes.

1. **Memory.** Investigations can run for months or years. Without notes, details fade and are reconstructed, often inaccurately.
2. **Continuity.** Investigators change jobs, fall ill or are reassigned. Records allow someone else to pick up the work.
3. **Accountability.** Decisions about who to interview, which leads to follow and when to stop may later be challenged. A record made at the time shows what was known and why each decision was taken.
4. **Disclosure and fairness.** In criminal cases, the prosecution must disclose relevant material to the defence. In Canada, *R. v. Stinchcombe* (1991) established a broad duty to disclose; in the United States, *Brady v. Maryland* (1963) requires disclosure of evidence favourable to the accused; and in England and Wales the Criminal Procedure and Investigations Act 1996 requires investigators to record and retain material that may be relevant. Material that was never recorded cannot be disclosed, and its absence can undermine a prosecution.

The same logic applies outside criminal justice. A workplace investigation that leads to a dismissal will be scrutinised by an employment tribunal, which will want to see what evidence was gathered and how the employee was given a chance to respond (Acas, 2019).

The main types of record



Figure 1. The main layers of investigative documentation. Each higher layer should be traceable to the records beneath it. Diagram by ModQu.

Contemporaneous notes

Notes made at the time, or as soon as possible afterwards, are the foundation of the record. They should be dated and timed, written in a bound notebook or a secure electronic system that shows when entries were made, and never altered after the fact. Corrections should be made by striking through and initialling, so that the original remains legible. Police in England and Wales have long been required to keep such records, and courts give more weight to notes made at the time than to later recollection.

Interview records

Wherever possible, interviews should be audio or video recorded. Research shows why. Lamb et al. (2000) compared investigators' notes of interviews with children against recordings of the same interviews and found that the notes missed more than half of the details the children provided and most of the investigators' own questions, which made it impossible to judge whether answers had been prompted by leading questions. Where recording is not possible, notes should capture questions as well as answers, as close to verbatim as possible, and should be shared with the interviewee for correction where appropriate (Milne & Bull, 1999).

Evidence and exhibit register

Every item of evidence needs a unique reference, a description, the date and place it was obtained, the person who obtained it and its chain of custody. For digital evidence, the record should include how it was acquired and the hash values used to show it has not changed (International Organization for Standardization [ISO], 2012; Kent et al., 2006).

Decision log

A decision log, sometimes called a policy file, records each significant decision, the information available at the time, the options considered and the reasons for the choice. Police doctrine in England and Wales treats it as a core record for senior investigators (Association of Chief Police Officers [ACPO], 2005). It is especially important for decisions not to do something, such as not pursuing a lead or not interviewing a witness, because those are the decisions most likely to be questioned later.

The report

The final report draws the investigation together. A good report states the mandate and scope, summarises the method, sets out the evidence relied on, explains how conflicting evidence was weighed, states conclusions and the standard of proof they meet, and identifies limitations and unanswered questions (Stelfox, 2009; Tong et al., 2009). Every factual statement should be traceable to a record. Investigative journalism manuals make the same point: reporters are advised to keep a master file that links every claim in a story to its source document or interview (Hunter et al., 2011).

Electronic records and case management systems

Most investigations now keep their records electronically. Case management systems can link notes, documents, exhibits, interviews and decisions, and can show who created or changed each entry and when. These audit trails are valuable, but only if the system is configured to keep them and users cannot overwrite earlier versions. Shared folders and email are a poor substitute: files are renamed, copied and edited without trace, and it becomes impossible to show which version of a document was relied on. Organisations that conduct investigations regularly should decide in advance where records will be kept, who can access them, how long they will be retained and how they will be exported if needed for legal proceedings.

Electronic records also raise questions of data protection. Investigation files often contain sensitive personal information about subjects, witnesses and third parties. Access should be limited to those who need it, and retention should follow the organisation's legal obligations rather than convenience.

Common failures

Reviews of investigations that have gone wrong often find the same documentation problems:

- Notes written up days after an interview, from memory, with no record of the questions asked.
- A final report that states conclusions without showing which evidence supports each one.

- No record of leads that were considered and dropped, so the investigation cannot show it looked beyond its main theory.
- Several versions of key documents with no indication of which is final.
- Exhibits that cannot be matched to the record of where and when they were obtained.

Each of these failures is easy to prevent at the time and difficult or impossible to repair afterwards. A short checklist at the end of each working day, confirming that notes are complete, exhibits are logged and decisions are recorded, prevents most of them.

Principles of good documentation

Across these records, a few principles apply:

- **Record at the time.** The longer the delay, the less reliable the record.
- **Record facts and inferences separately.** "The door was unlocked" is an observation. "The suspect left the door unlocked" is an inference, and should be identified as such.
- **Record what did not happen.** Searches that found nothing, witnesses who could not be traced and leads that were closed are part of the record.
- **Keep records secure and complete.** Access should be controlled, and nothing relevant should be destroyed until retention rules allow it.
- **Write for a reader who was not there.** A supervisor, judge or successor should be able to understand the record without asking the author.

Documentation beyond investigation

The same discipline benefits any work that produces evidence for decisions. Research projects that log their decisions, keep raw data unaltered and record every transformation are easier to check, to repeat and to defend. The principle is simple: if it is not written down, it cannot be shown to have happened, and if it cannot be shown, it cannot be relied upon.

References

Acas. (2019). *Conducting workplace investigations*. Advisory, Conciliation and Arbitration Service.

Association of Chief Police Officers. (2005). *Practice advice on core investigative doctrine*. National Centre for Policing Excellence.

Brady v. Maryland, 373 U.S. 83 (1963).

Criminal Procedure and Investigations Act 1996, c. 25 (UK).

Hunter, M. L., Hanson, N., Sabbagh, R., Sengers, L., Sullivan, D., & Svith, F. T. (2011). *Story-based inquiry: A manual for investigative journalists*. UNESCO.

International Organization for Standardization. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence* (ISO/IEC Standard No. 27037:2012).

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response* (NIST Special Publication 800-86). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-86

Lamb, M. E., Orbach, Y., Sternberg, K. J., Hershkowitz, I., & Horowitz, D. (2000). Accuracy of investigators' verbatim notes of their forensic interviews with alleged child abuse victims. *Law and Human Behavior, 24*(6), 699–708. https://doi.org/10.1023/A:1005556404636

Milne, R., & Bull, R. (1999). *Investigative interviewing: Psychology and practice*. Wiley.

R. v. Stinchcombe, [1991] 3 S.C.R. 326 (Supreme Court of Canada).

Stelfox, P. (2009). *Criminal investigation: An introduction to principles and practice*. Willan.

Tong, S., Bryant, R. P., & Horvath, M. A. H. (2009). *Understanding criminal investigation*. Wiley-Blackwell. https://doi.org/10.1002/9780470749616