Global Harmonization Working Party
GHWP Towards Medical Device Harmonization

PROPOSED DOCUMENT

Title: Playbook for Design and Implementation of Active Post-Market Surveillance System

Authoring Group(s): Working Group 4 - Post-Market

Date: **September 2025**

Acknowledgement

This GHWP Document was prepared by Global Harmonization Working Party (GHWP), Working Group 4 (Post-Market). Special acknowledgment is extended to **Professor Pei GAO** (Working Group 4 Advisor) and her exceptional team at Peking University, including **Xun TANG, Huijuan LI, Tianran XU, Chenxuan WANG, Jiajun QIAN, and Yingying TENG**. Their dedication and expertise were instrumental in the development of this playbook, ensuring it meets the highest standards of quality and relevance. This playbook was endorsed by the GHWP.

Contents

Foreword

This GHWP Document was developed by the Global Harmonization Working Party (GHWP), Working Group 4 (Post-Market). The Working Group members include Kitty Mao, Abdulmohsen AL-HAJLAN, Sara ALHARTHI, Yan ZHAO, Dong LI, Xiaoxue WANG, Pei GAO, Xun TANG, Huijuan LI, Aisha AL-GHAITHI, and Wentao Vincent WANG, under the leadership of Dr. Ambrose Wong and Dr. Aaron Hung, Chair and Acting Chair of GHWP Working Group 4 (Post-Market). GHWP is a voluntary group of representatives from medical device regulatory authorities and the regulated industry. This document is intended to provide non-binding guidance for use in the regulation of medical devices, and subject to consultation throughout its development process.

This GHWP Document shall be read in conjunction with the current laws and regulations used in member economies.

Any statements or references from external sources are used under appropriate citations as specified in the normative references and bibliography.

There are no restrictions on the reproduction, distribution, translation or use of this document. However, incorporation of this document, in part or in whole, into any other document does not convey or represent an endorsement of any kind by the Global Harmonization Working Party.

In this GHWP Document, the following verbal forms are used:

— “shall” indicates a requirement;

— “should” indicates a recommendation;

— “may” indicates a permission; and

— “can” indicates a possibility or a capability.

1. Introduction

The safety and effectiveness of medical devices throughout their lifecycle are paramount to public health. Robust post-market surveillance (PMS) is essential for stakeholders – including regulatory authorities, manufacturers and healthcare providers – to monitor medical devices by collecting and analyzing data to detect, assess, understand, and respond to adverse events or other device-related problems after market entry.

Currently, passive surveillance, primarily reliant on spontaneous or voluntary adverse event reporting (AER), remains the predominant approach for PMS globally. While valuable for signal detection, this method is inherently constrained by well-documented limitations, including significant underreporting, reporting delays, data incompleteness, and the absence of reliable denominator data (i.e., population exposure), which limit the timely identification and mitigation of emerging safety risks associated with medical devices.

In contrast, the concept of active surveillance presents a compelling alternative. By systematically leveraging diverse data sources (such as electronic health records, registries, and claims databases) and employing rigorous analytical methodologies, active surveillance aims to proactively monitor device performance within populations continuously. This approach can identify potential safety signals earlier, characterize risks more comprehensively, and provide real-world evidence on the effectiveness and safety of the device.

While the concept and application of active surveillance are relatively well-established and increasingly harmonized in pharmacovigilance, the landscape for medical devices is markedly different and more complex. The inherent heterogeneity of medical devices, the influence of user technique on outcomes, iterative product development cycles, and challenges in unique device identification present distinct methodological hurdles. Consequently, definitions, methodologies, and best practices for medical devices' active surveillance remain varied and lack global consensus. The field is still in its formative stages, with significant variations in implementation across regions and limited standardized guidance.

This lack of harmonization presents a challenge for regulators, manufacturers, healthcare providers, and ultimately, patient safety on a global scale. There is an urgent and recognized need for international convergence on aligned standards, common definitions, and practical frameworks for the active surveillance of medical devices.

The Global Harmonization Working Party (GHWP), dedicated to promoting convergence in medical device regulatory practices among its member National Regulatory Authorities (NRAs), recognizes this critical gap. This Document, part of a series of GHWP Documents on Active Post-Market Surveillance (APMS) for medical devices, aims to address this need. It seeks to promote a common understanding of APMS concepts, outline core principles for methodology and governance, and provide foundational guidance to facilitate the development and implementation of effective, harmonized active surveillance systems for medical devices worldwide.

This Document is intended to provide non-binding guidance for use in the regulation of medical devices, and is subject to consultation throughout its development process.

The GHWP Document shall be read in conjunction with the current laws and regulations used in member economies.

2. Purpose

This Document provides a foundational framework for implementing active post-market surveillance systems for medical devices. Its primary objectives are to:

i. **Establish Standardized Terminology**: Define core concepts and harmonized terminology specific to medical device active surveillance, reducing ambiguity and fostering global alignment among regulators, industry, and healthcare stakeholders.
ii. **Outline a Scalable System Architecture**: Propose a functional and technical architecture for APMS systems, detailing essential components (e.g., data integration, analytics, signal management) and their interoperability to support adaptable implementation across jurisdictions.
iii. **Characterize Fit-for-Purpose Data Sources**: Evaluate real-world data (RWD) sources (e.g., electronic health records, registries, claims databases, wearable devices) for applicability to APMS, addressing their strengths and limitations specific to medical device surveillance.
iv. **Define Key System Attributes and Sustainability Principles**: Identify critical characteristics of effective APMS systems (e.g., timeliness, representativeness, analytical rigor), and provide guidance on ensuring long-term operational viability through resource optimization, system governance, and adaptive maintenance strategies.

3. Scope

This Document applies to Active Post-Market Surveillance for legally marketed medical devices. It establishes principles for designing and operating a closed-loop surveillance framework that encompasses a proactive data ecosystem, dynamic signal detection and validation, predictive risk assessment and decision-making, corrective action integration, real-world performance feedback, and a self-optimizing architecture. It enables systematic surveillance activities, including not only pre-planned methodologies for continuous safety and performance monitoring but also scenarios of reactive investigations (e.g., triggered by passive reports).

Target Stakeholders

This Document primarily addresses the following stakeholders involved in the design, implementation, and operation of APMS systems:

i. **Regulatory authorities** set standards and expectations for APMS frameworks. They establish technical standards, define surveillance requirements, and enforce regulations requiring manufacturers to implement robust APMS systems. They may directly operate national APMS systems or delegate operational functions to accredited third-party entities while retaining oversight accountability.
ii. **Manufacturers** act as data contributors and compliance executors. They furnish device-specific data (e.g., Unique Device Identification (UDI) traceability logs, production batch records) and implement corrective actions, leveraging APMS outputs for risk management under regulatory mandates.
iii. **Healthcare institutions and providers** function as essential evidence generators and frontline operators. They integrate surveillance protocols into clinical workflows,

contribute electronic health records and registry data, and execute field safety actions (e.g., device firmware updates in hospital networks).

iv. **Third-party technical operators** (when delegated by regulators) assume system implementation/maintenance roles, managing infrastructure such as data lakes, analytical pipelines, and cybersecurity controls under regulatory supervision.

NOTE. Patients participate indirectly through ethical data governance mechanisms; their safety interests are represented via regulator-led benefit-risk assessments.

While APMS Systems require multi-stakeholder collaboration, this document specifically directs regulators in establishing national or regional APMS infrastructures, as GHWP membership primarily comprises regulatory authorities. All stakeholder obligations described herein derive exclusively from regulatory mandates enacted within respective jurisdictions.

Technical Boundaries

This Document establishes principles for the APMS system by defining its technical scope and boundaries. This Document focuses on conceptual frameworks for end-to-end surveillance architecture and evidence-based best practices that have been validated through scientific literature and established regulatory precedents. More importantly, this Document does not prescribe specific technical implementations, including particular analytical algorithms (such as machine learning models for signal detection), commercial database solutions (like proprietary electronic health record platforms or data vendors), or IT infrastructure specifications (including cloud architecture or hardware requirements). The framework is designed to provide flexible, principle-based guidance while allowing for technological adaptability across different implementation environments.

4. Normative References

There are no normative references in this document.

5. Terms and Definitions

5.1 Active Post-Market Surveillance (APMS) constitutes a continuous, scientifically rigorous process to proactively monitor the safety and performance of medical devices throughout their lifecycle. By applying validated analytical protocols to diverse real-world data sources, including the existing spontaneous report system for the adverse event report, electronic health records, and device registries etc., APMS enables the detection of emerging safety signals, validation of known risk hypotheses, and data-driven decision-making for corrective actions. The outcomes of this surveillance are systematically disseminated to key stakeholders (regulators, manufacturers, healthcare providers, and the public, as appropriate) to ensure transparency and collaborative risk management within the medical device ecosystem.

5.2 Active Post-Market Surveillance System: An APMS system is a system designed to operationalize APMS activities through a closed-loop architecture. This system comprises multiple functionally interconnected components that form a continuous surveillance cycle.

5.3 Passive Post-Market Surveillance is a monitoring process reliant on spontaneous adverse event reporting from relevant stakeholders such as healthcare providers, patients and manufacturers. It employs manual data aggregation and reactive analyses of reported datasets to identify known risks, with decision-making constrained by reporting biases and delayed access to clinical context. Outcomes are communicated through various means such as periodic regulatory notifications and manufacturer-initiated field actions.

5.4 Safety Signal is the information arising from one or multiple sources that suggests a new, potentially causal association between a medical device and an event or set of related events (often adverse) that is of sufficient likelihood to warrant further investigation. Safety signals may originate from various data sources, including existing adverse event reports and continuous monitoring activities in APMS.

5.5 Data Ecosystem refers to an interconnected network of structured and unstructured real-world data sources, including EHRs, insurance claims, device registries, and/or patient-generated data, integrated through standardized protocols. This ecosystem enables the generation of longitudinal evidence by transforming raw inputs into risk-computable streams while preserving data provenance.

5.6 Signal Detection in APMS is a systematic process that involves recognizing potential safety concerns related to a medical device through the collection, monitoring, and analysis of data from multiple sources. This process primarily employs the quantitative statistical methods to identify patterns or trends that suggest new safety issues, changes in known safety profiles, new at-risk populations, or unintended product uses that warrant formal recognition and further investigation.

5.7 Signal Validation in APMS is a rigorous and multi-stage process to verify the validity of detected safety signals that begins with an initial assessment of confirming data quality, establishes the association within one type of data source between the medical device and the suspected clinical event, and followed by the comprehensive analysis by multiple data sources with careful considerations for confounding factors. The results of the signal validation are crucial for triggering the next step in APMS, informing a regulatory decision.

5.8 Risk Assessment constitutes the systematic process of evaluating identified hazards to determine their impact on a medical device's benefit-risk profile. In passive surveillance, this can involve committee review of severity-frequency matrices derived mainly from the spontaneous reporting system. Active surveillance may employ complicated evidence synergy that integrates findings from different data sources and epidemiological study designs.

5.9 Corrective Action in APMS represents a risk-proportionate intervention initiated in response to validated safety signals, characterized by its dynamic, tiered implementation across temporal and hierarchical dimensions. Unlike traditional passive surveillance measures, which are limited to broad recalls or static labeling changes, active surveillance systems can enable precision interventions calibrated to the severity, urgency, and specific characteristics of the affected product. These actions can be inherently integrated with

continuous monitoring data streams, allowing corrective outcomes to inform and refine ongoing signal detection and validation processes automatically. The approach ensures immediate risk mitigation while systematically enhancing the surveillance system's predictive capabilities through structured feedback loops, fulfilling regulatory requirements for adaptive risk management throughout a device's lifecycle.

6. Considerations and Recommendations for Designing and Implementing the Active Post-Market Surveillance System

As defined above, the active surveillance system for medical devices is an integrated framework designed to proactively monitor the safety and performance of medical devices in the market. It is characterized by a systematic and planned approach, leveraging diverse data sources to provide comprehensive insights. It emphasizes timely data collection and robust analytical capabilities to detect potential safety signals early. In addition, ensuring data security and privacy is paramount, and collaboration among multiple stakeholders is essential. Continuous improvement and feedback mechanisms should also be considered to optimize the monitoring process and ensure timely risk management. Therefore, the system should comprise six functionally interconnected components that form a continuous surveillance cycle:

Comprehensive Data Ecosystem
The foundation of the system lies in its ability to aggregate and standardize multi-source real-world evidence often under a regulator-led governance framework. This ecosystem may incorporate electronic health records, claims data, device registries, and patient-generated health data *etc*. Critically, all data processing should adhere to jurisdictional data protection regulations and employs privacy-by-design principles.
This ecosystem can also employ advanced data processing protocols, normalization algorithms and secure multi-party computation to ensure interoperability across disparate sources while maintaining data integrity and confidentiality. By systematically incorporating both structured and unstructured data streams, it can create a comprehensive evidence base for continuous monitoring beyond traditional spontaneous reporting systems.

Dynamic Signals Intelligence
This component integrates algorithmic screening tools with clinical expert review processes and can identify and validate potential safety signals. Machine learning models continuously scan incoming data for anomalies using predefined statistical thresholds, while maintaining human oversight through curated case review panels. The dual-layer validation approach strikes a balance between computational efficiency and clinical relevance, thereby reducing both false positives and detection delays characteristic of passive systems.

Risk Assessment Engine
As one of the cores of the system, quantitative modeling modules can transform validated signals into actionable risk assessments. Utilizing predefined decision matrices that weigh clinical severity, population exposure, and temporal patterns, the engine generates risk scores that can trigger tiered response protocols and enable dynamic updating of risk estimates as new evidence emerges, supporting data-driven risk mitigation interventions.

Corrective Action Interface
This operational bridge can convert risk assessments into concrete interventions

through predefined workflows, supporting various action modalities, for examples label updates, safety notices for medical devices, etc. The interface can maintain audit trails for all actions, synchronizing with manufacturers' quality management systems to ensure traceability and compliance.

Performance Feedback Loop

Post-intervention outcomes can be systematically tracked through UDI-enabled device identification and longitudinal outcome monitoring. The loop measures intervention effectiveness using predefined key performance indicators (e.g., time-to-action metrics) and feeds these insights back into earlier system components. This continuous evaluation cycle can allow evidence-based refinement of both surveillance parameters and risk mitigation strategies.

Adaptive Self-Optimizing Infrastructure

The system's self-optimizing architecture can utilize machine learning to continually enhance its own operations. Through reinforcement learning algorithms, it can automatically adjust detection sensitivities, refine risk models, and rebalance resource allocation based on performance data. System changes should be fully traceable and documented to ensure compliance during updates.

Figure 1 illustrates the proposed interconnected components of an APMS system. These components enable end-to-end monitoring from data acquisition to risk mitigation while maintaining system evolution in response to emerging safety patterns.

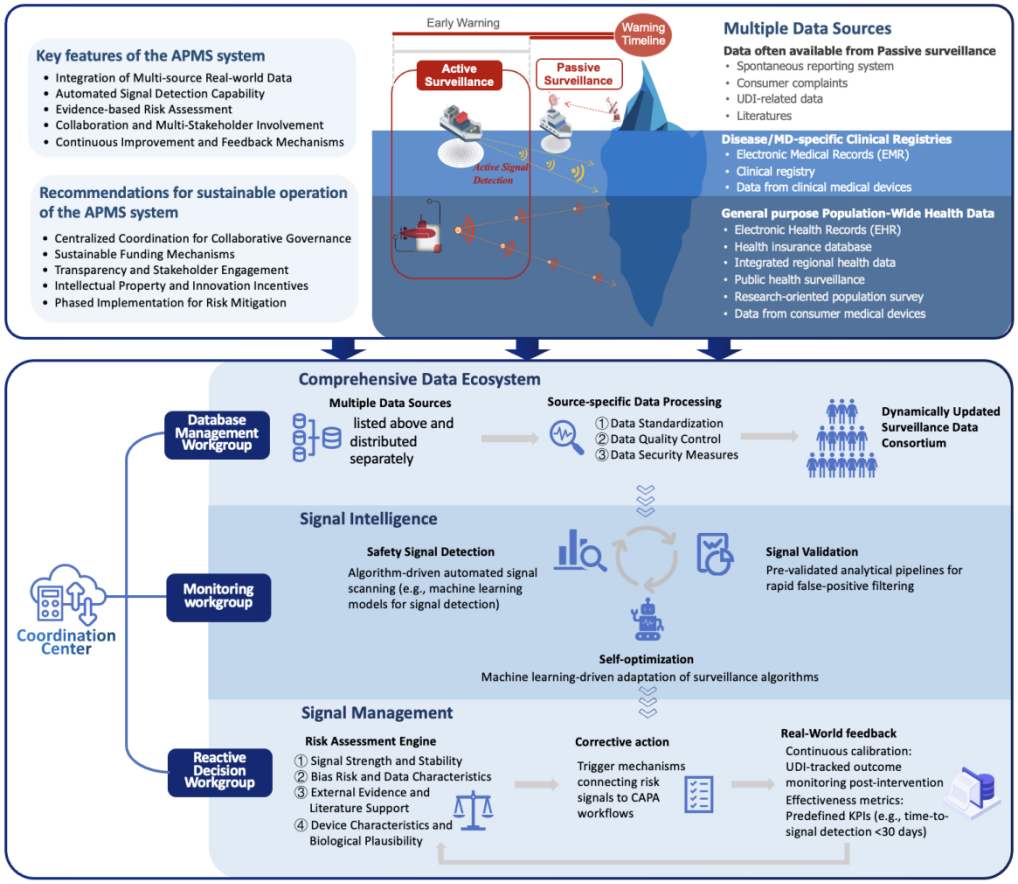

Figure 1. Proposed Conceptual Framework of an Active Post-Market Surveillance System

6.1 Key Characteristics of the APMS system

Integration of multi-source real-world data
The APMS system should be fundamentally built upon the integration of multi-source real-world data, which constitutes its foundational evidence base. This comprehensive data ecosystem should not only utilize structured passive surveillance inputs such as the spontaneous reporting system and mandatory manufacturer incident documents, but also actively incorporates clinical data from electronic health records, hospital systems, and healthcare claims databases. It can also include patient-generated health data from mobile health applications and wearable devices, combined with disease or device-specific clinical registries, creating a robust evidentiary matrix that enables cross-verification of potential safety signals through independent data streams.

Automated signal detection capability
At the operational core of the system lies its automated signal detection capability, designed to process real-world clinical data with minimal latency. Through the implementation of pre-configured analytical modules that employ statistical monitoring methods, the system can continuously scan for anomalies against predefined safety profiles. This near real-time surveillance mechanism should be designed to specifically detect emerging risks during routine clinical practice, with configurable alert thresholds triggering prioritized investigations when pre-established risk benchmarks are exceeded.

Systematic signal assessment and verification
Following detection, the system should support a systematic process of signal assessment and verification. It should apply rigorous analytical methods to synthesize evidence from across the integrated data sources. This process can confirm a signal, explore the strength of the evidence, and characterize the potential risk by evaluating criteria such as the frequency of the event, the strength of the association, and biological plausibility. This can provide a scientifically defensible foundation for subsequent risk assessment and decision-making.

Collaboration and Multi-Stakeholder Involvement
Sustainability is one of the key factors to be implemented for the system through carefully designed stakeholder engagement mechanisms grounded in regulatory oversight and proportional responsibilities. Regulators can benefit from standardized data and reports submission that reduce compliance burdens, while manufacturers can gain early risk identification capabilities that mitigate potential recall costs. (20) Critically, manufacturer participation is strictly defined by regulatory mandates; they are not responsible for operating the APMS closed-loop but for executing mandated corrective actions based on regulatory outputs. Healthcare institutions and providers should be equipped with automated reporting tools that integrate seamlessly with clinical workflows, and patient data rights should be safeguarded through the use of privacy-preserving technologies. This balanced value proposition can ensure continued participation across the medical device ecosystem.

Continuous Improvement with Feedback Loops
A defining feature of the APMS system is its closed-loop, self-optimizing architecture. Corrective action outcomes tracked through potential data sources, such as Unique Device Identification systems, can be systematically fed back into the detection algorithms, enabling continuous refinement of signal parameters. Performance metrics, including time-to-detection and accuracy rates, should undergo periodic review, creating an iterative improvement cycle that adapts to emerging safety challenges while maintaining rigorous methodological standards.

Finally, to better clarify the system characteristics, the following table provides a general comparison of implementation approaches between active and passive surveillance for the aforementioned features and processes (Table 1).

Table 1. Comparative overview of proposed selective features between active and passive surveillance approaches.

Processes	Passive Surveillance	Active Surveillance
Data Collection and Reporting	• Primarily rely on the spontaneous reporting system • Fragmented data	• Multi-source capture • Comprehensive data ecosystem
Signal Monitoring and Verification	• Manual analysis • Individual case causality assessment	• Preset algorithm library • Semi-automated verification with AI- assisted algorithms flag high-risk signals
Risk Assessment and Decision-making	• Committee review	• Evidence-based risk assessment engine for tiered and temporal decision-making
Implementation of Corrective Actions	• Paper recall notice and independent preventive actions	• Over-the-Air management and direct connection to the product lifecycle management
Effect Evaluation and Feedback	• Sampling statistics of the recall rate • Annual reported data analysis	• Real-time dashboard monitoring • Closed-loop learning mechanism: New adverse event characteristics automatically expand the monitoring algorithm rule library
Continuous Improvement of the System	• Manual SOP update • Discrete audit	• AI-driven optimization: - Automatically identify blind spots in data sources (e.g., new nursing home data sources); - Dynamically adjust the signal scanning frequency • Blockchain audit and traceability

6.2 Recommendations for the sustainable operation of the APMS system

Centralized Coordination for Collaborative Governance

The APMS system should have a dedicated coordination center to serve as the central hub for integrating surveillance activities, data management, and stakeholder collaboration. This center should facilitate seamless coordination among regulatory authorities, manufacturers, healthcare institutions, and academic researchers to prevent fragmented oversight and information silos. By standardizing processes for assessing adverse event signals and responding to them, the coordination center can ensure the implementation of scientifically validated risk mitigation measures.

Additionally, it can enable centralized decision-making to harmonize regulatory actions and optimize resource allocation. A well-structured governance framework can enhance system responsiveness and should be aligned with international best practices in post-market surveillance.

Sustainable Funding Mechanisms

To ensure long-term viability, the APMS system should establish diversified and stable funding sources. Initial government investment may be required for system development and infrastructure setup. However, sustainable operations should be supported through a combination of industry contributions, public-private partnerships, and research grants. Contingency planning for system upgrades and unexpected operational costs may also be required to mitigate financial risks. A phased funding strategy can ensure uninterrupted functionality while preventing scenarios where the system is "built but not used" or discontinued due to financial constraints.

Transparency and Stakeholder Engagement

Transparency in data sharing and public communication should help building trust and maximizing the system's societal impact. The APMS system should regularly publish aggregated safety findings and risk assessments in accessible formats to enhance regulatory transparency. Secure, anonymized data access for researchers and regulators should be facilitated to advance evidence generation and inform policy decisions. Furthermore, targeted outreach initiatives should educate healthcare providers and patients about the risks associated with medical devices and the system's role in ensuring patient safety. These measures can enhance credibility and foster proactive stakeholder engagement.

Intellectual Property and Innovation Incentives

Clear intellectual property (IP) governance should protect contributions and encourage innovation. Agreements should define ownership rights for collected data, analytical outputs, and predictive models generated through active surveillance. Conditional licensing of system-derived insights for research and development can strike a balance between open science and commercial interests, providing a framework for a mutually beneficial approach. Additionally, attribution mechanisms should recognize stakeholders, such as clinicians and manufacturers, who contribute high-quality data. A robust IP framework can foster long-term collaboration while safeguarding the interests of all participants.

Phased Implementation for Risk Mitigation

A structured, phased rollout can minimize operational risks and ensures system robustness. The initial pilot phase should test core functionalities, such as signal detection algorithms and data integration, in a controlled environment. Performance metrics, including data accuracy and response times, should be evaluated before scaling. Lessons learned during the pilot phase should inform iterative refinements, leading to a full-scale deployment aligned with global models. This approach can ensure system maturity and reliability before nationwide or even global adoption.

7. Data Sources for Active Post-Market Surveillance (APMS)

The characteristics, advantages and disadvantages of potential data sources for active post-market surveillance of medical devices are listed in the Table 2. It is critical to emphasize that the applicability and accessibility of these data sources vary significantly across jurisdictions due to differences in healthcare infrastructure, data

governance frameworks, and technological maturity. Regulators should prioritize data sources aligned with local capabilities, adopting a phased approach where necessary. Minimum viable solutions (e.g., starting with device registries or claims data before integrating electronic health records) are encouraged to ensure global feasibility. When implementing APMS systems, regulators must balance surveillance objectives with regional constraints, including privacy regulations and stakeholder readiness.

Table 2. Potential data sources for Active Post-Market Surveillance (APMS)

Data Sources	Characteristics	Advantages for APMS	Limitations for APMS
Data often available from Passive surveillance			
Spontaneous reporting system	Data on device-related adverse events reported by medical institutions etc., targeting the safety monitoring of specific devices.	Rapid detection of risk signals, reliance on statutory reporting mechanisms	High underreporting, many confounding factors, and difficulty in establishing causality
Consumer complaints	Problems with device usage are actively reported by users, allowing for the collection of feedback on performance or safety issues related to specific devices.	Direct access to subjective patient experience, and low cost of data acquisition	Highly unstructured information, low level of evidence, and underrepresentation
UDI-related data	Data linked to Unique Device Identifiers for tracking specific medical devices throughout their lifecycle.	Enables precise tracking of specific devices throughout their lifecycle for targeted issues	Limited to device identification, lacks clinical outcome data, and relies on universal UDI adoption.
Literatures	Evidence on device applications extracted from academic literature is universally applicable to post-market surveillance of various devices.	Integrates evidence from multiple studies, low cost	Poor timeliness, susceptible to publication bias
Other Potential External Data Sources			
Administrative data			
Data from digital health devices*+	Data on patient physiological indicators actively collected by wearable devices, etc., primarily for specific types of intelligent medical devices	Real-time dynamic monitoring of physiologic parameters to enhance patient engagement	Questionable accuracy of devices, selection bias (limited population)
Electronic Medical Records (EMR)+	Hospital-based electronic data recording of daily diagnostic and treatment information is widely used to collect patient data across various device applications.	Single-institution, rich in clinical detail, real-time	Closed platforms are difficult to form longitudinal data and require complex governance
Electronic Health Records (EHR)*	Regional electronic health data integrates healthcare information across multiple institutions, generally applicable to post-market surveillance of various medical devices.	Cross-organizational integration to support full-cycle patient health trajectory tracking	Severe data fragmentation and high difficulty in standardization and integration
Health insurance claims database*	Existing data recording medical expenses and service usage of insured populations, generally reflecting the clinical application and cost information of various devices	Large sample size with good coverage, complete tracking of costs, and medication use	Lack of clinical details (e.g., lab testing results) and reliance on coding accuracy
Integrated regional health data*	A system integrating medical data from multiple institutions in a region, universally covering the use of various devices in real-world healthcare settings	Multi-source data integration, reflecting the complete picture of disease in regional populations	High system interoperability requirements, huge cost of cross-organizational governance
Public health surveillance*	Systematic collection of population-level health data to monitor disease trends and device impacts across diverse medical devices	Provides population-level trends and long-term impacts across diverse devices via systematic data collection	Lacks device-specific granularity and may have reporting delays or incomplete data
Research-oriented data			
Clinical registries+	A data framework established around specific diseases, devices, or medical service models, integrating multi-source data and targeting specific devices or diseases	Proactive collection of high-quality structured data to reduce bias	High construction cost, narrow coverage of the population, and delayed data output
Research-oriented population surveys*	Prospective or retrospective data from studies designed to evaluate health outcomes related to medical devices, applicable to specific or multiple device categories based on research objectives	Offers detailed, hypothesis-driven research data with strong data quality for specific or multiple devices	High cost/time-consuming, potential selection bias, and limited generalizability to real-world populations

NOTE. *Indicates the data source is disease/device-specific clinical data, + Indicates the data source is general purpose population-wide health data.

7.1 Data security management

The APMS system shall implement comprehensive data security protocols to ensure the protection of sensitive information while maintaining functional utility. For all collected data, a rigorous de-identification process shall be applied, involving the removal or modification of both direct and indirect personal identifiers. This process shall be carefully calibrated to preserve the utility of data for research and analytical purposes while rendering the information non-attributable to specific individuals. Particular attention shall be given to maintaining the appropriate level of identifiability based on intended use - fully anonymized datasets for general research applications, while preserving necessary identifiers for case verification and causality assessment processes. For research applications, a standardized de-identification protocol shall be applied, including removal of direct identifiers, application of statistical disclosure control methods and implementation of data perturbation techniques where appropriate etc. Conversely, for case investigation and database linkage purposes, additional protective measures shall be applied to identifiable data elements, including strict access limitations, enhanced encryption standards and specialized audit trails etc. All processes involving identifiable data shall be conducted within secure, access-controlled environments with comprehensive activity monitoring.

Secure data storage systems shall be implemented following the CIA (Confidentiality, Integrity, Availability) principles. All stored data shall be protected through multiple layers of security measures, including, but not limited to, advanced encryption standards for data at rest, comprehensive access logging, and physical security controls for the storage infrastructure. The system shall employ robust data firewalls to establish granular control over all data flows, with particular emphasis on monitoring and restricting cross-system data transfers, especially those involving sensitive personal health information.

A multi-tiered access control framework shall be implemented, strictly adhering to the principle of least privilege. Access rights shall be role-based and regularly reviewed, with special consideration given to researchers requiring access to pseudonymized data. All network transmissions and database operations shall employ end-to-end encryption, with complete activity logging maintained for audit purposes. These logs shall be subject to regular, systematic review by qualified security personnel to identify potential breaches or anomalous patterns.

The operation of the APMS system shall be supported by a formal security governance program. This program includes maintaining comprehensive documentation of all security policies and procedures, from de-identification methods to incident response plans. To ensure their effectiveness, these security controls shall be subject to regular, independent risk assessments and technical audits to identify vulnerabilities and drive continuous improvement. Furthermore, a culture of security shall be fostered through mandatory and ongoing training for all personnel with access to system data, ensuring they understand and adhere to all data protection principles.

7.2 Recommendations for transitioning from passive to active surveillance

The transition from traditional passive surveillance to comprehensive active monitoring can be a significant strategic undertaking that requires a phased and systematic implementation plan. This evolution should be guided by a clear roadmap that addresses several key domains. These can include developing a federated data integration strategy, leveraging enabling technologies, establishing a robust data quality framework, and fostering multi-stakeholder collaboration. The following

recommendations outline the core principles for navigating this transition effectively, ensuring the resulting system is both technologically advanced and methodologically sound.

Technological innovation forms the cornerstone of effective active surveillance. Artificial intelligence technologies can be implemented to automate the identification of adverse events and data extraction processes, thereby significantly improving efficiency and accuracy. Concurrently, mobile health solutions can be integrated to enable direct data collection from patients, effectively reducing reporting delays and enhancing the timeliness of detection.

The transition to active surveillance should prioritize intelligent data harmonization over rigid standardization, enabling meaningful analysis of distributed, heterogeneous data sources without requiring uniform collection formats. Instead of enforcing identical data structures, the system should implement semantic interoperability frameworks to map disparate datasets to common safety surveillance concepts while preserving their original context. This approach can leverage federated querying, metadata standardization, and analytical harmonization to extract insights from decentralized data without mandating structural changes at the source. By focusing on flexible data integration rather than centralized collection, the system can reduce implementation barriers for healthcare providers and registries while maintaining data richness. International collaboration can also develop open-source harmonization tools, shared ontologies, and governance models to ensure interoperability across jurisdictions. This distributed strategy can strike a balance between data utility and real-world feasibility, enabling the APMS system to maximize coverage and responsiveness while respecting existing data ecosystems.

A robust, multi-layered security framework should support this transition. Advanced privacy-preserving techniques should be employed to enable secure data sharing. Comprehensive security management systems should combine technical safeguards, such as end-to-end encryption and granular access controls, with organizational measures, including rigorous personnel training and regular security audits.

Data quality management requires particular attention during this transition. A standardized quality assessment framework should be implemented, featuring automated monitoring tools for quality evaluation and correction throughout the entire data lifecycle, from collection and storage to processing and utilization. Quality control mechanisms should be tailored to different data acquisition methods, with regular audits and targeted training programs established to minimize human errors. Audit frequencies should be adapted to regional requirements and system maturity levels.

The transition process should incorporate a multidimensional, continuous improvement approach to ensuring data quality. This can include establishing feedback loops for quality enhancement, implementing periodic system evaluations, and maintaining ongoing staff training programs to ensure continuous improvement. A tiered quality control structure should be implemented, combining automated checks with human oversight at appropriate intervals to provide long-term data reliability while accommodating evolving surveillance needs and technological advancements.

In summary, a successful transition to active surveillance hinges on a balanced and comprehensive strategy. By following a clear roadmap that adopts a federated data approach, leverages enabling technologies, and is underpinned by robust frameworks for data quality and security, stakeholders can build an advanced system. This strategic approach can ensure the resulting active surveillance system delivers timely

and reliable evidence for decision-making, ultimately enhancing patient safety while maintaining the trust of all participants and ensuring regulatory compliance.

Bibliography

[1] Regulation (EU) 2017/745 Medical Device Regulation (EU MDR)
[2] European Commission (2013). Guidance document on Market surveillance: Guidelines on a Medical Devices Vigilance System (MEDDEV 2.12/1 rev.8)
[3] World Health Organization (WHO) (2020), Guidance for post-market surveillance and market surveillance of medical devices, including in vitro diagnostics.
[4] Study group 2 of Global Harmonization Task Force (2006). Post Market Surveillance: Global Guidance for Adverse Event Reporting for Medical Devices. (GHTF/SG2/N54R8:2006)
[5] Adverse Event Terminology Working Group of International Medical Device Regulators Forum (IMDRF) (2024), Common Data Set for Adverse Event Data Exchange Between IMDRF Regulators. (IMDRF/AET WG/N85 FINAL: 2024)
[6] Patient Registries Working Group of International Medical Device Regulators Forum (IMDRF) (2017), Methodological principles in the use of international medical device registry data authoring group: IMDRF patient registries working group. (IMDRF/Registry WG N42 FINAL: 2017)
[7] ISO 14971:2019 Medical devices - Application of risk management to medical devices.
[8] ISO 13485-2016 Medical devices - Quality management systems - Requirements for regulatory purposes.
[9] ISO 8000-114:2024 Data quality - Part 114: Master data.
[10] U.S. Food and Drug Administration (FDA) (2024), Best Practices for FDA Staff in the Postmarketing Safety Surveillance of Human Drug and Biological Products.
[11] U.S. Government Accountability Office (GAO) (2024), Medical Devices: FDA Has Begun Building an Active Postmarket Surveillance System.