

# Enforcing Software and AI as Medical Devices: Expert Witness Insights on Civil Lawsuits, Regulation, and Legal Liability Pathways

---

Rudolf Wagner<sup>1</sup>

---

As an expert witness to German courts (Landgerichte, Oberlandesgerichte) and federal courts for Medical Devices and IVDs the number of expert statements has constantly increased, especially for Software and AI in Healthcare and focusing on their Medical Device classification.

The paper also examines how competition and insurers may respond to claims arising from the use of improperly classified software, artificial intelligence including Large Language Models (LLMs) with denial of coverage, increased premiums, and subrogation actions against hospitals or AI developers. Regulatory challenges are discussed in light of Software as a Medical Device (SaMD) frameworks, highlighting the effective and valid regulations to classify the risk of Software and AI when used in Healthcare, which are enforced today although the dynamic and evolving nature of AI systems.

This paper concludes the used regulatory and legal pathways used in cases with expert witness statements between competitors or by competitors to file a lawsuit against a competitor with incorrect classification based on experience and draws the parallels to the US FDA regulation. Beyond it demonstrates that authority driven enforcement of existing regulation is transferred to courts acting on behalf of the authority driven by compliant legal manufacturers.

---

## 1. Introduction

The development of Software as a Medical Device (SaMD) and AI as SaMD has transformed modern healthcare, providing sophisticated diagnostic and therapeutic support independent of traditional hardware. SaMD includes software that performs medical functions such as diagnosis, monitoring, or treatment guidance. AI-based SaMD leverages advanced algorithms to offer automated, data-driven medical insights.

However, the rapid adoption of these technologies has raised significant concerns regarding their classification, regulation, and compliance under both EU MDR in Europe and FDA regulations in the United States. These regulatory frameworks are designed to ensure the safety and effectiveness of SaMD in medical practice. Despite this, passive enforcement by regulatory authorities and regulatory loopholes have allowed some non-compliant products to succeed in the market, undermining patient safety and competitive fairness.

This paper provides an overview of the existing regulations for SaMD and AI as SaMD in Germany and the United States, discusses the regulatory obligations for manufacturers, outlines potential legal breaches due to misclassification, and examines how passive enforcement contributes to the persistence of non-compliant devices in the market. The paper concludes with an analysis of the current state of regulatory changes and the challenges of reform in this rapidly evolving technological field.

## 2. Existing Regulations for SaMD and AI as SaMD in Germany and the United States

### 2.1 EU Medical Device Regulation (EU MDR) and MDCG 2019-11

The EU Medical Device Regulation (MDR 2017/745) sets comprehensive standards for the approval and post-market surveillance of SaMD. Software that fulfills a medical purpose, such as providing diagnostic or therapeutic guidance, is classified as a medical device and must undergo a conformity assessment based on its risk classification.

---

<sup>1</sup> Expert Witness Medical Devices and IVDs, ADHOCON, Germany, [expert.adhocon.com](mailto:expert.adhocon.com), [info@adhocon.com](mailto:info@adhocon.com)

*MDCG 2019-11 Guidance*

The Medical Device Coordination Group (MDCG) provides clarification through MDCG 2019-11, which explains how SaMD should be classified under the MDR. The classification depends on the software's intended use and the associated risks.

*The EU MDR classifies SaMD into four classes:*

- Class I: Low-risk devices, including administrative software with minimal patient impact.
- Class IIa: Moderate-risk devices that support clinical decisions for non-critical conditions.
- Class IIb: Higher-risk software used in critical medical situations or conditions requiring active monitoring.
- Class III: High-risk devices that control or influence treatment for life-threatening conditions.

*Classification Table: EU MDR for SaMD*

| Class     | Example SaMD Functions                                         | Risk Level | Regulatory Requirements                              |
|-----------|----------------------------------------------------------------|------------|------------------------------------------------------|
| Class I   | Administrative and monitoring software                         | Low        | Self-certification, basic oversight                  |
| Class IIa | Diagnostic support for non-critical conditions                 | Moderate   | Notified body assessment                             |
| Class IIb | Monitoring software for critical conditions                    | High       | Rigorous conformity assessments, clinical evaluation |
| Class III | Autonomous diagnostic or therapeutic systems for critical care | Highest    | Strict oversight, extensive clinical validation      |

## 2.2 US FDA SaMD Rules

The US FDA regulates SaMD under the Federal Food, Drug, and Cosmetic Act (FDCA), classifying it based on its intended use and potential risks to patient health. The FDA's approach is also risk-based, with SaMD products assigned to one of three classes.

### FDA Risk Classification and Regulatory Pathways

- Class I: Low-risk devices, subject to general controls and usually exempt from premarket notification (510(k)).
- Class II: Moderate-risk devices that require 510(k) clearance. Manufacturers must demonstrate substantial equivalence to a previously approved device.
- Class III: High-risk devices that require Premarket Approval (PMA), which involves rigorous clinical testing and submission of safety and efficacy data.

The FDA's Quality System Regulation (21 CFR Part 820) mandates strict design controls, risk management, and quality assurance for SaMD products, ensuring they are safe and effective throughout their lifecycle. The Digital Health Innovation Action Plan further addresses AI-based software, acknowledging the need for adaptive frameworks to regulate AI/ML-based SaMD.

*Classification Table: US FDA for SaMD*

| Class     | Example SaMD Functions                     | Risk Level | Regulatory Requirements                                 |
|-----------|--------------------------------------------|------------|---------------------------------------------------------|
| Class I   | Administrative tools                       | Low        | General controls, exempt from 510(k)                    |
| Class II  | Diagnostic support (non-critical)          | Moderate   | 510(k) clearance, demonstrating substantial equivalence |
| Class III | AI for life-threatening diagnostic support | High       | PMA, requiring clinical data and premarket validation   |

### 2.3 IMDRF (International Medical Device Regulators Forum)

The IMDRF SaMD Working Group established a globally recognized framework that harmonizes SaMD classification standards, including those for AI. The IMDRF framework evaluates SaMD based on:

1. The significance of the software's role in clinical decision-making.
2. The criticality of the healthcare situation being addressed.

For instance:

- Class A (Low): Software that supports non-critical information (e.g., wellness monitoring).
- Class B (Moderate): SaMD that informs decisions for non-critical medical conditions.
- Class C (High): Systems that influence decisions for serious conditions.
- Class D (Highest): Software that provides critical guidance in life-threatening situations.

This system helps determine the level of regulatory oversight required based on the intended use and risk impact of the SaMD.

## 3. Regulatory Obligations for SaMD and AI as SaMD

### 3.1 Pre-market Obligations

- EU MDR: For Class IIa and above, manufacturers must complete clinical evaluations, perform risk assessments, and obtain approval from a notified body.
- US FDA: Class II and III devices require 510(k) clearance or PMA approval, involving clinical testing and risk assessments.

### 3.2 Post-market Surveillance

- EU MDR: Obligates manufacturers to conduct post-market surveillance, including vigilance reporting, and continuous performance monitoring through Periodic Safety Update Reports (PSURs).
- US FDA: The Quality System Regulation requires SaMD developers to maintain post-market compliance, including adverse event reporting and Corrective and Preventive Actions (CAPA).

### 3.3 Risk Classification Obligations

| Class     | Obligations                                                              |
|-----------|--------------------------------------------------------------------------|
| Class I   | Self-certification, minimal monitoring                                   |
| Class IIa | Clinical evaluation, notified body assessment, regular reporting         |
| Class IIb | Stringent conformity assessments, post-market updates                    |
| Class III | Comprehensive trials, notified body or PMA approval, strict surveillance |

## 4. Legal Framework: Germany

### 4.1 Medical Device Regulation (MDR and MPDG)

Germany, as part of the European Union, adheres to the Medical Device Regulation (EU MDR 2017/745), which governs the classification, approval, and use of medical devices, including SaMD and AI. The Medizinprodukteführungsgesetz (MPDG) implements EU MDR regulations into German law, ensuring that all devices, including software, are subjected to rigorous safety and performance standards. Under the MDR, any software that provides diagnostic or therapeutic recommendations qualifies as a medical device and must undergo Notified Body scrutiny to ensure compliance.

If a medical professional or healthcare provider uses an LLM for diagnostic or treatment decisions without the software being certified as a Class II medical device, this would be a clear violation of EU MDR and MPDG. Legal consequences could include product recalls, administrative fines, and civil lawsuits. Additionally, there could be criminal liability if patient harm results from the use of uncertified software.

## **4.2 Criminal and Civil Liabilities in Germany**

Germany's legal system provides for both civil and criminal penalties in cases where patient harm results from non-compliance with medical device regulations.

### **4.2.1 Bodily Harm (Körperverletzung) and Negligent Bodily Harm**

If an improperly certified device (such as an LLM used in medical decision-making) causes harm, the responsible parties could be held liable for Körperverletzung (bodily harm) under § 223 StGB of the German Criminal Code. This applies if the harm was intentional or reckless. If the harm was the result of negligence, § 229 StGB covers negligent bodily harm, which could be invoked if the improper use of an LLM leads to patient injury due to failure to comply with regulatory standards.

For example, if a doctor uses LLM to suggest a treatment and the patient suffers harm due to incorrect advice, the doctor and potentially the hospital could face criminal charges for negligence.

### **4.2.2 Unfair Competition and Product Liability**

Under German civil law, companies or individuals that falsely represent the classification of medical devices, including AI systems like LLMs, could face significant liability under unfair competition laws. The Gesetz gegen den unlauteren Wettbewerb (UWG), or Act Against Unfair Competition, is the primary legal framework regulating unfair business practices in Germany. If a competitor, such as a hospital or software provider, improperly uses an unapproved AI system for diagnostic purposes, they could be sued by another party (such as a properly regulated competitor) for unfair competitive practices. The improper classification of a medical device as lower-risk (such as self-certification as Class I rather than Class II or III) is a violation of these laws.

Additionally, under § 8 UWG, any party whose interests are harmed by unfair practices, including misrepresentation of a medical device, can bring an action for injunctive relief. This would prevent the continued sale or use of the improperly classified AI system, potentially leading to market withdrawal or fines.

For product liability, the Produkthaftungsgesetz (ProdHaftG) applies in cases where defective products, including medical devices, cause harm. In the case of LLMs, if the software produces an incorrect diagnosis or treatment suggestion that leads to patient harm, the manufacturer, distributor, and potentially the hospital could be liable for damages under this law. The ProdHaftG establishes strict liability for manufacturers of defective products, meaning that the injured party does not need to prove fault, only that the product was defective and caused the injury.

### **4.2.3 Failure to Render Assistance (Unterlassene Hilfeleistung)**

Another potential area of liability in Germany is "Unterlassene Hilfeleistung" or failure to render assistance, under § 323c StGB. While this law is traditionally applied to situations where individuals fail to provide necessary assistance in emergencies, it could be extended to medical professionals or institutions that fail to take appropriate action when they become aware that an improperly certified or defective medical device (including software) is being used.

If a doctor or hospital is aware that an LLM is being used in a diagnostic capacity without the appropriate regulatory approvals and does not take steps to prevent its continued use, they could be prosecuted for failure to render assistance if this inaction leads to patient harm. The law could be interpreted to mean that healthcare professionals have a duty to intervene when they know that a medical device being used is potentially harmful due to non-compliance with regulatory standards.

For example, if a hospital administrator knows that ER doctors are using LLMs in place of approved diagnostic software and does not intervene, and if a patient is harmed as a result, the administrator could be liable under § 323c StGB.

**Summary of Legal Liabilities in Germany**

| <b>Legal Basis</b>                                        | <b>Description</b>                                                                                                                                    | <b>Relevant Law</b>                                                 | <b>Possible Outcome</b>                                 |
|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|---------------------------------------------------------|
| Unfair Competition (Wettbewerbsrecht)                     | Misclassification of the device leading to unfair competition, such as self-certifying a higher-class device as Class I.                              | Gesetz gegen den unlauteren Wettbewerb (UWG)                        | Injunctions, removal from the market, financial damages |
| Product Liability (Produkthaftung)                        | If the misclassified device causes harm or injury to patients due to defects or misclassification.                                                    | Produkthaftungsgesetz (ProdHaftG)                                   | Compensation for damages to harmed patients             |
| Medical Device Regulation (MDR) Violation                 | Violation of MDR by incorrectly classifying the device under Class I when it should be Class II due to clinical claims (treat, diagnose).             | EU MDR 2017/745 & German Medizinprodukte-durchführungsgesetz (MPDG) | Fines, product recall, damages to competitors           |
| Bodily Harm (Körperverletzung)                            | Criminal liability if the use of the non-compliant device causes physical harm or injury to a patient.                                                | § 223 StGB                                                          | Fines or imprisonment based on severity                 |
| Negligent Bodily Harm (Fahrlässige Körperverletzung)      | If the misclassification and resulting product use causes harm due to negligence (e.g., failure to adhere to regulatory standards).                   | § 229 StGB                                                          | Fines or imprisonment based on severity                 |
| Failure to Render Assistance (Unterlassene Hilfeleistung) | If the company becomes aware of the risks associated with the misclassified product and fails to take necessary actions (recall, notify users, etc.). | § 323c StGB                                                         | Criminal charges, potentially fines or imprisonment     |

**5. Legal Framework: U.S.A.**

The U.S. legal framework concerning the use of LLMs in clinical settings is governed primarily by federal law, including Food and Drug Administration (FDA) regulations, as well as state-level tort laws related to medical malpractice and product liability. The use of AI systems in healthcare is subject to strict regulations, particularly when the software falls under the category of Software as a Medical Device (SaMD).

**5.1 FDA Medical Device Regulations (21 CFR, FDCA)**

In the U.S., any software used for medical purposes, including diagnosis or treatment, is classified as a medical device under the Federal Food, Drug, and Cosmetic Act (FDCA). The FDA regulates the marketing and use of medical devices, including SaMD, under 21 CFR Part 820 (Quality System Regulation) and 21 U.S.C. § 360e for premarket approval. SaMD must undergo rigorous testing, clinical validation, and regulatory approval before being used in clinical settings.

If a doctor uses an LLM to assist in diagnostic or treatment decisions without FDA approval, the software would be considered an unapproved medical device. The hospital or physician using the software could face penalties under 21 U.S.C. § 331, which prohibits the introduction of misbranded or adulterated devices into interstate commerce.

Violations of these regulations can lead to:

- FDA Warning Letters or product seizures under 21 U.S.C. § 334.
- Criminal penalties for introducing unapproved devices under 21 U.S.C. § 333.
- Civil penalties for using unapproved medical devices or making false claims about their approval status under 21 U.S.C. § 352.

## **5.2 Criminal and Civil Liabilities in the U.S.**

Similar to Germany, there are both civil and criminal liabilities that can arise from the improper use of AI in healthcare settings.

### **5.2.1 Introduction of Misbranded Devices (21 U.S.C. § 331)**

Under 21 U.S.C. § 331, it is illegal to introduce misbranded or adulterated medical devices into interstate commerce. If a hospital uses LLMs for diagnostic purposes without FDA approval, the software could be considered misbranded. Misbranding occurs when a device is marketed without the necessary labeling or regulatory clearance, particularly when it is used in a capacity for which it is not approved (e.g., making clinical decisions).

Criminal penalties for introducing misbranded devices can include:

- Fines and imprisonment under 21 U.S.C. § 333, particularly if the misbranding results in harm to patients.
- Civil penalties may also apply, including product seizures and injunctions to prevent further use of the software in clinical settings.

### **5.2.2 Negligence and Medical Malpractice**

If an unapproved LLM is used to make diagnostic decisions and a patient is harmed as a result, the doctor and hospital could be sued for medical malpractice. In the U.S., medical malpractice is governed by state tort law, and the standard of care is based on what a reasonably competent physician would have done under similar circumstances. If the use of an unapproved AI system deviates from the standard of care, the physician and hospital could be found liable for negligence.

In medical malpractice cases, the plaintiff must prove:

1. Duty of care: The physician or hospital owed a duty of care to the patient.
2. Breach of duty: The use of unapproved AI deviated from the accepted standard of care.
3. Causation: The breach of duty caused harm to the patient.
4. Damages: The patient suffered measurable harm (e.g., injury, death) as a result.

If the hospital or physician is found liable, they may be required to pay compensatory damages for medical costs, lost wages, pain and suffering, and potentially punitive damages if the conduct was egregious (e.g., knowingly using unapproved software).

### **5.2.3 HIPAA Violations**

Another area of potential liability in the U.S. arises from the Health Insurance Portability and Accountability Act (HIPAA). If a LLM is used in a clinical setting and processes protected health information (PHI) without the appropriate safeguards, the hospital could be liable for HIPAA violations. This could occur if the AI system is not HIPAA-compliant and allows unauthorized access or disclosure of PHI.

HIPAA violations can result in:

- Civil penalties imposed by the U.S. Department of Health and Human Services (HHS).
- Criminal penalties for willful violations

HIPAA (Health Insurance Portability and Accountability Act) ensures the protection of protected health information (PHI) in healthcare settings. If an LLM is used in clinical settings, and it processes, stores, or transmits PHI without complying with HIPAA's strict privacy and security rules, this could result in significant penalties for the healthcare provider. Since LLMs are not inherently designed to be HIPAA-compliant, using them without proper safeguards could lead to breaches of patient privacy.

The potential consequences of HIPAA violations include:

- Civil penalties: These range from \$100 to \$50,000 per violation, depending on the degree of culpability, with a maximum annual penalty of \$1.5 million for identical violations.
- Criminal penalties: If the violation is intentional or involves willful neglect, criminal charges can be filed, which may result in fines of up to \$250,000 and imprisonment for up to 10 years.
- Loss of reputation: In addition to financial penalties, healthcare providers could face reputational damage, loss of patients, and increased scrutiny from regulators.

HIPAA violations are particularly concerning in cases where LLMs might store or transmit PHI to third-party servers without explicit patient consent or secure encryption. Hospitals are obligated to ensure that any software processing PHI complies with HIPAA regulations, and failure to do so could lead to civil lawsuits from patients, in addition to regulatory penalties.

#### **5.2.4 Fraud (False Claims Act and Health Care Fraud)**

In the United States, hospitals and healthcare providers are subject to strict regulations regarding the False Claims Act (FCA) and healthcare fraud statutes, especially in the context of billing Medicare, Medicaid, or other federal health programs. If an LLM is used in the diagnostic process or treatment without regulatory approval, the hospital could be subject to fraud charges if they billed federal programs based on the use of an unapproved medical device.

- False Claims Act (FCA): The FCA imposes liability on any person or entity that submits false claims to the federal government. If a hospital uses an unapproved AI system in diagnosing or treating patients and then bills Medicare or Medicaid for these services, they could be liable under the FCA for submitting fraudulent claims. Penalties under the FCA can include:
  - Treble damages: Hospitals can be required to pay three times the amount of the fraudulent claim.
  - Civil fines: Each false claim can result in fines ranging from \$5,000 to \$23,000.
- Whistleblower actions: Employees who report improper practices involving the use of unapproved medical devices can file qui tam lawsuits under the FCA, potentially earning a portion of the recovered damages.
- Health Care Fraud (18 U.S.C. § 1347): Health care fraud occurs when false representations are made to obtain funds from federal healthcare programs. Using a LLM in patient care without FDA approval and subsequently billing the government for those services could be considered fraudulent. Penalties for healthcare fraud include:
  - Imprisonment: Up to 10 years in prison for each offense.
  - Fines: Substantial financial penalties, including restitution for losses incurred by the government programs.
  - Exclusion: Healthcare providers found guilty of fraud may be excluded from participating in federal healthcare programs, such as Medicare and Medicaid, which can be financially devastating.

#### **5.2.5 Negligence and Criminal Negligence**

In the U.S., negligence is the primary cause of action in medical malpractice cases. If a hospital or healthcare provider uses an unapproved AI system in making diagnostic or treatment decisions, and a patient suffers harm as a result, the provider may be sued for negligence. The legal standard for medical negligence includes:

1. Duty of care: The healthcare provider owes a duty to the patient to provide treatment that meets the standard of care.
2. Breach of duty: The use of unapproved AI in making medical decisions could be viewed as a breach of that duty.
3. Causation: The patient must prove that the breach caused their injury or harm.
4. Damages: The patient must have suffered actual harm, whether physical, emotional, or financial.

In some cases, if the use of the LLM is particularly egregious, such as knowing the software was not approved and still relying on it for patient care, the hospital could face criminal negligence charges. Criminal negligence is a higher standard than civil negligence and applies when an individual or entity's reckless behavior leads to harm or death. For example, if an LLM gives incorrect diagnostic advice and the patient dies as a result, the physician or hospital could face charges under involuntary manslaughter statutes, punishable by imprisonment and substantial fines.

### Summary of Legal Liabilities in the U.S.

| Description                                 | Relevant Law                                                                                                                                                     | Possible Outcome                       |                                                               |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|---------------------------------------------------------------|
| FDA Violation (Misbranded Devices)          | Using a LLMs without FDA approval as a medical device could result in violations for introducing misbranded devices into interstate commerce.                    | 21 U.S.C. § 331 (FDCA)                 | Criminal fines, product seizures, imprisonment                |
| HIPAA Violations                            | Unauthorized use of LLMs to process protected health information (PHI) could result in violations of privacy regulations.                                        | HIPAA (45 CFR Parts 160 and 164)       | Civil fines, criminal penalties, reputational damage          |
| Negligence (Medical Malpractice)            | If using LLMs results in patient harm, the hospital or physician could be sued for medical malpractice under negligence claims.                                  | State Tort Law                         | Civil compensation for damages, including medical expenses    |
| False Claims Act                            | If the hospital bills Medicare/Medicaid for services rendered based on AI-driven diagnostics or treatment without FDA approval, it could result in false claims. | 31 U.S.C. §§ 3729–3733 (FCA)           | Treble damages, civil fines, whistleblower actions            |
| Health Care Fraud (18 U.S.C. § 1347)        | Using unapproved AI systems and billing federal healthcare programs could result in health care fraud charges.                                                   | 18 U.S.C. § 1347                       | Imprisonment, fines, exclusion from federal programs          |
| Negligent Bodily Harm (Criminal Negligence) | If patient harm occurs due to negligent use of LLMs, the hospital or physicians may face criminal negligence or involuntary manslaughter charges.                | State Criminal Codes, 18 U.S.C. § 1112 | Imprisonment, fines, criminal penalties for reckless behavior |

## 6. Insurance Considerations

The use of unapproved AI systems for clinical decision-making introduces new legal and financial risks for hospitals and their insurers. If a hospital allows its physicians to use LLMs for diagnostics or treatment without ensuring the software complies with FDA regulations, the consequences could lead to increased liabilities, affecting the hospital's insurance coverage and premiums.

### 6.1 Denial of Coverage

One of the first potential reactions from insurers would be the denial of coverage for claims arising from the use of unapproved software in clinical settings. Medical malpractice insurance policies typically contain clauses that exclude coverage for illegal activities or practices that fall outside the scope of standard care. If a LLM is used without FDA approval, the hospital could be considered to be engaging in an illegal or non-compliant practice.

- **Illegal Use of Unapproved Medical Devices:** If the AI system is not cleared or approved by the FDA, the insurer may argue that any resulting claims—whether for medical malpractice or regulatory fines—are not covered because they arise from the use of an unapproved medical device.
- **Exceeding Scope of Policy:** Policies may explicitly exclude coverage for emerging technologies like AI unless those technologies have been specifically approved for



use. Using a LLM without such approval could lead to a denial of coverage for any related claims, leaving the hospital financially exposed.

## 6.2 Medical Malpractice Claims and Premium Increases

If a LLM is used in diagnostics or treatment and results in patient harm, hospitals could face medical malpractice lawsuits. Even if the insurer covers the claim, the hospital could experience a significant increase in insurance premiums due to the heightened risk associated with the use of unapproved software.

- **Risk of Malpractice Claims:** Insurers could assess the use of AI in healthcare as a higher-risk activity, leading to increased premiums to account for the potential of patient harm. For example, if a misdiagnosis or incorrect treatment advice from a LLM leads to serious complications or death, the insurer may reclassify the hospital as a high-risk policyholder.
- **Loss of Coverage:** In some cases, repeated violations or failure to adhere to best practices in the use of AI could result in the loss of insurance coverage. Insurers may refuse to renew policies if the hospital continues to use unapproved AI technologies in patient care, leaving the hospital vulnerable to uncovered liabilities.

## 6.3 Subrogation Actions

If an insurer pays out claims related to the use of a LLM or another unapproved AI system, they may pursue a subrogation action against the hospital or the software provider to recover those costs.

Subrogation occurs when an insurer pays out a claim on behalf of an insured party and then seeks to recover those costs from a third party responsible for the loss. In cases where hospitals use unapproved LLMs and patient harm results, insurers may argue that the responsibility for the harm lies with either the hospital for using an unapproved device or the software provider for failing to properly certify the device.

- **Subrogation Against the Hospital:** If the insurer believes the hospital knowingly used an unapproved AI system, they may pursue a subrogation action to recoup the costs paid out for patient claims. This would be particularly likely if the hospital failed to adhere to regulatory standards or its internal policies regarding the use of AI in clinical settings.
- **Subrogation Against the Software Provider:** Insurers may also target the developers of the AI system, especially if the software was marketed in a way that implied it was suitable for clinical use without the necessary regulatory approval. The insurer may claim that the software provider misled the hospital or failed to properly certify the device under FDA or EU MDR regulations. In such cases, the software company could be held liable for damages.

## 6.4. HIPAA and Data Breach Liability

In the event that an AI system is used in healthcare and exposes protected health information (PHI) in violation of HIPAA, insurers might face large claims related to data breaches or privacy violations. Insurers typically offer cyber liability insurance or professional liability insurance that covers healthcare providers for certain HIPAA-related penalties or civil lawsuits, but there are key limitations:

- **HIPAA Fines and Penalties:** If a hospital's use of a LLM leads to a breach of patient data and violates HIPAA, the insurer may not cover the regulatory fines associated with the violation, especially if the use of a LLM was unauthorized. Insurance policies often exclude coverage for intentional or reckless violations of the law and using an unapproved AI system in a clinical setting might fall into this category.
- **Data Breach Notification Costs:** In the event of a HIPAA breach, the hospital may be required to notify all affected patients, which could result in substantial costs. Some cyber liability insurance policies cover the costs of breach notification, credit monitoring, and public relations efforts to mitigate reputational damage. However, if the breach is traced back to the use of an unapproved AI system, coverage might be limited or denied.

## 6.5 Exclusion of Future AI-Related Claims

Given the evolving risks associated with AI in healthcare, insurers may choose to exclude coverage for claims arising from the use of LLMs in future policies. Hospitals may be required to seek additional endorsements or specialized coverage to address the risks associated with using AI in clinical settings. Insurers could also place specific conditions on coverage, such as requiring the hospital to demonstrate that any AI system in use has been FDA-approved or complies with EU MDR requirements.

- **AI Exclusions in Malpractice Policies:** Insurers could introduce specific exclusions for the use of AI systems unless they are explicitly approved for clinical use. This would leave hospitals that use unapproved LLMs unprotected in the event of a malpractice claim related to AI-based diagnostics or treatment.
- **Riders for AI Use:** Alternatively, insurers may offer riders or endorsements to cover the use of AI in healthcare, but this coverage could come with higher premiums and stricter conditions, such as regular audits to ensure compliance with regulatory standards.

## 7. Regulatory Violations and AI-Specific Issues

The regulatory landscape governing the use of artificial intelligence (AI) in healthcare is still developing, especially as LLMs are increasingly integrated into clinical settings. These models present unique challenges in terms of regulation, classification, and safety, which existing frameworks—such as the FDA’s SaMD regulations and the EU MDR—are only beginning to address.

### 7.1 Challenges in Classifying AI as a Medical Device

The core challenge in regulating AI systems as medical devices lies in their unique functionality. Traditional medical devices are designed with specific, limited functionality and are subject to rigorous premarket testing and validation. AI, particularly LLMs, operates in a much broader, dynamic fashion, capable of generating responses that go beyond the traditional scope of medical devices.

1. **Continuous Learning Systems:** AI systems that rely on machine learning, especially those that are self-improving over time, pose additional challenges. These systems may not behave in the same way after deployment as they did during testing, which makes it difficult to ensure they meet safety standards over time. The current regulatory frameworks may not be fully equipped to monitor the evolving nature of AI systems in real-time clinical use.
2. **Software as a Medical Device (SaMD):** According to the FDA and IMDRF (International Medical Device Regulators Forum), SaMD is defined as software intended to be used for medical purposes independent of a hardware device. LLMs may fall under this definition if they are used to assist with clinical decisions. However, many AI systems, including popular LLM, are general-purpose AI models not specifically developed or validated for medical use, creating a grey area in terms of regulatory classification.

### 7.2 FDA and EU MDR Approaches to AI Regulation

Regulatory bodies like the FDA and the European Commission (under the EU MDR) have frameworks in place for software used in medical contexts, but the application of these frameworks to AI systems like LLMs remains limited and is evolving.

- **FDA:** The FDA has developed specific guidelines for SaMD and has approved certain AI-based software for diagnostic and treatment purposes. However, these approvals are typically for narrow AI systems designed for a specific medical task (e.g., radiological analysis or screening for diabetic retinopathy). The broader use of LLMs for general diagnostic advice has not been specifically addressed by the FDA, making it unclear how these systems would be regulated in a clinical setting.
- **EU MDR:** The EU Medical Device Regulation (MDR) has similar provisions for software classified as medical devices, but the dynamic and evolving nature of AI presents challenges. Under the MDR, AI systems must undergo rigorous conformity assessments, including clinical evaluations, before being certified for medical use. However, the use of general-purpose AI systems for diagnostics may not fit neatly into the current MDR framework, especially if the AI system was not specifically designed for medical purposes.

### 7.3. Liability for AI-Related Errors

As AI systems or LLMs become more integrated into clinical settings, determining liability for errors made by these systems will become increasingly complex. Current medical malpractice laws and product liability statutes are designed for human errors or traditional medical devices but may not be well-suited to AI-generated errors.

1. **Shared Liability:** In cases where AI is involved in a medical decision, shared liability between the hospital, physician, and AI developer may arise. For example, if a physician uses a LLM to assist in diagnosing a patient and the patient is harmed due to incorrect AI-generated advice, the physician, hospital, and AI developer could all potentially be liable.
2. **Challenges with AI Autonomy:** If AI systems are treated as autonomous entities capable of making independent decisions, this could shift the standard of care in malpractice cases. Courts may need to determine whether physicians acted reasonably in relying on the AI system, or whether the AI developer should bear responsibility for the system's decisions. The "black box" problem—where the reasoning behind AI decisions is opaque—further complicates liability attribution.

### 7.4 Potential New Regulatory Frameworks for AI in Healthcare

The unique challenges posed by AI in healthcare may lead to the development of new regulatory frameworks designed specifically for AI-driven medical systems. Such frameworks could address the limitations of current regulations by focusing on the specific risks posed by AI, including:

- **Dynamic updating and continuous learning:** Ensuring AI systems are safe and effective over time, even as they improve and adapt.
- **Transparency and explainability:** Requiring that AI decisions be interpretable by humans, particularly in critical healthcare contexts.
- **Post-market surveillance:** Implementing robust post-market monitoring systems to identify issues with AI systems in real-time clinical use.

## 8. Discussion

The integration of AI systems into healthcare is inevitable as technological advancements accelerate. However, the legal, regulatory, and insurance implications of using unapproved AI systems in medical settings are vast and multifaceted. This paper has outlined the numerous ways in which the use of non-compliant AI systems can lead to both civil and criminal liabilities for healthcare providers in the United States and Germany, along with the potential for denial of insurance coverage and increased premiums for hospitals.

### 8.1 Legal and Regulatory Challenges

Both the U.S. and Germany have robust regulatory frameworks for medical devices and software used in clinical settings, but the application of these frameworks to general-purpose AI systems remains in its infancy. The current legal frameworks are primarily designed for narrow AI systems that perform specific, well-defined tasks, but the dynamic, evolving nature of LLMs presents new challenges for regulatory bodies.

The FDA and EU MDR will need to develop more detailed guidelines for general-purpose AI systems used in healthcare, focusing on: Real-time monitoring and validation of AI

The current regulatory structures for Software as a Medical Device (SaMD) under the FDA and EU MDR are well-suited for traditional medical devices, but they are less equipped to handle the evolving and dynamic nature of general-purpose AI systems like LLMs (Large Language Models). These systems represent a fundamental shift in how healthcare could potentially incorporate AI, as they operate beyond the static, pre-programmed functions of traditional medical software. The dynamic updating, vast scope of knowledge, and potential for unpredictable outputs create a gray area in regulation.

The development of new guidelines could include:

- **Specific AI Classification:** Regulators will need to clarify how to classify AI-based systems when they are used in healthcare. This might involve placing general-purpose AI in a separate classification from narrow AI systems that are designed for specific tasks, such as analyzing medical images or assisting with specific diagnoses.
- **Dynamic Learning and Monitoring:** AI systems that learn and improve autonomously over time present unique risks, as they may change their behavior after deployment. Regulatory frameworks must address the continuous validation and monitoring of these systems to ensure they remain safe and effective throughout their lifecycle. This may include regular re-evaluations, post-market surveillance, and mandatory updates based on real-world data.
- **AI Accountability and Explainability:** One of the central challenges with AI, particularly black-box models, is their lack of transparency. When AI systems generate outputs that healthcare professionals use in diagnosis or treatment, there must be clear mechanisms for understanding how these decisions were made. Regulatory frameworks may need to require that AI systems provide explanations or justifications for their outputs, especially in cases where a physician's reliance on AI results in patient harm.

## 8.2 Liability and Legal Precedents

In both Germany and the United States, legal precedents surrounding the use of AI in healthcare are still in early stages, and many unresolved issues remain. Courts will likely need to decide how to distribute liability when AI systems contribute to medical decisions that lead to patient harm.

- **Shared Liability:** As mentioned earlier, liability in AI-related malpractice cases may involve multiple parties: the physician who used the AI system, the hospital that allowed it, and the AI developer. Legal systems in both countries will need to determine to what extent each party is responsible when an AI system gives incorrect advice or a diagnosis that leads to harm.
- **Standard of Care and AI:** Courts will need to address whether using an AI system constitutes an acceptable standard of care. If a physician follows the advice of an LLM and the patient suffers as a result, the legal question becomes whether the physician reasonably relied on the AI system. Standards of care may need to evolve to incorporate the use of AI in clinical practice, but this transition period will likely lead to complex litigation.
- **Precedents for AI:** There are few, if any, definitive legal precedents for the use of LLMs in healthcare. This lack of legal history creates uncertainty for healthcare providers who wish to use these technologies, as they may not have clear legal guidelines on how to do so safely or without assuming excessive risk.

## 8.3 Insurance and Risk Management

For hospitals and insurers, the use of unapproved AI systems presents significant financial and legal risks. As detailed earlier, insurers are likely to take several actions in response to claims arising from the use of unapproved AI, including denying coverage for illegal activities, raising premiums, or excluding AI-related claims from future policies.

- **Denial of Coverage:** Insurers may refuse to cover claims related to the use of unapproved AI systems in clinical settings, particularly if those systems were used without regulatory approval. Hospitals could face significant financial exposure if patients are harmed due to AI-generated decisions, and the hospital's malpractice insurance does not cover the incident.
- **Premium Increases:** Even if claims related to the use of AI systems are covered, insurers are likely to increase premiums to account for the additional risk. The use of AI in healthcare introduces new uncertainties, especially when the AI systems are not fully understood by medical professionals or not properly validated for clinical use.
- **Subrogation:** Insurers may also pursue subrogation actions against hospitals or AI developers to recover the costs of paid claims. This would allow insurers to shift the financial burden of AI-related malpractice claims onto the parties responsible for introducing the technology.

## 8.4 Ethical Considerations

The use of AI in healthcare raises significant ethical concerns that intersect with legal and regulatory challenges. Healthcare providers must balance the potential benefits of using AI systems with the risks of patient harm and the erosion of trust in clinical judgment.

- **Reliance on AI:** One of the most pressing ethical issues is the degree to which physicians may rely on AI for medical decisions. While AI systems may offer valuable insights, there is a risk that physicians could defer too much responsibility to these systems, leading to decisions that may not be in the patient's best interest. The ethical principle of autonomy dictates that patients should receive care based on human judgment, not solely on algorithmic outputs.
- **Transparency and Consent:** Another ethical consideration is whether patients are aware of and have consented to the use of AI systems in their treatment. If patients are not informed that AI is playing a role in their diagnosis or treatment decisions, this could violate ethical standards of informed consent. Additionally, the lack of transparency in how AI models generate their recommendations could undermine patient trust.
- **Equity and Bias:** AI systems, including LLMs, are only as unbiased as the data on which they are trained. There is a growing body of evidence that suggests AI systems can perpetuate or even exacerbate biases in healthcare, particularly in diagnosing and treating marginalized groups. Healthcare providers must be vigilant in ensuring that AI systems do not introduce disparities in care or disproportionately harm certain populations.

## 9. Conclusion

The integration of AI systems into healthcare offers exciting possibilities for enhancing diagnostic accuracy, improving treatment recommendations, and reducing the workload of medical professionals. However, the use of these technologies also introduces a host of legal, regulatory, and ethical challenges that healthcare providers, regulators, and insurers must address.

### Key Findings

1. **Legal and Regulatory Gaps:** Both Germany and the United States have well-established frameworks for regulating medical devices and software, but these frameworks are not yet fully equipped to handle the complexities of general-purpose AI. The current regulatory landscape is designed for narrow AI systems, and new guidelines will be needed to address the unique risks posed by AI systems that evolve and learn over time.
2. **Civil and Criminal Liability:** In both jurisdictions, Software Developers and Software and AI providers as well as healthcare providers could face civil liability for malpractice, product liability claims, and breaches of regulatory standards. Criminal liability could arise in cases of negligence or recklessness, particularly if the use of AI leads to patient harm. Physicians and hospitals must be cautious in relying on unapproved AI systems, as the potential for harm—and subsequent legal action—is significant.
3. **Insurance Implications:** Insurers are likely to react strongly to the use of unapproved AI in clinical settings, with potential actions including the denial of coverage, increased premiums, or subrogation actions. Hospitals may need to seek specialized insurance coverage for AI-related risks, but this coverage will come at a higher cost.
4. **Ethical Concerns:** The ethical considerations surrounding AI in healthcare must not be overlooked. Ensuring transparency, preventing bias, and maintaining the patient-physician relationship are critical to the successful integration of AI technologies. These issues must be addressed alongside regulatory and legal reforms.

### Recommendations

1. **Regulatory Development:** Governments and regulatory bodies such as the FDA and European Commission should develop AI-specific guidelines that account for the unique risks and benefits of LLMs and other general-purpose AI systems. These

- guidelines should address issues such as real-time validation, continuous monitoring, and AI accountability.
2. **Liability Frameworks:** Courts and legal systems in both the U.S. and Germany need to clarify how liability will be distributed in cases involving AI-generated errors. This should include establishing clear standards for shared liability among physicians, hospitals, and AI developers.
  3. **Insurance Innovation:** Insurers should develop new policies and riders that specifically address the use of AI in healthcare, offering coverage that protects both patients and providers while incentivizing the safe and compliant use of AI systems.
  4. **Ethical Oversight:** Hospitals and healthcare providers must adopt ethical frameworks for using AI, ensuring that patients are fully informed, and that AI systems are used to augment, not replace, human judgment. Additionally, steps should be taken to minimize bias and ensure equitable outcomes in AI-assisted care.
  5. **Stricter Enforcement and Surveillance:** Regulators should adopt a more proactive enforcement approach, including random audits and increased scrutiny of self-certified Class I devices, especially those claiming diagnostic or therapeutic functionalities that might warrant higher classification.
  6. **Clarification of Regulatory Requirements for AI:** Given the dynamic nature of AI-based systems, the EU MDR and FDA guidelines should provide more specific criteria for classifying AI as SaMD, ensuring that devices are not misclassified due to ambiguities in the risk classification frameworks.
  7. **Increased Transparency and Industry Collaboration:** Regulators should enhance collaboration with industry stakeholders, including clear communication about compliance expectations and providing resources or programs that support manufacturers in correctly classifying and validating their products.

## References

- European Commission. (2017). Medical Device Regulation (EU MDR 2017/745). European Parliament and Council of the European Union.
- Food and Drug Administration (FDA). (2017). Digital Health Innovation Action Plan. FDA.gov.
- Food and Drug Administration (FDA). (2019). Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD). FDA.gov.
- International Medical Device Regulators Forum (IMDRF). (2013). Software as a Medical Device (SaMD): Key Definitions. [Online]. Available at: <http://www.imdrf.org>
- Medizinprodukte-Durchführungsgesetz (MPDG). German Medical Devices Implementation Act, implementing EU MDR in Germany.
- Produkthaftungsgesetz (ProdHaftG). German Product Liability Act, covering liability for defective products, including medical devices.
- Gesetz gegen den unlauteren Wettbewerb (UWG). German Act Against Unfair Competition, regulating commercial practices and the misrepresentation of medical devices.
- StGB §§ 223, 229, 323c. German Criminal Code provisions on bodily harm, negligent bodily harm, and failure to render assistance.
- 21 U.S.C. § 331, § 352, § 3729–3733. Federal Food, Drug, and Cosmetic Act and False Claims Act, addressing medical device violations in the U.S.
- 18 U.S.C. § 1347, § 1001. Healthcare fraud and false statements statutes under U.S. federal law.
- 45 CFR Parts 160 and 164. HIPAA regulations on the privacy and security of protected health information.

- Communications Act of 1934 (as amended). Federal Communications Commission regulations to prevent the dissemination of misleading medical information through communication channels.
- Hodge, J. G., Orenstein, D. G., & Weidenaar, K. (2020). HIPAA and emerging technologies in health care. *Journal of Law, Medicine & Ethics*, 48(1), 191-195.
- Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. *Science*, 366(6464), 447-453.
- ISO 13485:2016. International standard for quality management systems in medical devices.
- ISO 14971:2019. International standard for risk management in medical devices.

#### Disclaimer

I am releasing this paper without exact details of the steps to take either to register and AI as SaMD or integrate as non-SaMD into existing hospital systems as those details are subject to active NDAs.

Please anticipate errors and limitations as the regulatory landscape is evolving quickly.

I welcome feedback and evaluations of the content.

THIS PAPER IS NOT LEGAL ADVICE in any form or way.

Specific references to trials cannot be provided as per court orders for Expert Witness obligations.

#### Author Contributions

The work of conceptualization, methodology, evaluation, analysis was done by the author. A local, specifically trained (regulations of US, EU Germany and Australia for SaMD, AI and Hospitals) Large Language Model was used to generate Abstract and original draft. The author read, reviewed and approved the final manuscript.

#### Declaration of Interests

The author is Expert Witness to all German Courts and International Courts for Medical Devices and In-Vitro Diagnostics and has consulted companies and hospitals in regard to Software and AI integration either into EHR Software or as SaMD.