SCHILLING VIGILANCE · WHITE PAPER SERIES · NO. 2 · REV. 0

The AI-Enabled PSMF

From Periodic Document Maintenance to a Controlled Digital Representation of the Pharmacovigilance System

The pharmacovigilance system master file (PSMF) must describe the pharmacovigilance system as it actually operates. This paper argues that the PSMF should remain a controlled regulatory document while its maintenance moves from periodic manual consolidation to governed, effective-dated and evidence-linked system data. It sets out an operating model, the boundaries for AI support, and a bounded pilot to start with.

Scope: EU human-medicines pharmacovigilance. Regulatory position as of 23 September 2026.

Reinhold Schilling

Correspondence and further publications: www.schilling-vigilance.com

Rev. 0 · September 2026

How to cite

Schilling R. The AI-Enabled PSMF: From Periodic Document Maintenance to a Controlled Digital Representation of the Pharmacovigilance System. Schilling Vigilance White Paper Series, No. 2, Rev. 0. September 2026.

Contents

Author perspective

Most problems with the pharmacovigilance system master file (PSMF) that I have met in audits and in inspection preparation did not start in the document. They started earlier: a provider contract amended without anyone telling pharmacovigilance, a local website launched with an untested adverse event form, a deputy who had left the company months before. By the time the annex was wrong, the operating reality had already moved on.

This paper argues that the answer lies in better control of the information from which the PSMF is written, not in more sophisticated documents. Artificial intelligence (AI) can help with that control, but only inside clear boundaries.

> **How to read this paper.** Regulatory statements are tied to their source and status. Binding EU law, final Good Pharmacovigilance Practices (GVP) guidance, procedural guidance, reflection papers, voluntary principles and consultation drafts are identified as such. Principles borrowed from Good Manufacturing Practice (GMP) are marked as transferred by analogy. The eight frameworks proposed by the author are labelled "Author-proposed framework. Not a regulatory standard." Where the paper says what an organisation should do, or must not allow AI to do, it states the author's position unless a source is cited. Regulatory references reflect the position as of 23 September 2026.

1. Executive Summary

Why the PSMF matters. The pharmacovigilance system master file (PSMF) is the detailed description of the pharmacovigilance (PV) system that a marketing authorisation holder (MAH) uses for one or more authorised medicinal products [1]. Its content must be accurate and reflect the system in place [3]. It supports the supervisory role of the Qualified Person Responsible for Pharmacovigilance (QPPV), the planning of audits, and the verification of compliance by competent authorities, including inspections [3][8]. An inaccurate PSMF is a compliance deficiency. It can also be a sign that the MAH does not fully know how its own PV system works.

Why document-centred maintenance creates avoidable risk. Many MAHs still maintain the PSMF through periodic email requests, local spreadsheets and manual transcription into word-processing templates. None of these tools is non-compliant in itself. The risk lies in the operating model built around them: information arrives late, owners are unclear, effective dates go unrecorded and annexes go stale. When an inspector asks what was true on a given date, someone has to reconstruct the answer. In the most detailed published industry survey, obtaining data in a timely and efficient way was the challenge companies named most often [17].

The PSMF is not the PV system. The PV system consists of the organisation, people, processes, contracts, computerised systems and controls that actually perform PV obligations. The PSMF describes that system. It can be accurate or inaccurate, current or stale, but it is never the system itself.

What a controlled digital representation means. This paper proposes that the PSMF remain a controlled regulatory document, while its content comes from approved, effective-dated and evidence-linked structured records instead of periodic consolidation from scratch. Those records describe providers, roles, safety-data sources, systems, products, audits, deviations and the relationships between them. PSMF sections and annexes are generated from them and released under document control.

What role AI may play. Artificial intelligence (AI) can support change detection, extraction from controlled documents, discrepancy identification, relationship and impact analysis, prioritisation, drafting and inspection preparation.

What role AI must not play. AI must not own operational facts, act as the definitive interpreter of regulatory requirements, approve master data or PSMF content, close deviations or corrective and preventive actions (CAPAs), or stand in for QPPV oversight.

The recommended starting point. Start with governance and data ownership, then run a bounded master-data pilot. A good candidate combines the service-provider inventory with local safety-data sources, applies deterministic consistency rules first and adds restricted AI extraction only under mandatory human verification.

Recommendations for MAHs

1. Treat the PSMF as the controlled output of a governed information process. It should not be the place where information is first collected.
2. Designate an authoritative source and a named owner for every material category of PSMF information.
3. Record effective-from and effective-to dates, together with transaction and approval dates, for every material record.
4. Replace free-text country questionnaires with a structured, conditional and evidence-linked Country PV Profile.
5. Combine event-driven change reporting with risk-based periodic certification.
6. Generate PSMF content only from approved records, and release it only through controlled review and approval.

7. Introduce deterministic rules before AI, and restrict AI to assistive functions with documented assurance and human verification.
8. Give the QPPV a risk-focused view of open exceptions, and make sure no one confuses dashboard visibility with QPPV approval.

Author-proposed frameworks in this paper

Framework	Role in the operating model	Section
Controlled digital representation of the PV system	Overall target state	4
PSMF Consistency Triangle	Central control objective	5
PSMF Truth Chain	Central process model	6
Source-to-Statement Rule	Traceability principle	7
Country PV Profile operating model	Interface for local facts	10
Event-Driven Change Framework	Change workflow combined with periodic certification	11
Multidimensional PSMF Status Model	Monitoring approach	17
AI-Enabled PSMF Maturity Model	Implementation and development path	25

None of these frameworks has been adopted by the European Medicines Agency (EMA), the European Commission, the Heads of Medicines Agencies (HMA), the US Food and Drug Administration (FDA) or any other authority. They are the author's proposals for discussion and practical use.

2. The PSMF Must Reflect Operating Reality

2.1 Accountability and the PV system

Directive 2001/83/EC requires the MAH to operate a pharmacovigilance system for the fulfilment of its PV tasks. The Directive defines that system as the one used by the MAH and by Member States to fulfil the tasks and responsibilities listed in Title IX of the Directive, designed to monitor the safety of authorised medicinal products and to detect any change to their risk-benefit balance. As part of the system, the MAH must have a QPPV permanently and continuously at its disposal, and must maintain a PSMF and make it available on request [1].

Responsibility stays with the MAH when activities are delegated to affiliates, licence partners or service providers: the MAH retains full responsibility for the completeness and accuracy of the PSMF even where activities are subcontracted [3]. Commission Implementing Regulation (EU) 2025/1466, most of whose provisions apply from 12 February 2026, tightened the rules on delegation [4]:

- Subcontracts must describe the roles and responsibilities of the third party, its obligation to exchange safety data and the method for doing so where relevant, the arrangements for audits and inspections, and the third party's agreement to be audited by or on behalf of the MAH and inspected by competent authorities.
- A third party may not further subcontract any PV task assigned by the MAH without the MAH's written consent.
- Third parties performing PV tasks must be audited by or on behalf of the MAH, taking into account the risk of the subcontracted activity.

GVP Module IV describes how risk-based audit programmes, audit reporting and the follow-up of findings should work in practice [10].

2.2 The QPPV

The QPPV must reside and carry out his or her tasks in the Union [1]. The PSMF must describe the QPPV's responsibilities in a way that demonstrates sufficient authority over the PV system to promote, maintain and improve compliance. It must also include a summary curriculum vitae, contact details and back-up arrangements [3]. The MAH must ensure that the QPPV has permanent access to the PSMF [3], and GVP expects relevant changes to the PSMF to be notified to the QPPV [8]. GVP Module I sets out the wider expectations for the PV quality system within which the QPPV exercises oversight [7].

This matters for everything that follows. A maintenance model that leaves the QPPV unaware of material change fails, however advanced its technology.

2.3 The PSMF, its location and the PV-system summary

The Implementing Regulation sets out the minimum content of the PSMF [3][4]:

- information on the QPPV, including back-up arrangements and, where nominated, national PV contact persons;
- the organisational structure of the MAH, including the list of sites where specified PV activities are undertaken, such as individual case safety report (ICSR) collection and evaluation, safety database entry, periodic safety update report (PSUR) production, signal detection, the preparation, implementation and maintenance of the risk management plan (RMP), study management and safety variations;
- the location, functionality and operational responsibility of the computerised systems and databases used for safety information, with an assessment of their fitness for purpose;

- PV processes and data handling;
- the quality system, including human resources, record management, performance monitoring and subcontracted activities.

The annex must list the products covered, PV policies and procedures, subcontracts, tasks delegated by the QPPV, scheduled and completed audits, performance indicators where applicable, other PSMFs held by the same MAH where applicable, and a logbook [3]. The PSMF and its annex are subject to version control and must show the date of the last update. Major or critical deviations from PV procedures, their impact and their management must be documented in the PSMF until resolved. Before the 2025 amendment, this applied to any deviation [3][4].

The PSMF must be located at the site in the Union where the main PV activities are performed or where the QPPV operates. It must be permanently and immediately available for inspection at that site, and if it is kept electronically, the data must be directly available there. Electronic storage is permitted, provided the storage media remain readable over time and a clearly arranged printed copy can be made available for audits and inspections [3]. EMA's questions and answers on the PV system give practical guidance on these points [12].

The marketing authorisation application does not contain the PSMF. It contains a summary of the applicant's PV system: proof that a QPPV is at the applicant's disposal, the Member States in which the QPPV resides and carries out tasks, the QPPV's contact details, a signed statement that the applicant has the means to fulfil its PV tasks, and a reference to the location of the PSMF [1]. Changes to the PSMF location or to the QPPV's name and contact details must be notified to EMA immediately [3].

2.4 Local arrangements, outsourced activities and availability

Local PV arrangements belong to the MAH's PV system: local contact persons, national reporting obligations, local literature screening, patient support programmes, medical information and local vendors. Outsourced activities belong to it as well. GVP Module II expects the PSMF to describe the sources of safety data, the contractual arrangements and the relevant systems, and to hold frequently changing information in the annexes [8].

Availability is a hard legal requirement. A national competent authority, or EMA for centrally authorised products, may ask for a copy of the PSMF at any time, and the MAH must submit it within seven days of receiving the request [1][2]. The authority may limit its request to specific parts or modules, and competent authorities may ask for copies of the logbook at regular intervals [3]. An operating model that needs weeks of reconstruction to produce a current PSMF does not meet this standard.

2.5 Inspection use

Inspectors use the PSMF to plan and conduct inspections. GVP Module III Revision 2, in effect since 10 September 2026, incorporates the amended subcontracting rules, including the audit and inspection of third parties [9]. The 2025 amendment also makes clear that third parties performing PV tasks for an MAH may be inspected by competent authorities whether or not the subcontract mentions it [4]. Inspection scope can extend to the accuracy, completeness and maintenance of the PSMF, the QPPV's access to quality-system information, the fitness for purpose of systems, contractual arrangements, and the activities of contractors and their subcontractors [9].

GVP modules are revised from time to time. Module II Revision 2 dates from 2017, before generative AI was in practical use and before the 2025 amendments. EMA has announced that the modules will be updated to reflect those amendments, so readers should check EMA's GVP pages for current versions [11].

2.6 Three things that must not be confused

This paper keeps three things apart throughout:

- **The operating PV system:** what people, providers and systems actually do.
- **Its approved structured representation:** the verified, effective-dated records that describe the system.
- **The released PSMF document:** the controlled, versioned text and annexes approved for regulatory use.

A mature MAH keeps all three aligned and can demonstrate the alignment.

3. The Limits of Document-Centred Maintenance

3.1 The typical pattern

In a document-centred model, the PSMF owner sends a periodic request to affiliates and functions. Replies arrive by email, often as marked-up extracts of the previous version or as local spreadsheets. The owner consolidates them, updates the body and annexes by hand, obtains review and releases a new version. Between cycles, a change reaches the PSMF only if someone remembers to report it.

3.2 Where risk arises

Practice	Characteristic risk
Periodic email collection	Changes arrive late, incompletely or not at all. There is no reliable record of who confirmed what, and when.
Standalone spreadsheets	The same provider appears under different names, formulas break, and local copies drift away from the central version.
Local lists	Several versions of the truth coexist, and nobody can say which one governs.
Repetitive copying into Word	Transcription errors creep in and the text drifts away from its source.
Inconsistent ownership	Nobody is accountable for a fact's accuracy, only for forwarding it.
Missing effective dates	Nobody can say when an arrangement started or ended.
Stale annexes	Annexes meant for frequently changing information are updated only at the next cycle.
Disconnected provider inventories	Procurement, PV and Quality each hold a different list of vendors.
Incomplete safety-data sources	Programmes, websites and social media channels go unrecorded.
Obsolete system and SOP references	Retired standard operating procedures (SOPs) and replaced systems are still cited.
Inspection-time reconstruction	Evidence is assembled under time pressure, with a higher risk of error.
Dependence on individual knowledge	Continuity is lost when key people leave.

3.3 What the evidence shows

The most detailed published evidence comes from a benchmarking survey run in September and October 2019 by the PSMF Networking Group of the European Federation of Pharmaceutical Industries and Associations (EFPIA) and

published in 2022 [17]. Thirty companies responded and 29 described their PSMF practices; 24 were pharmaceutical companies and the rest contract organisations or consultancies.

Asked for their three biggest challenges in producing the EU PSMF, respondents most often named obtaining data in a timely and efficient way (16 of 29). Next came interpreting the scope of PSMF content (12), source systems that were not designed to produce PSMF data (12), accountability for the information provided (11), and data quality and accuracy (10). Companies with PSMFs outside the EU added the difficulty of understanding differing country requirements and of maintaining several PSMF documents in parallel [17].

The survey was qualitative, relied on open-ended questions and predates the latest regulatory changes. In the author's experience its findings still hold, and they locate the core problem in information management.

3.4 The real question

Word, Excel and email are not inherently non-compliant, and no regulation says they are. The regulatory question is different: can the MAH's operating model reliably keep PSMF information accurate, current, complete, controlled, traceable and retrievable? For a small MAH with one PV system and a stable provider base, a disciplined document model may well answer yes. For a complex MAH, the burden of proof grows with every affiliate, provider and product.

4. The Controlled Digital Representation

Author-proposed framework. Not a regulatory standard.

4.1 Definition

> **Controlled digital representation of the pharmacovigilance system:** a governed set of structured, effective-dated, evidence-linked and approved information objects describing the MAH's PV system, maintained through controlled workflow, from which PSMF content is generated and released under document control.

The representation has ten elements:

- **Controlled information objects:** providers, roles, contracts, safety-data sources, systems, products and quality events, each with a unique identifier and a lifecycle status.
- **Authoritative sources:** a designated system or record that governs each fact.
- **Named ownership:** a data owner accountable for each record, and a verifier for local facts.
- **Jurisdiction and scope:** the countries, legal entities, products and PSMF that each record applies to.
- **Effective dates:** when the arrangement was, is or will be operationally valid.
- **Evidence links:** a reference to the controlled source that supports the record.
- **Review and approval status:** who verified and approved the record, when, and on what basis.
- **Relationships:** for example, that a provider performs an activity under a contract for a territory.
- **Historical versions:** earlier states are preserved, never overwritten.
- **Controlled generation:** PSMF sections and annexes are assembled only from approved records and then released through document control.

4.2 Why not "digital twin"

"Digital twin" comes from engineering, where it implies real-time synchronisation, simulation of behaviour and often autonomous feedback. Applied to the PSMF, the term invites three misunderstandings: that the representation is complete and always current, that it can predict how the system behaves, and that it can act on its own. None of these is the purpose of a PSMF. "Controlled digital representation" says what matters to a regulator: the information is governed, approved and bounded.

4.3 What this model is not

EU law requires the PSMF to be accurate, current, version-controlled and available. It permits electronic form but prescribes no architecture [3]. Structured data, graph databases, retrieval-augmented generation (RAG), large language models (LLMs) and real-time generation are not mandatory. An MAH that uses a different model is compliant if it meets the regulatory requirements.

4.4 How the frameworks fit together

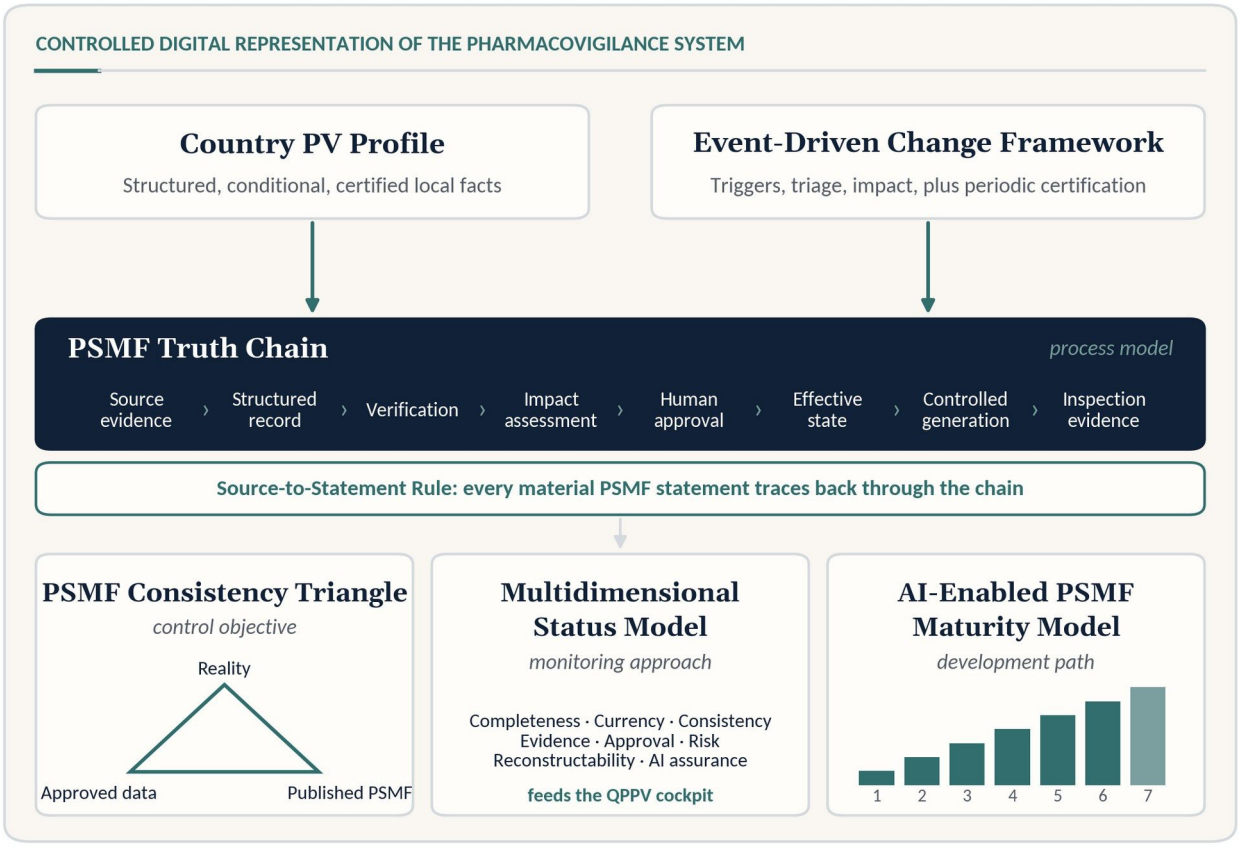

Figure 1. How the author-proposed frameworks form one operating model.

Local facts enter through the Country PV Profile, and changes enter through the event-driven workflow. The Truth Chain carries each fact from evidence to inspection-ready output, and the Source-to-Statement Rule keeps every material statement traceable along the way. The Consistency Triangle defines what the chain must achieve. The status model shows how well it is working, and the maturity model describes how an MAH can build the capability in steps.

5. The PSMF Consistency Triangle

Author-proposed framework. Not a regulatory standard.

The central control objective of an AI-enabled PSMF is consistency among three points.

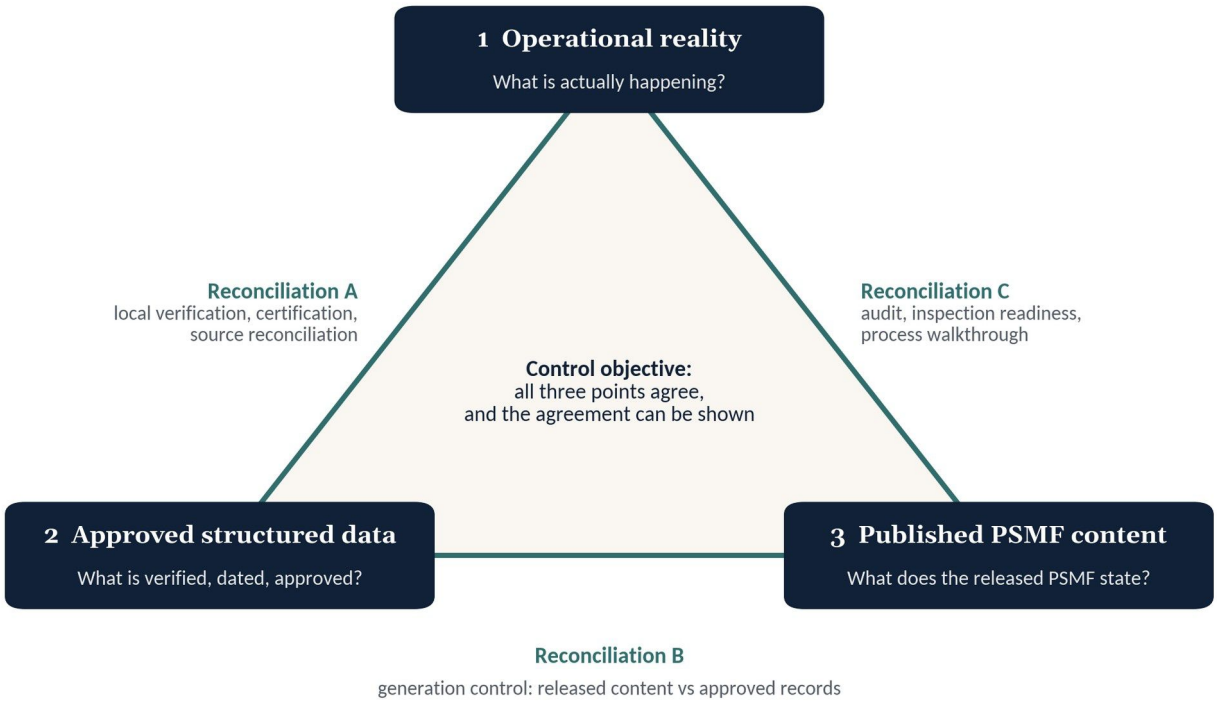

Figure 2. The PSMF Consistency Triangle.

- **Operational reality:** what is actually happening in the PV system. This is the provider actually receiving calls, the safety database actually in use, the person actually acting as local contact.
- **Approved structured system data:** what has been verified, effective-dated, approved and recorded.
- **Published PSMF content:** what the current released PSMF and its annexes state.

5.1 Three principal failure patterns

Reality changed, but structured data did not. A local affiliate engages a new call-centre provider and nobody raises a change record. The data are internally consistent and the PSMF faithfully reproduces them, but both are wrong. This is the most dangerous pattern, because every downstream control will pass. Only contact with reality detects it: certification, audit, reconciliation against procurement or finance records, and analysis of where cases actually come from.

Structured data changed, but the PSMF did not. The provider record was approved, but the annex was never regenerated or released. This failure is easy to detect by comparing the approved record set with the released version, and it usually points to weak workflow or release discipline.

The PSMF changed without adequate evidence of operational reality. Someone edited the annex directly on the strength of an email, or an AI-drafted statement was approved without anyone checking the source. The document now claims something the MAH cannot substantiate. This is the characteristic risk of careless automation.

5.2 Reconciliation as control

Each side of the triangle needs its own reconciliation:

- **Reconciliation A (reality and data)** relies on local verification, periodic certification, reconciliation against authoritative source systems and audit sampling.
- **Reconciliation B (data and PSMF)** relies on generation controls, automated comparison of released content with the approved record set, and independent sample checks.
- **Reconciliation C (PSMF and reality)** relies on audits, inspection-readiness walkthroughs and process observation.

No single reconciliation is sufficient. A platform that performs only Reconciliation B, which is the easiest one to automate, gives false comfort.

6. The PSMF Truth Chain

> **Author-proposed framework. Not a regulatory standard.**

The Truth Chain is the process through which an operational fact becomes inspection evidence:

> **Source Evidence → Structured Record → Verification → Impact Assessment → Human Approval → Effective System State → Controlled PSMF Generation → Inspection Evidence**

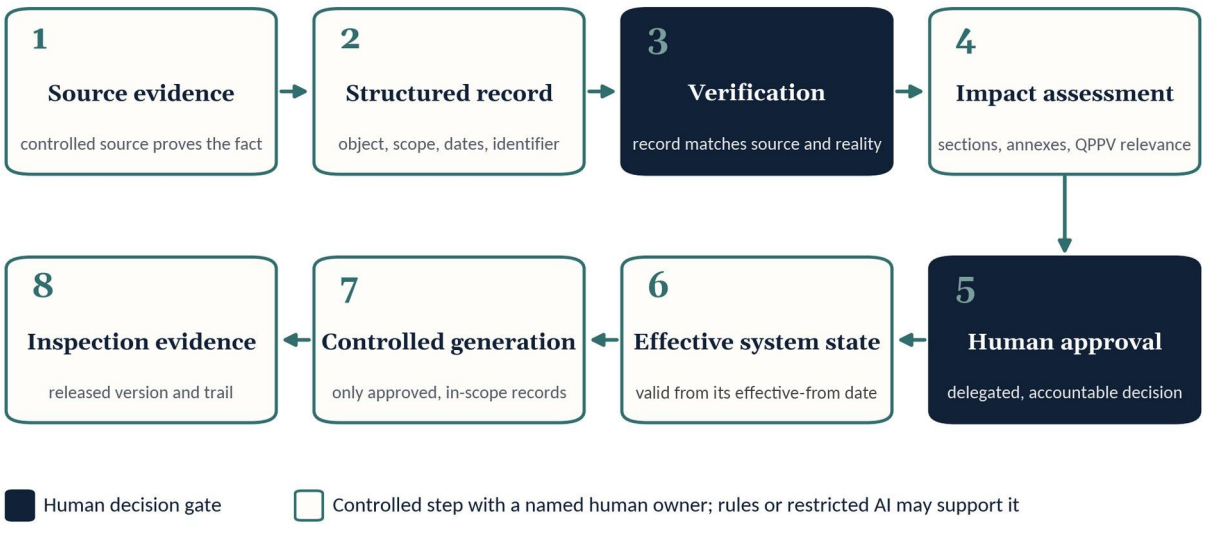

Figure 3. The PSMF Truth Chain, with its two mandatory human decision gates.

The cards below describe each link: its objective, the responsible role, the evidence it produces, how it typically fails, and the preventive, detective and escalation controls that keep it reliable.

Link 1: Source Evidence	
Objective	Establish the controlled source that proves the fact.
Responsible role	Source owner, for example Procurement, Legal, Regulatory Affairs or HR.
Evidence	Executed contract or PV agreement, regulatory database record, approved organisation record or system inventory entry.
Typical failure	The "source" is an email, a draft or an unsigned document.
Preventive control	A source hierarchy that defines acceptable evidence for each object type.
Detective control	An evidence-type check before verification.
Escalation	To the data owner if no controlled source exists.

Link 2: Structured Record	
Objective	Capture the fact as a structured object with identifier, scope and dates.
Responsible role	Data owner, or the local submitter for local facts.
Evidence	The record, linked to its source.
Typical failure	Wrong legal entity, wrong territory, or a planned arrangement recorded as active.
Preventive control	Mandatory fields, controlled vocabularies and matching against the entity master.
Detective control	Duplicate and anomaly detection.
Escalation	Rejection back to the submitter.

Link 3: Verification	
Objective	Confirm that the record matches the source and operational reality.
Responsible role	Local verifier for local facts; data owner for master facts.
Evidence	A verification entry recording the verifier, the date and the evidence viewed.
Typical failure	Rubber-stamping.
Preventive control	Competence requirements, source evidence shown in the review screen, and segregation between submitter and verifier.
Detective control	Sampling of review quality.
Escalation	To the PSMF owner or PV Quality.

Link 4: Impact Assessment	
Objective	Determine which PSMF sections, annexes, countries, products and processes are affected, and whether the QPPV must be informed.
Responsible role	PSMF owner and global process owner.
Evidence	An impact-assessment record.
Typical failure	PSMF relevance wrongly dismissed, or a dependency missed because it is not modelled.
Preventive control	Relationship-based impact rules combined with human review.
Detective control	Periodic review of "no impact" decisions.
Escalation	To the QPPV for material changes.

Link 5: Human Approval	
Objective	Accountable acceptance of the factual record and of its PSMF consequence.
Responsible role	An approver with delegated authority.
Evidence	Electronic approval capturing identity, date, record version and the meaning of the signature.
Typical failure	Approval by someone without authority.
Preventive control	A delegated-authority matrix enforced by the workflow.
Detective control	Audit of approval authority.
Escalation	The approval is invalidated and the record returns to review.

Link 6: Effective System State	
Objective	The approved record becomes part of the system state from its documented effective-from date.
Responsible role	PSMF owner; the platform applies the state change.
Evidence	A versioned record with effective dates.
Typical failure	A future arrangement shown as current, or a late change applied without retrospective assessment.
Preventive control	A multi-temporal data model (Section 9).
Detective control	A temporal anomaly report.
Escalation	Correction through a new version.

Link 7: Controlled PSMF Generation	
Objective	Assemble PSMF content from approved, in-scope records and release it under document control.
Responsible role	PSMF owner or document owner.
Evidence	A generation record identifying the template version, the record snapshot and the output identifier, and the release approval.
Typical failure	Template logic omits records, or includes unapproved or future-dated ones.
Preventive control	Tested templates and a filter that admits only approved records effective on the version date.
Detective control	Reconciliation of the output against the record snapshot.
Escalation	Release is blocked.

Link 8: Inspection Evidence	
Objective	Provide released documents and supporting evidence on request.
Responsible role	PSMF owner, supported by the QPPV office.
Evidence	Released version, logbook, evidence index and approval history.
Typical failure	An unapproved draft or a dashboard view is presented as the PSMF.
Preventive control	Release-state control and immutable output identifiers.
Detective control	Inspection-readiness drills.
Escalation	To the QPPV immediately.

Automating one link does not validate the chain. A thoroughly tested generation engine (Link 7) produces a perfectly formatted wrong annex if Links 1 to 3 were weak. Assurance effort has to follow the weakest link, which is rarely the most visible one.

7. The Source-to-Statement Rule

Author-proposed framework. Not a regulatory standard.

> **The rule.** Every material statement in a generated PSMF should be traceable to an approved structured record, identifiable source evidence, a responsible owner, a documented review and approval decision, an effective date and the applicable PSMF scope. Where AI contributed, the statement should also be traceable to the model and provider version, the prompt and template version, and the retrieval set used.

7.1 Necessary but not sufficient

Traceability proves that a statement has a pedigree. It does not prove:

- that the source was complete, since a traceable provider list can still omit a provider;
- that the evidence was authentic;
- that the regulatory interpretation was correct;
- that all relevant records were selected;
- that the statement is still valid after a later change.

The rule therefore needs six supplementary controls:

- **Completeness controls:** reconciliation against procurement, finance, product and programme registers.
- **Reconciliations:** systematic comparison across authoritative sources.
- **Source authentication:** confirmation that the evidence is the executed or controlled version.
- **Periodic certification:** owners confirm that nothing material is missing.
- **Regulatory review:** qualified professionals confirm the interpretation.
- **Historical reconstruction:** the ability to show what the statement rested on when it was released.

7.2 The email principle

> **An email may trigger a controlled change assessment, but it should not automatically become approved PSMF truth.**

An email can legitimately be evidence that a notification was sent, that an instruction was given, or that a decision was taken, where governance allows decisions to be recorded that way. It cannot replace verification of the underlying fact. An affiliate's email saying "we have a new literature vendor from March" opens a change record. The executed agreement, the qualification record and local verification establish the fact.

7.3 Supporting source hierarchy

Source category	Suitable to establish master facts	Suitable to trigger change
Approved regulatory record, validated regulatory database	Yes, for regulatory and product facts	Yes
Executed contract or PV agreement	Yes, for the delegated scope	Yes
Approved HR or organisation record	Yes, for role facts	Yes
Approved system inventory, controlled document system	Yes, for system and document facts	Yes
Approved Country PV Profile	Yes, for local arrangements	Yes
Audit, inspection, deviation or CAPA record	Yes, for quality status	Yes
Approved meeting decision	Limited, depending on governance	Yes
Email or informal communication	No	Yes
AI-generated suggestion	No. Only the controlled source it points to can establish the fact	Yes

8. PSMF Information Objects

A structured PSMF rests on a limited number of object types. Their value lies less in the objects themselves than in the relationships between them.

8.1 Core relationships

Organisation and scope. An MAH holds marketing authorisations (MAs) and one or more PSMFs. Each PSMF covers defined products and, through them, countries. A country has local requirements, local roles and a Country PV Profile. Legal entities and sites perform PV activities.

People and roles. A person holds a role, such as QPPV, deputy or local contact person, for a defined period, and a deputy is named where required. Every role change therefore has a start date, an end date and a successor, which is exactly what the PSMF must reflect.

Delegation. A provider or partner performs one or more PV activities under a contract. The contract applies to defined products, territories, legal entities and dates, and it records whether further subcontracting is permitted. This chain matters more since the 2025 amendment tightened the rules on subcontracting [4].

Safety-data sources. A programme, study, registry, website or contact centre creates one or more safety-data sources, each linked to a receiving process and system.

Systems. A computerised system supports an activity, exchanges data through interfaces and data flows, and carries an assurance record.

Governance. Controlled documents govern activities and carry a version, an effective date and a scope of applicability. Regulatory requirements apply by jurisdiction and effective date. Authority communications may trigger assessments.

Quality. Audits and inspections produce findings. Findings and deviations create CAPAs, which may create change records that affect PSMF content. Key performance indicators (KPIs) measure processes and may reveal deviations.

Control. A change record captures trigger, evidence, impact, decision and implementation. Reviews and approvals attach to records and changes. Evidence records identify their source, integrity status and retention.

Output. PSMF sections and annexes define contribution rules, that is, which approved objects feed which content. A released document version references the immutable set of approved records used to generate it.

Every object should carry a minimum set of attributes: identifier, type, status, owner, source, jurisdiction and scope, effective-from and effective-to dates, transaction date, approval date, last-verified and next-certification dates, evidence link, review and approval state, related objects, change history and confidentiality classification.

8.2 Information-object catalogue

Object	Typical owner	Core relationship	Evidence	Lifecycle status	Possible PSMF contribution
MAH / legal entity	Legal / Regulatory Affairs	Holds MAs and PSMFs; hosts sites	Registry extract	Active / inactive	Organisation description
PSMF	PSMF owner	Covers products, countries, processes	Released versions, logbook	Draft / released / superseded	Whole document
Country	Global PV	Has requirements, roles, profile	Country PV Profile	Active / withdrawn	Local arrangements
Site	Legal / Facilities	Performs activities	Organisation record	Active / closed	List of sites and activities
Role / person / deputy	HR / Local PV	Person holds role for a period	Appointment record	Planned / active / ended	QPPV, contacts, organisation
Provider / partner	Procurement / Vendor Management	Performs activity under contract	Registration, qualification	Candidate / qualified / active / exited	Subcontract annex
Contract / PV agreement	Legal / Procurement	Governs provider, activity, territory, product	Executed agreement	Draft / effective / expired / terminated	Subcontract annex
PV activity	Global process owner	Performed by entity or provider, using a system	Process definition	Planned / active / retired	Process description
Safety-data source	Local PV / Global PV	Arises from programme or channel; routes to process	Source assessment	Proposed / assessed / active / closed	Sources of safety data

Object	Typical owner	Core relationship	Evidence	Lifecycle status	Possible PSMF contribution
Programme / study / registry	Programme owner	Creates safety-data sources and obligations	Protocol, approval	Planned / active / closed	Sources of safety data
Computerised system	System owner	Supports activity; has interfaces	Assurance or validation record	Planned / live / retired	Systems description
Interface / data flow	IT / system owner	Links systems or organisations	Specification, test	Designed / live / retired	Data-flow description
Controlled document	Document owner	Governs activity	Approved version	Draft / effective / retired	List of procedures
Product / MA	Regulatory Affairs	Links MAH, country and status	Regulatory database	Authorised / marketed / withdrawn / divested	Product annex
Risk-minimisation measure (RMM)	RMP owner	Applies to product and country	Implementation evidence	Planned / implemented / closed	RMP-related description
KPI	Process owner	Measures an activity	Metric definition, results	Defined / active / retired	Performance indicators
Audit / inspection	PV Quality	Produces findings	Report	Planned / completed	Audit annex
Finding / deviation / CAPA	PV Quality / process owner	Affects objects; creates change	Investigation, effectiveness check	Open / closed / verified	Major or critical deviations; quality section
Regulatory requirement	Regulatory Affairs / Global PV	Applies by jurisdiction and date	Legal text	Proposed / effective / superseded	Local requirements
Authority communication	Regulatory Affairs / QPPV office	Triggers assessment	Correspondence record	Received / assessed / closed	Indirect
Evidence record	Records owner	Supports any object	Controlled reference	Valid / expired / withdrawn	Evidence index
Change record	PSMF owner	Links trigger, evidence, impact, decision	Change file	Open / approved / implemented / closed	Logbook
Review / approval	Designated reviewer or approver	Attaches to record or change	Electronic approval	Pending / approved / withdrawn	Approval history
PSMF section / annex	PSMF owner	Defines contribution rules	Template version	Active / retired	Structure
Released document version	Document owner	References approved record snapshot	Generation and release record	Released / superseded / archived	The released PSMF

9. Temporal Truth and Historical Reconstruction

9.1 Four dates, not one

Date	Meaning
Effective-from / effective-to	When the arrangement was operationally valid
Transaction date	When the information entered the platform
Verification or approval date	When accountable people accepted the record
Publication date	When the content appeared in a released PSMF version

In a document-centred model these dates collapse into one, the date of the version. That hides the questions an inspector is most likely to ask.

9.2 Handling difficult cases

- **Future arrangements** are recorded with a future effective date. They are not shown as current before that date and generate no current-state content early.
- **Temporary arrangements** carry an explicit effective-to date and trigger an alert before expiry.
- **Late-reported changes** keep their true effective-from date alongside the later transaction date. If a provider started in March but was reported in June, a retrospective impact assessment asks whether safety data were received in the gap and whether they were processed.
- **Corrections** create a new version with a reason, and the erroneous version stays visible in the history.
- **Withdrawn approvals** are recorded as withdrawals; the original approval remains in the audit trail.
- **Superseded records** remain retrievable and linked to their successor.
- **The last known good state**, meaning the most recent approved state before an error was introduced, can be identified.

9.3 Questions the model should answer

For any date, the MAH should be able to say:

1. what was operationally true;
2. what had been reported;
3. what had been verified and approved;
4. what appeared in the released PSMF;
5. which later correction changed the record, why, and who approved it.

9.4 Status of this design

Bitemporal or multi-temporal data management is a proposed technical design. It is a strong way of meeting the legal requirements for version control, the logbook, record retrieval and traceability [3][7][8]. No PSMF-specific rule names it or prescribes a data model.

Two legal details make the design practical. The logbook must record alterations to PSMF content made within the last five years, with defined exceptions [3]. And the Implementing Regulation sets two different retention periods: the elements of the PSMF must be kept for at least five years after the described system has been formally terminated, while PV data and documents relating to individual authorised products must be kept as long as the product is authorised and for at least ten years after the marketing authorisation has ceased to exist, or longer where Union or national law requires [3].

10. The Country PV Profile

> **Author-proposed framework. Not a regulatory standard.**

10.1 Definition

The Country PV Profile is the structured interface through which local operational facts enter the controlled representation. It has six properties:

- **Structured:** discrete fields and controlled vocabularies instead of free text.
- **Conditional:** questions appear only when they apply. A country without patient support programmes is not asked about programme vendors.
- **Evidence-linked:** material answers reference controlled evidence.
- **Effective-dated:** every answer carries its validity period.
- **Certified:** the local verifier periodically confirms the profile as a whole.
- **Change-triggered:** material local changes are reported when they happen, not at the next cycle.

It replaces the annual free-text questionnaire, which produces narrative answers nobody can reconcile and invites a "no change" copied from last year.

10.2 Modules

Module	Typical content
Local roles and contacts	Local contact person, deputy, contact details, effective dates
Authority notifications	National notification requirements, submissions, proof
Organisation	Legal entity, reporting lines, interfaces with PV
Providers and partners	Entity, contract, activity, territory, product
Safety-data sources	Source types, receipt routes, systems
Programmes, studies and registries	Type, sponsor, status, data route
Literature	Local journals, provider, frequency, escalation route
Digital channels	Websites, forms, social media, moderation, adverse event route
Medical information	Intake route, transfer timeline, reconciliation
Product complaints	Interface with PV, reconciliation
Systems	Local systems, intended use, assurance status
Procedures	Applicable local and global controlled documents
Reconciliations	Parties, frequency, results, open exceptions

Module	Typical content
KPIs	Locally monitored metrics and trends
Audits and inspections	Local audits and authority inspections
Deviations and CAPAs	Open local deviations and actions
Products	Local product status, verified against the Regulatory Affairs master
Risk-minimisation measures	Local implementation of RMMs
Local legislation	National PV requirements and their changes
Authority interactions	Relevant correspondence and requests
Business continuity	Contact chain, fallback, date of last test

10.3 Local verification is not master ownership

Local PV should normally verify local operational facts. It does not necessarily own every master record, and it should not have to:

- **Provider identity** is typically owned by Procurement or Vendor Management.
- **Product status** is owned by Regulatory Affairs.
- **System assurance** is owned by the system owner, with IT Quality oversight.
- **Contract status** is owned by Legal or Procurement.

Local PV confirms the local facts: that the provider actually performs the activity in the country, from which date, and through which safety-data route. Making Local PV the owner of every record creates duplicate masters and overloads local teams.

10.4 Conditional example: a new local service provider

When a local user selects "New provider or partner", the profile asks for:

1. the provider's legal entity and registration identity, matched against the vendor master;
2. the products, territories and MAHs affected;
3. the activities performed;
4. whether the provider may receive, process, store or transmit safety information;
5. whether it has direct contact with patients or healthcare professionals;
6. the systems, databases, interfaces and data locations used;
7. any subcontractors, and whether the MAH's written consent exists;
8. the contract and PV agreement reference;
9. qualification and audit status;
10. start and planned end dates;
11. continuity and fallback arrangements;
12. source evidence;
13. the PSMF sections and annexes expected to be affected;
14. a named local verifier and a global process reviewer.

If the provider may receive safety information and no PV agreement exists, the profile does not block the submission. It escalates it immediately to PV Quality and makes it visible to the QPPV. Blocking would suppress exactly the information the MAH needs.

11. Event-Driven Change with Periodic Certification

11.1 Regulatory baseline

The law requires the PSMF to be kept up to date, version-controlled and accompanied by a logbook, and it requires major or critical deviations to be documented until resolved [3][4]. GVP expects relevant changes to be notified to the QPPV [8]. Neither prescribes a workflow.

11.2 A hybrid, not a choice

> **Author-proposed framework. Not a regulatory standard.**

Event-driven and periodic maintenance are not competitors. Event-driven reporting keeps data current but depends on people recognising and reporting events, so silent change escapes it. Periodic certification catches silent change, but only at intervals. The hybrid, which this paper calls the Event-Driven Change Framework, uses both:

- event-driven change reporting as the default;
- risk-based periodic certification, more frequent for high-risk countries and providers;
- exception-focused review, so that reviewers look at what changed or looks anomalous instead of rereading everything;
- immediate escalation of material changes.

11.3 Proposed change workflow

1. **Trigger:** an event from a controlled source, a user notification, an integration rule, an audit, an inspection, a KPI breach, a regulatory change or an AI detection.
2. **Structured notification:** a change record naming the object, jurisdiction, product, effective-from date and source.
3. **Evidence:** a link to a controlled source record, not only an email.
4. **Triage:** classification as no PSMF impact, administrative impact, material impact on the PV system, or urgent or critical impact. A person decides the class; AI may propose one.
5. **Impact assessment:** the affected sections, annexes, countries, products, providers, systems and processes.
6. **Review routing:** to the local verifier, data owner, global process owner, PV Quality, Regulatory Affairs, IT Quality or a legal specialist, as the change requires.
7. **QPPV visibility:** for material changes affecting capacity, functioning, compliance, location, QPPV oversight, critical outsourced services or product scope.
8. **Approval:** accountable human approval of the factual record and of the PSMF consequence.
9. **Effective-state update:** the approved record becomes part of the effective system state from its documented effective-from date, subject to completion of the required approval workflow. Where that date lies in the past, the retrospective assessment in Section 9.2 applies.

10. **Document generation:** proposed PSMF content is generated only from approved, in-scope records that are effective on the version date.
11. **Controlled release:** review, approval, versioning and publication.
12. **Logbook:** what changed, why, its effective-from and publication dates, who approved it, and the linked evidence.
13. **Closure:** confirmation that the change is implemented, the evidence is complete and downstream actions are done.
14. **Certification:** periodic confirmation by country and process owners.
15. **Correction without overwriting history:** errors are corrected through new versions.

11.4 Practical triggers

- A new or departing QPPV, deputy or local PV contact person.
- A new, changed or terminated provider, contract or subcontractor.
- A new patient support programme, market research programme, registry or study.
- A new website, app, social media channel or contact centre.
- A system implementation, migration, upgrade or retirement.
- A product authorisation, launch, withdrawal, divestment or transfer.
- A new or changed RMM.
- An audit or inspection finding, or a major or critical deviation.
- A repeated KPI breach.
- New national PV legislation.
- Introduction of an AI-enabled component into a PV process.

12. Appropriate AI Use Cases

EMA's reflection paper on AI anticipates AI supporting post-authorisation activities, including PV, and places responsibility on the MAH to validate, monitor and document model performance and to include AI operations in the PV system [13]. The ten guiding principles published jointly by EMA and FDA in January 2026 point the same way. Among them are human-centric design, a risk-based approach, a clear context of use, data governance and documentation, risk-based performance assessment and life-cycle management [14]. Neither document is binding law, but both indicate what regulators are likely to expect.

Seven use cases are defensible when they are bounded. Tables 1 and 2 summarise them; Table 3 shows where deterministic rules do the job better.

Table 1. AI use cases: function and risk.

Use case	Input	Output	Benefit	False-positive risk	False-negative risk
Change detection	Prior and current records or documents	Candidate differences	Finds material changes in large document sets	Formatting or wording changes flagged as substantive	Material change missed in unfamiliar phrasing
Inconsistency detection	Contracts, provider records, product and system data	Exception alerts	Cross-source reconciliation at scale	Alert fatigue	Semantic conflicts outside the model's context
Semantic extraction	Controlled agreements and documents	Proposed field values with source citations	Less manual entry	Values extracted that are not in the source	Wrong entity, date or scope extracted with confidence
PSMF impact suggestion	Change record, relationships, rules	Suggested sections, annexes and reviewers	Faster, more complete scoping	Over-routing burdens reviewers	A dependency that is not modelled is missed
Drafting	Approved records and template	Draft text or change summary	Less transcription	Overlong or generic text	Unsupported or overgeneralised statement
QPPV oversight support	Open changes, exceptions, metrics	Risk-ordered queue	Better visibility	Minor items ranked high	Material item ranked low
Inspection-package preparation	Released records and evidence index	Candidate package and index	Faster retrieval	Irrelevant content included	Unreleased content included, or evidence omitted

Table 2. AI use cases: control.

Use case	Required human control	Permitted autonomy	Validation or assurance	Monitoring	Fallback
Change detection	Owner confirms each material change	Detect only	Testing against known change sets	Ratio of detected to confirmed changes	Manual comparison
Inconsistency detection	Process owner disposes of each alert	Detect and prioritise	Measured precision and recall on labelled cases	Alert volume, disposition time	Deterministic rules only
Semantic extraction	Reviewer checks every value against the source text	Draft only	Field-level accuracy testing	Correction rate	Manual entry
PSMF impact suggestion	PSMF owner confirms scope	Suggest only	Scenario-based testing	Missed-impact findings	Rule-based routing
Drafting	Document reviewer approves wording	Draft only	Fact-check sampling	Rejection and edit rate	Template text without AI
QPPV oversight support	QPPV keeps the judgement	Prioritise only	Review of ranking logic	QPPV overrides	Unranked exception list
Inspection-package preparation	Inspection lead verifies the package	Assemble only	Test of the release-state filter	Drill results	Manual assembly

12.1 When deterministic rules are better

Many useful checks need no AI at all. Deterministic rules are transparent, testable and reproducible, and they should be preferred wherever the logic can be written down.

Table 3. Deterministic rules that often outperform AI.

Rule	Logic
Expired contract, active provider	Provider activity is active AND the contract's effective-to date has passed
Provider missing from safety sources	Provider activity includes receipt of safety data AND no safety-data source is linked
Retired SOP still referenced	Referenced document is retired or superseded
Product-status conflict	Status in the Country PV Profile differs from the Regulatory Affairs master
New role holder, old contact	Role holder has changed AND the released PSMF still shows the previous contact
Closed finding without system update	Finding is closed AND the linked change record is still open or missing

AI earns its place where the input is unstructured: reading an agreement, comparing narrative descriptions, or suggesting impacts across relationships that are not fully modelled.

13. What AI Must Not Decide

AI must not autonomously:

- determine that a provider or activity is finally not relevant to the PSMF;
- interpret binding regulatory requirements;
- approve a change;
- modify a released annex;
- close a deviation or CAPA;
- replace QPPV oversight;
- accept evidence without verification;
- treat uncontrolled email content as regulatory truth;
- reinterpret contractual responsibilities;
- delete history;
- release an inspection document;
- downgrade system risk;
- close a material inconsistency;
- place AI-generated text, from an internal or external service, directly into the PSMF.

In each case AI may still contribute. It can flag a provider as probably not relevant, retrieve and summarise cited regulatory text, extract contractual clauses, identify evidence gaps or draft a successor version. The decision stays with a qualified, accountable person.

> **The operating principle.** AI may detect, extract, compare, suggest, draft and prioritise. Accountable humans verify, assess, decide, approve and release.

14. Human Accountability and QPPV Oversight

A full RACI matrix (responsible, accountable, consulted, informed) across a dozen roles and several dozen activities is rarely read and even more rarely followed. Table 4 shows instead eight critical decisions and who provides, verifies, reviews, approves and oversees each one. The exact allocation is organisation-specific. In a small MAH one person may hold several roles, but no one should verify a critical record they submitted, and no single person should create, verify and approve it alone.

Table 4. Eight critical decisions.

Decision	Provides	Verifies	Reviews	Approves	Oversees
A local operational fact is correct	Local submitter / source owner	Local verifier	Global PV	Data owner	PSMF owner
A master record is accurate	Source owner	Data owner	PV Quality (sample)	Data owner	PSMF owner
A change is, or is not, PSMF-relevant	Submitter	Global process owner	PSMF owner	Global PV	QPPV (material changes)
A regulatory requirement applies	Regulatory Affairs	Global PV	Legal where needed	Regulatory Affairs / Global PV	QPPV
PSMF wording is correct	PSMF owner / AI draft	Document owner	Global PV, PV Quality	PSMF owner	QPPV
A PSMF version is released	PSMF owner	Document owner	PV Quality	PSMF owner, per governance	QPPV
An AI component is fit for use	AI owner	IT Quality	PV Quality, process owner	AI owner and business owner	QPPV (PV-impacting use)
A material system risk is escalated	Any role	PV Quality	Global PV	QPPV decides on action	Senior management

The QPPV's role changes but does not shrink. In a mature model the QPPV spends less time rereading unchanged text and more time on material changes, open exceptions and systemic risk. Senior management remains responsible for resources and governance.

15. System Assurance and Data Integrity

15.1 Direct PV expectations

The Implementing Regulation requires a description of the systems and databases used for safety information, including their location, functionality, operational responsibility and an assessment of their fitness for purpose. It also requires record management that ensures retrievability and traceability, a documented quality system with

performance monitoring, risk-based audits and corrective action, and defined retention periods [3]. GVP Modules I, II and IV describe how these requirements should work in practice [7][8][10].

15.2 Adapted computerised-system controls

The controls below are sensible for a structured PSMF platform. They come from computerised-system assurance practice, and several are informed by EU GMP Annex 11 [18]. Annex 11 applies by its own terms to computerised systems used as part of GMP-regulated activities. Its principles are useful by analogy, but they are not automatically binding for ordinary PSMF documentation. The revised Annex 11 and the proposed new Annex 22 on AI went through public consultation that closed in October 2025; at the time of writing they are still drafts and are not treated here as requirements [19].

Control	Application to a PSMF platform
Intended use	What the platform may and may not decide
User requirements	Traced to testing, proportionate to risk
Risk assessment	Based on the potential impact on PV compliance and patient safety
Access and segregation	Separate rights for entry, verification, approval and release
Audit trail	Field-level history of material changes
Versioning	Records and outputs versioned and never overwritten
Electronic approval	Linked to identity, date, record version and the meaning of the signature
Interfaces	Mapped, tested and monitored
Reconciliation	Periodic comparison with authoritative sources
Migration	Counts, values, history and attachments reconciled
Backup and recovery	Tested for critical PSMF data
Continuity	A manual fallback that still allows a PSMF copy within seven days of a request
Periodic review	Continuing suitability confirmed
Decommissioning	An exportable, retrievable archive preserved
Retention and retrieval	Aligned with the Implementing Regulation and national requirements

Supplier assessment should cover cloud, workflow, AI and integration providers. Where personal data are processed, such as the names and contact details of PV staff, the General Data Protection Regulation (GDPR) applies [6].

15.3 AI-specific lifecycle controls

AI components need controls on top of 15.2, described in Section 16. EMA's reflection paper expects a risk-based lifecycle approach, a defined context of use, data governance, performance assessment, monitoring and documentation [13]. The AI Risk Management Framework of the US National Institute of Standards and Technology (NIST) offers a practical vocabulary, organised around its four functions Govern, Map, Measure and Manage [15].

The EU AI Act deserves a precise reading [5]. An AI-enabled PSMF platform is not automatically a high-risk AI system. Under Article 6, a system is high-risk if it is a safety component of a product, or itself a product, covered by the Union harmonisation legislation listed in Annex I and subject to third-party conformity assessment, or if it falls within one of the use cases listed in Annex III, subject to the derogation in Article 6(3). A tool that supports PSMF documentation does not ordinarily meet these criteria merely because it operates in a regulated industry. Classification still has to be assessed against the actual intended use and deployment.

The timeline has also moved. Regulation (EU) 2026/1744, the Digital Omnibus on AI, entered into force on 27 July 2026. Obligations for Annex III high-risk systems now apply from 2 December 2027, and those for Annex I systems from 2 August 2028 [5][16]. Other provisions of the Act follow their own dates and should be assessed separately.

16. AI Assurance Package

For every AI component, the MAH should keep proportionate documentation of:

1. intended use and prohibited use;
2. users and their training;
3. data: sources, provenance, classification and privacy assessment;
4. model and provider version;
5. prompt and template version;
6. retrieval-source configuration;
7. representative test cases, including difficult and edge cases;
8. acceptance criteria defined before testing;
9. false-positive assessment;
10. false-negative assessment;
11. the human-review workflow and evidence that it works;
12. traceability of outputs to their sources;
13. monitoring measures and review frequency;
14. incident handling;
15. change control for model, prompt, retrieval corpus, rules and templates;
16. fallback to a non-AI process;
17. suspension criteria;
18. reassessment triggers;
19. retention of what is needed to reconstruct material outputs.

Proportionality matters. A component that extracts candidate fields for mandatory human verification needs lighter assurance than one that orders the QPPV's oversight queue. No single validation methodology is universally required, and public evidence on the right depth of assurance for low-risk administrative AI in PV is still thin. The rationale for the chosen depth should therefore be documented as well.

Two points are often missed. First, the false-negative rate usually matters more than the false-positive rate, because missed items never reach human review. Second, an update by the model provider is a change even when the MAH changed nothing, and it should trigger regression testing against the retained test set.

17. Measuring PSMF Control

17.1 The problem with a single percentage

A "PSMF completeness: 98%" indicator is reassuring and potentially misleading. The remaining 2% may contain an unqualified critical provider, a missing safety-data source or a product-status conflict. Completion can also be achieved by filling fields meaninglessly.

17.2 Multidimensional PSMF Status Model

> **Author-proposed framework. Not a regulatory standard.**

Dimension	Question
Completeness	Are all applicable records present, with their mandatory fields?
Currency	Have records been verified or certified within their assigned interval?
Consistency	Do records reconcile across authoritative sources?
Evidence	Does each record have valid required evidence?
Approval	Is each effective record in a current approved state?
Risk	How many critical or high exceptions are open, and how old are they?
Reconstructability	Can a valid historical state be produced on demand?
AI assurance	Are AI outputs reviewed, monitored and reproducible?

In any summary view, critical exceptions should override favourable aggregate scores.

17.3 KPI and KRI catalogue

The catalogue combines key performance indicators (KPIs) with key risk indicators (KRIs).

Table 5. KPI and KRI catalogue.

Metric	Calculation	Owner	Segment by	Interpretation and limitation
Data completeness	Complete applicable records ÷ applicable records	Data owner	Object type, country	Can drive meaningless field completion
Overdue certifications	Overdue certifications ÷ certifications due	PSMF owner	Country, risk tier	May encourage unjustified extensions
Evidence completeness	Records with valid evidence ÷ records requiring evidence	Data owner	Object type	A link may exist while the evidence is weak
Open change ageing (KRI)	Open changes beyond target ÷ open changes	PSMF owner	Triage class	Targets should be risk-based
Change processing time	Median time from trigger to closure	Process owner	Triage class	Speed may reduce review quality
Unresolved conflicts (KRI)	Open conflicts ÷ active records	Data governance	Rule, country	Depends on rule coverage
Expired contract with active activity (KRI)	Count, with ageing	Procurement / PV Quality	Provider, country	Contract databases may lag

Metric	Calculation	Owner	Segment by	Interpretation and limitation
Unqualified active providers (KRI)	Providers without current qualification ÷ active PV providers	PV Quality	Criticality	Needs a defined qualification standard
Stale document references	Retired documents cited ÷ active references	Document owner	Section	May miss external procedures
Local certification on time	On-time certifications ÷ due certifications	Local PV	Country	Can become a checkbox exercise
QPPV visibility	Material changes acknowledged ÷ material changes	QPPV office	Change type	Visibility is not approval
AI correction rate	Corrected AI outputs ÷ reviewed outputs	AI owner	Use case	A high rate may reflect strong review
AI false-positive rate	Rejected alerts ÷ reviewed alerts	AI owner	Use case	Requires labelled dispositions
AI missed-item rate (KRI)	Confirmed items the AI did not flag ÷ confirmed items	AI owner	Use case	Measurable only through independent detection, such as seeded tests, audits and reconciliations
Reconstruction success	Successful historical reconstructions ÷ drills	PSMF owner	Date range	Drills must be realistic

No regulatory threshold exists for any of these metrics. Thresholds should be risk-based, documented and adjusted to the complexity of the portfolio and the capacity of the organisation.

18. The QPPV Cockpit

Writing about the PSMF itself, one respondent in the industry survey warned of the "danger that too much [information] is included and oversight is lost" [17]. An oversight view of the underlying data carries the same risk, and the cockpit exists to prevent it. It is a risk-focused view of the exceptions that matter to QPPV oversight, showing risk, evidence, age and decision ownership. It does not replace the QPPV's professional assessment, and it does not constitute QPPV approval.

Table 6. QPPV cockpit items.

Item	Risk	Owner	Age tracked from	Evidence	Required action	Escalation	Closure criterion
QPPV or key role change	Oversight gap; wrong authority contact	PSMF owner	Effective date of change	Appointment record, proof of required notifications	Update records; notify EMA of QPPV changes, and national authorities where required	Senior management	Records and notifications complete
Overdue country certification	Stale local data	Local PV	Due date	Certification history	Certify or justify	Global PV, then QPPV	Certification complete
Unqualified provider	Outsourced activity without assurance	PV Quality	Activity start	Qualification, audit, contract	Qualify or stop the activity	QPPV	Qualified, or activity ended
Unassessed safety-data source	Missed case route	Local PV / Global PV	Detection date	Source record	Assess and approve process	QPPV if material	Process and PSMF impact approved
System without current assurance	Integrity of safety data	System owner / IT Quality	Assurance lapse	Assurance record	Complete assurance or mitigate	QPPV	Evidence accepted or mitigation active
Product-status conflict	Wrong scope	Regulatory Affairs	Detection date	Reconciliation report	Resolve the conflict	Global PV	Resolved and PSMF updated
Open major or critical finding	Material compliance risk	PV Quality	Finding date	Finding and CAPA	Implement the CAPA	Senior management	CAPA verified effective
Unapproved subcontractor	Delegation without MAH consent	Procurement / PV Quality	Detection date	Contract chain	Obtain consent or end the activity	QPPV	Written consent and terms in place
AI performance concern	Unreliable suggestions	AI owner	Incident date	Monitoring record	Investigate and retest	PV Quality; suspend if needed	Remediated and re-approved
Inspection-readiness gap	Evidence not retrievable	PSMF owner	Drill date	Drill results	Remediate	QPPV	Repeat drill passes

19. Inspection Readiness

A structured platform can support the following inspection deliverables:

- the approved PSMF and its current annexes;
- a complete logbook;
- the provider and subcontractor inventory;
- the system, interface and data-flow inventory;

- current roles and deputies;
- an evidence index with source references;
- record ownership and verification status;
- review and approval history;
- open changes and open inconsistencies, with their risk disposition;
- deviations and CAPAs;
- a register of AI-supported outputs and their human disposition;
- model, prompt, retrieval and template versions;
- generation records;
- demonstrated archive and historical retrieval.

> **An automatically assembled document is not the released PSMF until it has passed the controlled review, approval, versioning and release process.**

A dynamic dashboard can help staff find their way during an inspection. It is not a controlled regulatory document and should not be presented as one. The seven-day submission rule [1][2] is the practical test: the MAH should be able to submit the current released PSMF, and any requested part, well within that time.

20. Vendor-Neutral Target Architecture

Table 7. Target architecture layers.

Layer	Purpose	Main controls	Primary owner	Key failure risk
Source systems	Contracts, HR, regulatory, quality, documents, safety, vendors	Designation of authoritative sources, data quality	Respective source owners	The source itself is inaccurate
Ingestion and integration	Capture events and evidence references	Interface testing, reconciliation, security	IT / data engineering	Silent interface failure
Structured PSMF platform	Master data, relationships, effective dates	Access control, audit trail, lifecycle states	PSMF owner / data owners	Duplicate or unowned records
Rules engine	Mandatory fields, consistency checks	Versioned, tested rules	Process owner / IT	Rule gaps create false comfort
Workflow	Change, verification, review, approval	Segregation, escalation, electronic approval	PSMF owner	Approval without authority
Evidence repository	Controlled source documents	Immutable references, retention	Records owner	Broken or altered evidence
AI layer	Extraction, detection, suggestion, drafting	Intended use, logging, monitoring, fallback	AI owner	Unsupported output accepted
Human review	Expert verification and decision	Competence, role controls, evidence visibility	Function owners	Rubber-stamping
Document generation	Assemble PSMF versions	Template control, reconciliation, release	PSMF / document owner	Output diverges from data
QPPV cockpit	Oversight and escalation	Transparent risk logic, links to sources	QPPV office / PV Quality	Visibility mistaken for approval
Archive and retrieval	Historical reconstruction	Retention, export, retrievability	Records owner	History lost in migration

Technology choices may include low-code workflow tools, relational databases, graph layers for relationship analysis, regulatory information management (RIM) systems, controlled document management systems (DMS), rules engines, document-generation tools, private LLM services and RAG. A relational core with an optional graph layer is one reasonable design among several. No technology is inherently compliant. Suitability depends on intended use, controls, assured state, data classification and the operating model around it.

21. Practical Implementation Roadmap

Table 8. Staged roadmap.

Stage	Objective	Deliverables	Readiness evidence	Principal risk	Stop criterion
0. Governance	Define scope, intended use and risk appetite	Charter, decision rights, data policy, QPPV sponsorship	Approved governance	Treated as an IT project	No accountable owner
1. Data inventory and ownership	Identify sources and owners	Source map, object list, source hierarchy	Owners confirmed	Hidden sources	Sources unknown or unreconciled
2. Country PV Profile	Structure the capture of local facts	Profile modules, certification workflow	Local acceptance, data-quality results	Local burden	Burden out of proportion to value
3. Structured master data	Establish controlled objects	Provider, role, system, product and source records	Reconciliation with sources	Duplicate records	Duplicate or unowned records dominate
4. Event-driven workflow	Controlled change	Change record, approvals, logbook	End-to-end test trail	Unclear authority	Approval authority unclear
5. Controlled document generation	Generate selected annexes	Templates, generation reconciliation	Output equals approved data	Template errors	Mismatches cannot be explained
6. Deterministic consistency rules	Detect known inconsistencies	Rule library, exception handling	Measured rule performance	Alert overload	Alert volume overwhelms reviewers
7. Restricted AI support	Extraction and drafting assistance	Assurance package, tests, logs	Evidence of human-review performance	Over-reliance	Source traceability absent
8. QPPV cockpit and inspection package	Oversight and retrieval	Cockpit, inspection package	Successful drill	Stale data displayed	Data not current or not governed
9. Scaling	Extend to further countries and PSMFs	Configuration model	Pilot results replicated	Local variation	Local requirements unresolved

The stages describe a build sequence and do not map one-to-one onto the maturity levels in Section 25. The pilot in Section 22 exercises Stages 2 to 7 on a bounded scope, once Stages 0 and 1 are in place for that scope, and ends with an inspection-readiness drill.

AI comes late for good reasons. AI applied to ungoverned data accelerates error. Its outputs cannot be verified without authoritative sources and owners, and its performance cannot be measured without labelled, approved data to test against. Deterministic rules also set the baseline that any AI contribution has to beat.

22. Minimum Viable Pilot

22.1 Recommended focus

The recommended pilot combines the service-provider inventory with local safety-data sources. This area covers high-value PSMF content and involves both local and global ownership. It exposes the real complexity of contracts, qualification, subcontracting and safety-data routes. It has clear event triggers, suits deterministic rules, and can be tested without letting AI make any regulatory decision.

22.2 Scope

- One PV system and one PSMF.
- A limited number of countries or one region. Five to ten countries is an illustrative, manageable scope, not a prescription.
- Provider, contract, activity, country, product and safety-data source objects.
- The Country PV Profile modules for providers and safety-data sources.
- Controlled change records and an approval workflow.
- One generated inventory or annex.
- Restricted AI extraction from approved, executed agreements only, with mandatory human verification of every extracted value.

22.3 Success criteria

1. Every in-scope provider and safety-data source has an owner, evidence, effective dates and an approval.
2. The generated annex reconciles fully with the approved record set, and any difference is explained.
3. Deterministic rules find inconsistencies that were deliberately seeded for testing.
4. AI extraction accuracy meets acceptance criteria defined in advance, and every accepted value was verified by a person.
5. The platform can answer the questions in Section 9.3 for the provider inventory on a past date.
6. Local teams judge the burden acceptable compared with the previous questionnaire.
7. The QPPV confirms that material changes became visible within the defined timelines.
8. An inspection-readiness drill for the pilot scope passes, including production of the relevant annex well within the seven-day window.

Scaling should wait until these criteria are met and the lessons are documented.

23. Practical Scenarios

Scenario 1: New Local PV Manager	
Trigger	Appointment of a successor.
Structured record	Person-role assignment with effective dates, deputy and contact details.
Evidence	Appointment record.
Proposed automated support	AI: detects remaining references to the previous role holder.
Human decision	Local PV verifies the facts; Global PV confirms.
PSMF impact	Contacts and organisation annex; national contact-person notifications where local rules require them.
Approval	PSMF owner, with QPPV visibility.
Inspection trail	Change record, approval, released version and logbook entry.

Scenario 2: New literature provider	
Trigger	Contract signature.
Structured record	Provider, contract, literature activity, territory and journal scope.
Evidence	Executed agreement and qualification record.
Proposed automated support	AI: extracts candidate scope and dates and compares them with the previous provider.
Human decision	Global literature owner confirms continuity of coverage.
PSMF impact	Subcontract annex and sources of safety data.
Approval	Global PV and PV Quality.
Inspection trail	Agreement, handover evidence and logbook.

Scenario 3: New patient support programme	
Trigger	Programme approval.
Structured record	Programme, provider, safety-data source, products and countries.
Evidence	Programme documentation and PV agreement.
Proposed automated support	Rule: flags a programme with no linked safety-data route.
Human decision	PV defines the reporting process.
PSMF impact	Sources of safety data and subcontracts.
Approval	Global PV, with QPPV visibility.
Inspection trail	Process evidence, training records and reconciliation plan.

Scenario 4: New contact centre	
Trigger	Contract signature, before the service starts.
Structured record	Provider, activity, system, interface and reconciliation.
Evidence	Agreement, training records and test calls.
Proposed automated support	Rule: flags a missing interface for adverse events or product complaints.
Human decision	PV Quality confirms qualification.
PSMF impact	Subcontracts, sources of safety data and systems.
Approval	PV Quality and Global PV.
Inspection trail	Reconciliation results and qualification record.

Scenario 5: New local website	
Trigger	Launch request.
Structured record	Digital channel, form, receiving system and monitoring responsibility.
Evidence	Test of the adverse event intake route.
Proposed automated support	Rule: flags a channel with no mapped safety intake.
Human decision	Local PV verifies that the route works.
PSMF impact	Sources of safety data.
Approval	Local PV and the digital owner for the intake route; Global PV for the PSMF impact.
Inspection trail	Test evidence and monitoring log.

Scenario 6: Safety database migration	
Trigger	Migration project.
Structured record	New system, retired system, interfaces and migration event.
Evidence	Assurance package and migration reconciliation.
Proposed automated support	AI: finds references to the old system across controlled documents.
Human decision	IT Quality, PV and the QPPV accept the migration.
PSMF impact	Systems, data flows and procedures.
Approval	Global PV, under QPPV oversight.
Inspection trail	Reconciliation report and read-only access to the legacy archive.

Scenario 7: Provider contract termination	
Trigger	Notice of termination.
Structured record	Contract end date, activity transition, data transfer and retention.
Evidence	Termination record and exit plan.
Proposed automated support	Rule: flags a provider still shown as active after expiry (Table 3).
Human decision	PV Quality confirms the transition.
PSMF impact	Subcontract annex.
Approval	Global PV.
Inspection trail	Exit evidence and confirmation of data return.

Scenario 8: Product divestment	
Trigger	Transfer agreement.
Structured record	Product and MA status, contract scope and system access.
Evidence	Transaction and handover record.
Proposed automated support	Rule: lists affected providers, systems and countries from modelled relationships. AI: suggests links that are not modelled.
Human decision	Regulatory Affairs, PV and the QPPV agree the transition date.
PSMF impact	Product annex and contracts.
Approval	Global PV, under QPPV oversight.
Inspection trail	Handover agreement and effective-dated product record.

Scenario 9: New risk-minimisation measure	
Trigger	Approval of the RMP change.
Structured record	RMM per product and country.
Evidence	Implementation evidence per country.
Proposed automated support	AI: suggests links to related local programmes and channels.
Human decision	RMP owner confirms implementation.
PSMF impact	RMP-related description where applicable.
Approval	Global PV.
Inspection trail	Implementation records per country.

Scenario 10: Inspection finding	
Trigger	Inspection report.
Structured record	Finding, affected objects and CAPA.
Evidence	Report and CAPA plan.
Proposed automated support	AI: suggests related records that may be affected.
Human decision	PV Quality and the QPPV approve the CAPA.
PSMF impact	Deviations section while a major or critical deviation remains unresolved; quality-system section.
Approval	Global PV, under QPPV oversight.
Inspection trail	CAPA and effectiveness evidence.

Scenario 11: Repeated KPI failure	
Trigger	Breach in consecutive periods.
Structured record	KPI result, deviation and CAPA.
Evidence	Metric data and investigation.
Proposed automated support	Rule: detects the trend and a missing CAPA.
Human decision	Process owner classifies the deviation.
PSMF impact	Performance indicators; deviations section if major or critical.
Approval	PV Quality.
Inspection trail	Trend report and root-cause analysis.

Scenario 12: New AI-enabled PV service	
Trigger	Procurement of an AI-supported case-processing service.
Structured record	Provider, system, AI component and intended use.
Evidence	Assurance package, test results and fallback plan.
Proposed automated support	None in the acceptance decision; a checklist may be pre-populated.
Human decision	IT Quality, PV and the QPPV accept the service.
PSMF impact	Systems, subcontracts and quality-system description.
Approval	Global PV, under QPPV oversight.
Inspection trail	Model and monitoring evidence, change control.

24. Failure Modes and Red Flags

Table 9. Red flags.

Failure mode	Consequence	Prevention	Detection	Escalation	Fallback
Wrong legal entity	Contractual and PSMF statements inaccurate	Matching against the entity master	Evidence check	Data owner	Correct the mapping in a new version

Failure mode	Consequence	Prevention	Detection	Escalation	Fallback
Planned activity treated as active	PSMF overstates the system	Mandatory status and dates	Future-date rule	PSMF owner	Revert to the approved state
Obsolete contract	Activity performed without valid terms	Contract lifecycle alerts	Expired-contract rule	PV Quality	Hold publication pending review
Email accepted as master truth	Unsupported PSMF statement	Source hierarchy	Evidence-type check	PSMF owner	Convert into a verified change record
Missed subcontractor	Hidden delegation	Mandatory subcontractor declaration	Contract and audit reconciliation	PV Quality, QPPV	Retrospective assessment
Unreported programme	Missed safety-data source	Country PV Profile certification	Programme register comparison	Global PV	Retrospective case reconciliation
Product-status conflict	Wrong scope	Regulatory Affairs master designation	Reconciliation rule	Regulatory Affairs	Show the conflict; hold generation
Wrong effective date	Incorrect history	Date validation against evidence	Temporal anomaly report	Data owner	Versioned correction
Unsupported AI-generated claim	False PSMF content	Drafting from approved records only, with citations	Mandatory reviewer fact check	AI owner	Reject the draft; log an incident
Reviewer rubber-stamping	Errors pass verification	Evidence shown in review; competence	Review-quality sampling	PV Quality	Re-review the sample
Alert fatigue	Real exceptions ignored	Tuning and prioritisation	Alert-volume metric	Process owner	Suspend the noisy rule or model
Uncontrolled model or prompt change	Behaviour changes silently	Version registry, change control	Regression testing, configuration audit	AI owner	Roll back to the approved version, or use the non-AI fallback
Overwritten history	Reconstruction impossible	Append-only versioning	Audit-trail review	PSMF owner	Restore from backup
Generated annex differs from approved data	Released content wrong	Generation reconciliation	Independent sample check	Document owner	Block release; if already released, correct through a new version
Unapproved data used for inspection output	Misleading a regulator	Release-state filter	Package release control	QPPV	Regenerate from the approved snapshot
Non-reconstructable AI output	Decision cannot be defended	Logging of output, sources and versions	Traceability drill	AI owner	Disable the use case
Migration loss	History or evidence lost	Migration requirements	Comparison before and after migration	IT Quality	Read-only legacy archive

25. AI-Enabled PSMF Maturity Model

Author-proposed framework. Not a regulatory standard.

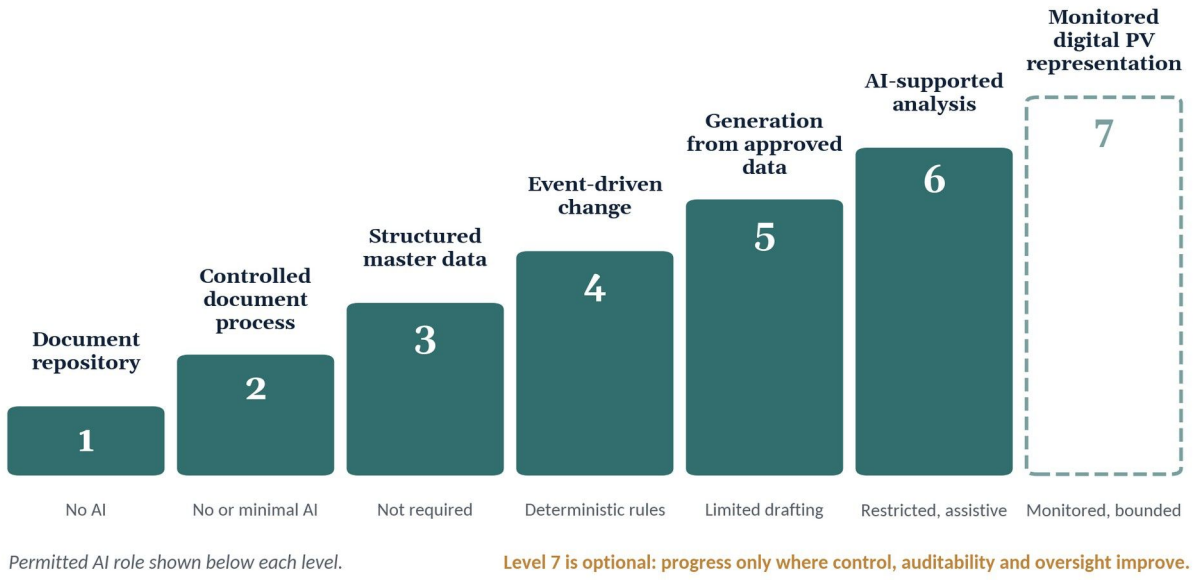

Figure 4. The seven levels of the AI-Enabled PSMF Maturity Model.

Level 1: Document repository	
Characteristics	PSMF files stored centrally; updates are ad hoc.
Required evidence	Released versions and logbook.
Typical weakness	Stale, manually collected content.
Inspection risk	High for accuracy and currency.
Local PV role	Answers requests.
Global PV role	Compiles the document.
QPPV role	Reviews full documents.
Permitted AI role	None.
Progression criterion	Controlled ownership and versioning in place.

Level 2: Controlled document process	
Characteristics	Templates, review cycles and logbook discipline.
Required evidence	Review records and change history.
Typical weakness	Periodic manual collection persists.
Inspection risk	Moderate, with gaps between cycles.
Local PV role	Completes questionnaires.
Global PV role	Consolidates and reviews.
QPPV role	Reviews versions.
Permitted AI role	None or minimal.
Progression criterion	Source ownership defined.

Level 3: Structured master data	
Characteristics	Core objects held as controlled records.
Required evidence	Owners, evidence links and reconciliations.
Typical weakness	Changes still batch-driven.
Inspection risk	Reduced for inventories.
Local PV role	Verifies local records.
Global PV role	Owns the data model and data quality.
QPPV role	Reviews exceptions and versions.
Permitted AI role	Not required.
Progression criterion	Relationships and effective dates implemented.

Level 4: Event-driven change management	
Characteristics	Trigger-to-approval workflow combined with periodic certification.
Required evidence	Change records, approvals and certifications.
Typical weakness	Documents still written by hand.
Inspection risk	Low to moderate.
Local PV role	Reports changes and certifies.
Global PV role	Triages and assesses impact.
QPPV role	Sees material changes promptly.
Permitted AI role	None; deterministic rules and alerts.
Progression criterion	Reliable effective dates and audit trail.

Level 5: Automated generation from approved data	
Characteristics	Approved records populate PSMF outputs.
Required evidence	Generation records and reconciliation.
Typical weakness	Errors in template logic.
Inspection risk	Low if outputs are reconciled.
Local PV role	Verifies.
Global PV role	Controls templates and release.
QPPV role	Oversees releases.
Permitted AI role	Limited drafting, under review.
Progression criterion	Outputs reconcile fully with the record set.

Level 6: AI-supported analysis	
Characteristics	Extraction, inconsistency detection and impact suggestions.
Required evidence	Assurance packages and performance data.
Typical weakness	Over-reliance and review fatigue.
Inspection risk	Depends on the quality of assurance.
Local PV role	Verifies AI-extracted facts.
Global PV role	Disposes of alerts.
QPPV role	Oversees AI-related risk.
Permitted AI role	Restricted and assistive.
Progression criterion	Demonstrated performance and governance.

Level 7: Continuously monitored digital PV representation	
Characteristics	Integrated sources, multidimensional monitoring and on-demand historical reconstruction.
Required evidence	Monitoring records, drills and periodic reviews.
Typical weakness	Heavy assurance and governance burden.
Inspection risk	Low if demonstrated.
Local PV role	Certifies by exception.
Global PV role	Governs the system.
QPPV role	Continuous, risk-focused oversight.
Permitted AI role	Monitored, bounded support.
Progression criterion	Reliable operation, auditability and oversight sustained over time.

Level 7 is not required, and it is not appropriate for every MAH. A small MAH with a stable system may be well controlled at Level 4 or 5. Technological complexity counts as maturity only when it demonstrably improves control, auditability and oversight.

26. Conclusions and Practical Recommendations

The PSMF remains a controlled regulatory document. What should change is how it is maintained: from periodic manual consolidation to governed, effective-dated and evidence-linked system data. The PSMF describes the PV system but is not the system, and the controls that matter most sit between operating reality and the data.

Structured data are not automatically trustworthy. A well-built database of unverified facts is only a faster route to an inaccurate PSMF. Trust comes from the Truth Chain: controlled sources, verification, impact assessment, accountable approval and controlled generation.

AI is useful only inside that chain. It can find what changed, compare what disagrees, extract what documents say and draft what approved records support. Accountable people stay responsible for deciding what is true, what it means and what is released.

Local factual verification remains essential. No central platform can reliably know that an affiliate engaged a new vendor unless someone locally reports and confirms it.

QPPV oversight does not become less important. It becomes more focused on risk: fewer hours rereading unchanged annexes, more attention to material change, open exceptions and systemic weakness.

The practical path is a bounded, testable pilot. Govern first, then establish data ownership, structure the facts, control change, generate from approved records and apply deterministic rules. Only then introduce restricted AI with documented assurance. Throughout, inspection readiness depends on approved records and decisions that can be reconstructed, far more than on the technology used.

Disclaimer

This whitepaper presents the author's professional views and author-proposed frameworks. It is not legal advice and does not represent the position of any regulatory authority. Regulatory references reflect the sources listed below as of 23 September 2026. Readers should check current versions before relying on them.

Abbreviations

Abbreviation	Meaning
AI	Artificial intelligence
CAPA	Corrective and preventive action
DMS	Document management system
EFPIA	European Federation of Pharmaceutical Industries and Associations
EMA	European Medicines Agency
FDA	US Food and Drug Administration
GDPR	General Data Protection Regulation
GMP	Good Manufacturing Practice
GVP	Good Pharmacovigilance Practices
HMA	Heads of Medicines Agencies
HR	Human resources
ICSR	Individual case safety report
IT	Information technology
KPI / KRI	Key performance indicator / key risk indicator
LLM	Large language model
MA	Marketing authorisation
MAH	Marketing authorisation holder
NIST	US National Institute of Standards and Technology
PSMF	Pharmacovigilance system master file
PSUR	Periodic safety update report
PV	Pharmacovigilance
QPPV	Qualified Person Responsible for Pharmacovigilance
RACI	Responsible, accountable, consulted, informed
RAG	Retrieval-augmented generation
RIM	Regulatory information management
RMM	Risk-minimisation measure
RMP	Risk management plan
SOP	Standard operating procedure

References

Binding EU law

[1] European Parliament and Council. Directive 2001/83/EC on the Community code relating to medicinal products for human use. Consolidated version of 1 January 2025. Binding EU law. https://eur-lex.europa.eu/eli/dir/2001/83/2025-01-01/eng

[2] European Parliament and Council. Regulation (EC) No 726/2004 laying down Union procedures for the authorisation and supervision of medicinal products and establishing a European Medicines Agency, as amended (Article 16(3a) on submission of the PSMF). Binding EU law. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32004R0726

[3] European Commission. Commission Implementing Regulation (EU) No 520/2012 on the performance of pharmacovigilance activities. Consolidated version of 12 February 2026. Binding EU law. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02012R0520-20260212

[4] European Commission. Commission Implementing Regulation (EU) 2025/1466 of 22 July 2025 amending Implementing Regulation (EU) No 520/2012. OJ L, 23.7.2025; most provisions applicable from 12 February 2026. Binding EU law. https://eur-lex.europa.eu/eli/reg_impl/2025/1466/oj/eng

[5] European Parliament and Council. Regulation (EU) 2024/1689 (Artificial Intelligence Act). Consolidated version of 27 July 2026, including the amendments made by Regulation (EU) 2026/1744 (Digital Omnibus on AI). Binding EU law. https://eur-lex.europa.eu/eli/reg/2024/1689/2026-07-27/eng

[6] European Parliament and Council. Regulation (EU) 2016/679 (General Data Protection Regulation). Binding EU law. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

EU pharmacovigilance guidance

[7] EMA and HMA. Guideline on good pharmacovigilance practices (GVP), Module I: Pharmacovigilance systems and their quality systems. 2012. Final guidance. https://www.ema.europa.eu/en/documents/scientific-guideline/guideline-good-pharmacovigilance-practices-module-i-pharmacovigilance-systems-and-their-quality-systems_en.pdf

[8] EMA and HMA. GVP Module II: Pharmacovigilance system master file (Rev 2), EMA/816573/2011 Rev 2. In effect since 31 March 2017. Final guidance. https://www.ema.europa.eu/en/documents/scientific-guideline/guideline-good-pharmacovigilance-practices-module-ii-pharmacovigilance-system-master-file-rev-2_en.pdf

[9] EMA and HMA. GVP Module III: Pharmacovigilance inspections (Rev 2), EMA/119871/2012 Rev 2 of 4 September 2026. In effect since 10 September 2026. Final guidance. https://www.ema.europa.eu/en/documents/scientific-guideline/guideline-good-pharmacovigilance-practices-module-iii-pharmacovigilance-inspections-rev2_en.pdf

[10] EMA and HMA. GVP Module IV: Pharmacovigilance audits (Rev 1). Final guidance. https://www.ema.europa.eu/en/documents/scientific-guideline/guideline-good-pharmacovigilance-practices-gvp-module-iv-pharmacovigilance-audits-rev-1_en.pdf

[11] EMA. Good pharmacovigilance practices (GVP): overview of current modules and revisions. Web page. https://www.ema.europa.eu/en/human-regulatory-overview/post-authorisation/pharmacovigilance-post-authorisation/good-pharmacovigilance-practices-gvp

[12] EMA. Pharmacovigilance system: questions and answers. Procedural guidance, web page. https://www.ema.europa.eu/en/human-regulatory-overview/post-authorisation/pharmacovigilance-post-authorisation/pharmacovigilance-system-questions-answers

AI governance: reflection papers, principles and frameworks

[13] EMA (CHMP and CVMP). Reflection paper on the use of artificial intelligence (AI) in the medicinal product lifecycle, EMA/CHMP/CVMP/83833/2023. 9 September 2024. Final reflection paper; not legally binding.

https://www.ema.europa.eu/en/documents/scientific-guideline/reflection-paper-use-artificial-intelligence-ai-medicinal-product-lifecycle_en.pdf

[14] EMA and FDA. Guiding principles of good AI practice in drug development. 14 January 2026. Voluntary principles. https://www.ema.europa.eu/en/news/ema-fda-set-common-principles-ai-medicine-development-0

[15] National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1. January 2023. Voluntary framework. https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf

[16] European Commission, AI Act Service Desk. Timeline for the implementation of the EU AI Act. Official information page. https://ai-act-service-desk.ec.europa.eu/en/ai-act/timeline/timeline-implementation-eu-ai-act

Scientific and industry evidence

[17] Lavery C, Emmott J, Jeck-Thole S, Rouben P, Usher D, van der Spuij W, Woodward L. An industry survey on managing the pharmacovigilance system master file in a global environment: the need for a pragmatic approach. Pharmaceutical Medicine. 2022;36(4):233-245. doi:10.1007/s40290-022-00422-2. Peer-reviewed industry survey. https://pmc.ncbi.nlm.nih.gov/articles/PMC9334448/

Transferred and draft GMP guidance

[18] European Commission. EudraLex Volume 4, Annex 11: Computerised systems. 2011. GMP guidance; used in this paper by analogy only. https://health.ec.europa.eu/system/files/2016-11/annex11_01-2011_en_0.pdf

[19] European Commission. Stakeholders' consultation on EudraLex Volume 4: Chapter 4, Annex 11 and new Annex 22 (Artificial Intelligence). Consultation held 7 July to 7 October 2025 (closed); documents are drafts. https://health.ec.europa.eu/consultations/stakeholders-consultation-eudralex-volume-4-good-manufacturing-practice-guidelines-chapter-4-annex_en