Medical XR Regulations Global Landscape

A comprehensive comparison of regulatory frameworks affecting immersive medical technologies across major global markets, essential for developers, healthcare providers, and policymakers navigating this emerging space.

Regulations are evolving rapidly - visit medical.xrsi.org for the most current information

	USA	UK	EUROPE	INDIA	CANADA
Areas of Growth	FDA MedXR policy development in progress; Consumer health XR gathers sensitive info not covered by FTC; Variable policies on data privacy by state.	Lack of clarity on how to categorize XR hardware and software as Medical Devices or SaMDs; MHRA to introduce new regulations for medical devices in 2025.	Harmony of approach across member states; standardization of digital health reform enforcement policies.	Data protection laws with specific focus on digital health information in progress; Stricter enforcement and emphasis on regulatory compliance from businesses.	Health Canada's Action Plan to strengthen medical device and digital health regulation is in progress; Harmonization across Canadian jurisdictions to ensure consistent oversight and public safety.
Major Risks	Regulatory revisions and lack of alignment between agencies negatively impacts ability to comply; Obfiscation of regulation commonly practiced by classification of XR applications as wellness.	Lack of guidance from regulatory bodies on XR technologies; Regulatory complexities poses major risks for effective compliance to protect patients	Separate governing agencies and standards by nation in a region that is trying to work cohesively, reducing interoperability; businesses may selectively operate where enforcement is more lenient.	Fragmented regulatory framework for XR and digital healthcare; Ambiguity surrounding data transfers, surveillence, and censorship creates risks with respect to data privacy and security.	Lack of clarity on health application regulation, various regulatory changes to be implemented in quick succession; Hampering compliance efforts for businesses, especially those operating in multiple jurisdictions due to lack of harmony.
Consumer Privacy Norms	• Federal Trade Commission (FTC): Consumer protection authority that regulates privacy and advertising practices in emerging technologies. • Department of Health and Human Services (HHS): Oversees HIPAA compliance and determines whether data collected by health-related immersive apps constitutes "protected health information."	• Information Commissioner's Office (ICO): Primary regulatory body responsible for enforcing data protection and privacy laws in the UK. • ICO has identified immersive technologies as a significant area of concern and has issued guidelines for organizations operating in this space.	• European Data Protection Board (EDPB): Ensures consistent application of data protection rules across the EU, including for immersive technologies. • EDPB provides guidelines on interpreting the General Data Protection Regulation (GDPR) as it applies to new technologies. • Each EU member state has its own data protection authority responsible for enforcing privacy regulations within their jurisdiction.	• Ministry of Electronics and Information Technology (MeitY): The primary government agency responsible for formulating policies related to digital technologies and data protection. • Personal Data Protection Board: A new regulatory body proposed under the Digital Personal Data Protection Act to investigate data breaches and handle consumer inquiries about personal data processing. • Reserve Bank of India (RBI): Regulates financial data and transactions, which may become relevant as AR/VR technologies are integrated into fintech applications.	• Office of the Privacy Commissioner of Canada (OPC): Key regulatory body for privacy protection. • Innovation, Science and Economic Development Canada (ISED): Key regulatory body for technology policy. • Digital Charter Implementation Act, 2022: Legislation aimed at strengthening Canada's private sector privacy law, increasing individual control, enhancing protections for minors, and introducing significant fines for non-compliance.
Medical Record/ PHI Policy	• Health Insurance Portability and Accountability Act (HIPAA): Defines "protected health information" (PHI) as any information about health status, provision of health care, or payment for health care that can be linked to an individual. • Department of Health and Human Services (HHS): Interprets HIPAA regulations and determines if data collected by health-related immersive technologies constitutes protected information.	• UK General Data Protection Regulation (UK GDPR): Primary legislation governing the protection of health information. • Data Protection Act 2018: Key legislation for data protection that complements the UK GDPR. • Caldicott Principles: Guidelines for handling sensitive patient data that health workers must follow. • Key regulatory agencies: Information Commissioner's Office (ICO), NHS England, Department of Health and Social Care.	• General Data Protection Regulation (GDPR): Primary legislation governing the protection of health information, classifying health data as "special category data" with heightened protection. • National laws: Supplement the GDPR in each member state. • European Health Data Space (EHDS): Proposed initiative to create a common space for sharing health data across the EU. • Data Protection Authorities: Each EU member state has its own authority responsible for enforcing these regulations.	• Information Technology Act, 2000 (IT Act): Provides the basic framework for electronic governance and data protection. • Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules): Offer some protection for sensitive personal data, including medical records. • Health Data Management Policy (2020, revised in 2022): Guidelines for managing health data. • Digital Personal Data Protection Act: Refines India's approach to health data protection.	• Personal Information Protection and Electronic Documents Act (PIPEDA): Primary federal law governing the collection, use, and disclosure of personal information in commercial activities. • Provincial health information privacy laws: Many provinces have enacted their own laws that take precedence over PIPEDA for health information within their jurisdictions. • Office of the Privacy Commissioner of Canada: Oversees compliance with PIPEDA. • Provincial privacy commissioners: Oversee compliance with their respective provincial privacy laws.
Medical Device Regulation	• Food and Drug Administration (FDA): Primary regulatory body overseeing medical devices through its Center for Devices and Radiological Health (CDRH). • Medical device classification: Devices are categorized into three risk-based classes to determine regulatory requirements. • Quality Management System Regulation (QMSR) Final Rule: Harmonizes FDA regulations with ISO 13485:2016 standards. • FDA inspections: Required for medical device compliance, beyond ISO certification.	• Medicines and Healthcare products Regulatory Agency (MHRA): Responsible for regulating medical devices in the UK, including software and hardware. • Northern Ireland: Has different regulations that align more closely with EU standards.	• Medical Device Regulation (MDR): Governed by Regulation (EU) 2017/745, implemented on May 26, 2021. • Replaces previous directives: Superseded the Medical Device Directive (MDD) and Active Implantable Medical Device Directive (AIMD).	• Medical Devices Rules, 2017: Primary regulation for medical devices, amended in 2020. • Central Drugs Standard Control Organization (CDSCO): Primary regulatory body for medical devices, operating under the Ministry of Health and Family Welfare. • The Drugs and Cosmetics Act of 1940: All medical devices must be registered under this act as of April 1, 2020.	• Medical Devices Regulations (MDR): Primary regulation governing medical devices under the Food and Drugs Act. • Health Canada: Primary agency responsible for regulating medical devices. • Classification system: Medical devices are categorized into four risk-based classes.
Digital Health Regulation/ Guidance	• FDA's Digital Health Center of Excellence: Primary oversight body for digital health regulation. • Digital Health Innovation Action Plan: FDA's framework for regulating software as a medical device (SaMD). • FDA Pre-Cert Program: Pilot program for streamlining regulatory oversight of digital health companies.	• Medicines and Healthcare products Regulatory Agency (MHRA): Key regulatory body for medical devices including digital health technologies. • National Institute for Health and Care Excellence (NICE): Provides guidance on digital health technologies. • Care Quality Commission (CQC): Regulates health and social care services, including those using digital technologies. • Health Research Authority (HRA): Oversees health research involving digital technologies.	• Digital Services Act (DSA): Regulates digital platforms and services, including health-related applications. • General Data Protection Regulation (GDPR): Governs data protection and privacy for all digital health technologies. • European Health Data Space (EHDS): Initiative for sharing health data across the EU for research and policy-making. • European Health Technology Assessment Regulation (HTAR): Framework for assessing health technologies. • European Digital Health Technology Assessment (EDiHTA): Specific initiative for evaluating digital health technologies.	• Ministry of Health and Family Welfare (MoHFW): Key regulatory body for health policies. • Central Drugs Standard Control Organization (CDSCO): Regulatory body for medical devices and digital health technologies. • Digital Personal Data Protection Act, 2023: India's first comprehensive data protection law. • Upcoming legislation: Government is developing specific laws on digital healthcare, information security, and personal data protection.	• Digital Health Review Division: Established in 2018 within Health Canada's Medical Devices Bureau to regulate digital health technologies. • Digital Charter Implementation Act: Introduced in 2022 to strengthen privacy protection and regulate AI. • Connected Care for Canadians Act: Introduced in June 2024 to enable secure access to personal health information. • Pan-Canadian Interoperability Roadmap: Initiative to set standards for connected care and secure information sharing.
Medical XR Regulation/ Guidance	• No comprehensive framework specifically for Medical XR regulation exists. • FDA applies existing medical device and software regulations to XR technologies. • FDA's Digital Health Center of Excellence provides guidance for innovative technologies including XR.	• No comprehensive policy specifically for Medical XR regulation exists. • XR medical applications are regulated under existing medical device and software frameworks by the MHRA. • NICE provides evaluation guidance for digital health technologies that would include XR applications.	• Medical XR devices categorized under Software as Medical Device (SaMD) regulations. • XR devices classified into risk categories: Class I, IIa, IIb, and III. • CE (Conformité Européenne) marking required before placing XR devices on the EU market.	• No explicit provisions for XR technologies in existing regulations. • Medical XR devices regulated under Medical Devices (Amendment) Rules, 2020. • Digital Personal Data Protection Act (2023): Protects health data gathered through XR technologies. • Licensing requirement: Implemented for Class C and D Medical Devices as of October 2023. • National Medical Device Policy (May 2023): Proposes a 'Single Window Clearance System' for licensing. • Ayushman Bharat Digital Mission (ABDM) data management policy: Emphasizes data security measures for digital health technologies.	• Health Canada: Primary federal agency responsible for regulating medical devices, including XR technologies. • Medical Device Establishment Licence (MDEL): Required for manufacturing, importing, or distributing medical XR devices. • Action Plan: Health Canada's initiative to strengthen medical device regulation, which would include XR technologies. • No specific XR regulatory framework: XR technologies are regulated under general medical device and software regulations.

Contact: info@xrsi.org | www.xrsi.org

Medical XR Regulations Global Landscape

A comprehensive comparison of regulatory frameworks affecting immersive medical technologies across major global markets, essential for developers, healthcare providers, and policymakers navigating this emerging space.

Regulations are evolving rapidly - visit medical.xrsi.org for the most current information

	USA	UK	EUROPE	INDIA	CANADA
Consumer Privacy Norms	• Federal Trade Commission (FTC): Consumer protection authority that regulates privacy and advertising practices in emerging technologies. • Department of Health and Human Services (HHS): Oversees HIPAA compliance and determines whether data collected by health-related immersive apps constitutes "protected health information."	• Information Commissioner's Office (ICO): Primary regulatory body responsible for enforcing data protection and privacy laws in the UK. • ICO has identified immersive technologies as a significant area of concern and has issued guidelines for organizations operating in this space.	• European Data Protection Board (EDPB): Ensures consistent application of data protection rules across the EU, including for immersive technologies. • EDPB provides guidelines on interpreting the General Data Protection Regulation (GDPR) as it applies to new technologies. • Each EU member state has its own data protection authority responsible for enforcing privacy regulations within their jurisdiction.	• Ministry of Electronics and Information Technology (MeitY): The primary government agency responsible for formulating policies related to digital technologies and data protection. • Personal Data Protection Board: A new regulatory body proposed under the Digital Personal Data Protection Act to investigate data breaches and handle consumer inquiries about personal data processing. • Reserve Bank of India (RBI): Regulates financial data and transactions, which may become relevant as AR/VR technologies are integrated into fintech applications.	• Office of the Privacy Commissioner of Canada (OPC): Key regulatory body for privacy protection. • Innovation, Science and Economic Development Canada (ISED): Key regulatory body for technology policy. • Digital Charter Implementation Act, 2022: Legislation aimed at strengthening Canada's private sector privacy law, increasing individual control, enhancing protections for minors, and introducing significant fines for non-compliance.
Medical Record/ PHI Policy	• Health Insurance Portability and Accountability Act (HIPAA): Defines "protected health information" (PHI) as any information about health status, provision of health care, or payment for health care that can be linked to an individual. • Department of Health and Human Services (HHS): Interprets HIPAA regulations and determines if data collected by health-related immersive technologies constitutes protected information.	• UK General Data Protection Regulation (UK GDPR): Primary legislation governing the protection of health information. • Data Protection Act 2018: Key legislation for data protection that complements the UK GDPR. • Caldicott Principles: Guidelines for handling sensitive patient data that health workers must follow. • Key regulatory agencies: Information Commissioner's Office (ICO), NHS England, Department of Health and Social Care.	• General Data Protection Regulation (GDPR): Primary legislation governing the protection of health information, classifying health data as "special category data" with heightened protection. • National laws: Supplement the GDPR in each member state. • European Health Data Space (EHDS): Proposed initiative to create a common space for sharing health data across the EU. • Data Protection Authorities: Each EU member state has its own authority responsible for enforcing these regulations.	• Information Technology Act, 2000 (IT Act): Provides the basic framework for electronic governance and data protection. • Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules): Offer some protection for sensitive personal data, including medical records. • Health Data Management Policy (2020, revised in 2022): Guidelines for managing health data. • Digital Personal Data Protection Act: Refines India's approach to health data protection.	• Personal Information Protection and Electronic Documents Act (PIPEDA): Primary federal law governing the collection, use, and disclosure of personal information in commercial activities. • Provincial health information privacy laws: Many provinces have enacted their own laws that take precedence over PIPEDA for health information within their jurisdictions. • Office of the Privacy Commissioner of Canada: Oversees compliance with PIPEDA. • Provincial privacy commissioners: Oversee compliance with their respective provincial privacy laws.
Medical Device Regulation	• Food and Drug Administration (FDA): Primary regulatory body overseeing medical devices through its Center for Devices and Radiological Health (CDRH). • Medical device classification: Devices are categorized into three risk-based classes to determine regulatory requirements. • Quality Management System Regulation (QMSR) Final Rule: Harmonizes FDA regulations with ISO 13485:2016 standards. • FDA inspections: Required for medical device compliance, beyond ISO certification.	• Medicines and Healthcare products Regulatory Agency (MHRA): Responsible for regulating medical devices in the UK, including software and hardware. • Northern Ireland: Has different regulations that align more closely with EU standards.	• Medical Device Regulation (MDR): Governed by Regulation (EU) 2017/745, implemented on May 26, 2021. • Replaces previous directives: Superseded the Medical Device Directive (MDD) and Active Implantable Medical Device Directive (AIMD).	• Medical Devices Rules, 2017: Primary regulation for medical devices, amended in 2020. • Central Drugs Standard Control Organization (CDSCO): Primary regulatory body for medical devices, operating under the Ministry of Health and Family Welfare. • The Drugs and Cosmetics Act of 1940: All medical devices must be registered under this act as of April 1, 2020.	• Medical Devices Regulations (MDR): Primary regulation governing medical devices under the Food and Drugs Act. • Health Canada: Primary agency responsible for regulating medical devices. • Classification system: Medical devices are categorized into four risk-based classes.
Digital Health Regulation/ Guidance	• FDA's Digital Health Center of Excellence: Primary oversight body for digital health regulation. • Digital Health Innovation Action Plan: FDA's framework for regulating software as a medical device (SaMD). • FDA Pre-Cert Program: Pilot program for streamlining regulatory oversight of digital health companies.	• Medicines and Healthcare products Regulatory Agency (MHRA): Key regulatory body for medical devices including digital health technologies. • National Institute for Health and Care Excellence (NICE): Provides guidance on digital health technologies. • Care Quality Commission (CQC): Regulates health and social care services, including those using digital technologies. • Health Research Authority (HRA): Oversees health research involving digital technologies.	• Digital Services Act (DSA): Regulates digital platforms and services, including health-related applications. • General Data Protection Regulation (GDPR): Governs data protection and privacy for all digital health technologies. • European Health Data Space (EHDS): Initiative for sharing health data across the EU for research and policy-making. • European Health Technology Assessment Regulation (HTAR): Framework for assessing health technologies. • European Digital Health Technology Assessment (EDiHTA): Specific initiative for evaluating digital health technologies.	• Ministry of Health and Family Welfare (MoHFW): Key regulatory body for health policies. • Central Drugs Standard Control Organization (CDSCO): Regulatory body for medical devices and digital health technologies. • Digital Personal Data Protection Act, 2023: India's first comprehensive data protection law. • Upcoming legislation: Government is developing specific laws on digital healthcare, information security, and personal data protection.	• Digital Health Review Division: Established in 2018 within Health Canada's Medical Devices Bureau to regulate digital health technologies. • Digital Charter Implementation Act: Introduced in 2022 to strengthen privacy protection and regulate AI. • Connected Care for Canadians Act: Introduced in June 2024 to enable secure access to personal health information. • Pan-Canadian Interoperability Roadmap: Initiative to set standards for connected care and secure information sharing.
Medical XR Regulation/ Guidance	• No comprehensive framework specifically for Medical XR regulation exists. • FDA applies existing medical device and software regulations to XR technologies. • FDA's Digital Health Center of Excellence provides guidance for innovative technologies including XR.	• No comprehensive policy specifically for Medical XR regulation exists. • XR medical applications are regulated under existing medical device and software frameworks by the MHRA. • NICE provides evaluation guidance for digital health technologies that would include XR applications.	• Medical XR devices categorized under Software as Medical Device (SaMD) regulations. • XR devices classified into risk categories: Class I, IIa, IIb, and III. • CE (Conformité Européenne) marking required before placing XR devices on the EU market.	• No explicit provisions for XR technologies in existing regulations. • Medical XR devices regulated under Medical Devices (Amendment) Rules, 2020. • Digital Personal Data Protection Act (2023): Protects health data gathered through XR technologies. • Licensing requirement: Implemented for Class C and D Medical Devices as of October 2023. • National Medical Device Policy (May 2023): Proposes a 'Single Window Clearance System' for licensing. • Ayushman Bharat Digital Mission (ABDM) data management policy: Emphasizes data security measures for digital health technologies.	• Health Canada: Primary federal agency responsible for regulating medical devices, including XR technologies. • Medical Device Establishment Licence (MDEL): Required for manufacturing, importing, or distributing medical XR devices. • Action Plan: Health Canada's initiative to strengthen medical device regulation, which would include XR technologies. • No specific XR regulatory framework: XR technologies are regulated under general medical device and software regulations.
Unmet Needs	The FDA has recognized the need for additional statutory authority in certain areas, alignment with international regulatory expectations, consistent application of digital health technology policies, and a reimagined regulatory paradigm tailored for digital health technologies. There is no specific comprehensive framework in the US solely for Medical XR regulation.	The MHRA needs to reform the UK Med Device regulations to align with international best practices. They intend to broadly mirror the EU model in their approach and introduce new regulations in 2025. Similar to the US, the UK has no comprehensive policy specific to Medical XR regulation. However, they intend to apply relevant aspects of the existing landscape to Medical XR. There is a need for clarity on how to categorize XR hardware and software as Med Devices or Software as a Medical Device (SaMD). There is no specific regulatory guidance on XR technologies from NICE or MHRA.	While the GDPR provides a common framework, member states have flexibility in implementing specific rules for health data. There is a need for a space for the sharing of health data across the EU for research/policy-making while maintaining strong privacy protection. EHDS has been proposed. Each member state is responsible for enforcing regulations - there is a need for some kind of standardized enforcement to harmonize approaches across the member states.	The current legal/regulatory framework governing digital health in India is fragmented. There is ambiguity surrounding data transfers, surveillance, and censorship; there is no explicit provision for Medical XR technology, digital health or telemedicine. Only partial aspects of digital health are covered. It is difficult to apply fragmented privacy laws to fully virtual spaces or assets. Given the rapid advancement of XR technologies in healthcare, it's likely that India will need to develop more specific guidelines or regulations for Medical XR applications in the future. Currently, these technologies would be regulated under the broader umbrella of medical devices and digital health, with potential gaps in addressing their unique characteristics.	There is a need for an Action Plan (which is currently developed and in the works) to improve how devices reach the market, strengthen monitoring and follow-up protocol for the devices already in use, and provide more information to citizens about the devices being used. The current framework lacks specificity for mHealth applications and clarity on which apps require regulation.
Major Risks	Legislation is currently more reactive than proactive. Large, complex regulatory systems, along with the resistance to introducing new regulatory categories - can cause a failure to capture potential harms. The need for collaboration between policymakers, healthcare providers, technology developers, and regulatory bodies may cause a delay in policy implementation. The current policy allows users to submit reports of tech malfunction or adverse responses online - however, slow enforcement of policies and lack of Medical XR specific policies can hamper regulation. Finally, businesses and innovators will find it difficult to conform to regulations that aren't specifically designed with Medical XR tech in mind - hampering innovation or slowing the reach to the market as well.	Improper navigation and difficulty in complying with existing regulations when implementing XR technologies is a major risk for business and providers/patients. Similar to the US, legisation is in a perpetual game of catch up, and the complex regulatory landscape right now can hamper the ability of business to comply. Introducing various frameworks at once can make it cumbersome for businesses to comply, and deter innovation in Medical Technology.	There are separate governing agencies and standards by nation in a region that is trying to work cohesively. This reduces interoperability and standardization of digital health solutions. Businesses will thus have to comply not only with the GDPR framework, but also the individual regulations of each member state. This is difficult and could hamper innovation. If XR use in medicine is not regulated to keep up with the revolution, there are risks for future misunderstandings and criticalities, especially for high-risk situations.	There are provisions within the regulatory framework that allow the government to exempt its own agencies from compliance with data protection laws. This can hamper trust in the legislative body and allow for egregious misuse of power. Biometric and behavioral data is being collected through XR devices without adequate safeguards. This is a major risk to data privacy and security.India is also vulnerable to cyberattacks and data breaches, as evidenced by the AIIMS Incident.	There is a need for harmonized standards across jurisdictions to ensure consistent oversight and public safety in radiation protection. A lot of reforms and plans are underway but there is no certainty as to whether these regulations will be implemented by 2025. The governing agencies might be too slow to catch up with the technological landscape. At the same time, the introduction of many distinct regulatory frameworks in quick succession would hamper the ability of the businesses to actually comply with all of them and release products in the market.

Contact: info@xrsi.org
www.xrsi.org