# Medical Exam Selfies and Records Negligence

Union of Saints

## Navigating OSIRAM in the Modern Medical Industry

The modern medical system is increasingly intertwined with digital technology. While these tools can improve efficiency, recordkeeping, and patient communication, they also introduce serious concerns regarding privacy, consent, and the security of medical data. Within the framework of Union of Saints doctrine, the concept of **OSIRAM**—the coercive or manipulative use of systems that compromise dignity, autonomy, or safety—provides a lens through which to examine emerging practices in healthcare.

One such concern is the growing practice of requiring patients to submit **selfies or facial verification images** during medical intake, telehealth access, or identity verification processes. In some contexts, these measures are introduced to prevent fraud, confirm identity, or comply with digital security standards. However, when patients feel pressured or compelled to provide biometric images without clear explanation or alternatives, questions arise regarding consent, necessity, and long-term data storage. Within an OSIRAM framework, the forcing of patients to provide personal biometric images—particularly in vulnerable medical settings—may represent an overreach of technological authority.

Another significant concern involves the **potential trafficking or misuse of medical records**. Medical records contain highly sensitive information, including personal identity data, medical histories, insurance details, and sometimes biometric identifiers. If improperly secured or shared across complex digital networks, these records may become valuable targets for cybercriminals, fraud rings, or illicit data markets. In recent years, cybersecurity experts and national security officials have increasingly warned that healthcare databases represent attractive targets for attackers because of the richness and permanence of the information they contain.

The risk is compounded by the complex ecosystem through which medical data now travels. Hospitals, insurance companies, laboratories, telehealth platforms, and third-party software vendors often exchange information within large digital supply chains. Each additional point of access introduces potential vulnerabilities. Patients may not fully understand how widely their information is distributed, who ultimately stores it, or what safeguards exist to prevent misuse.

At the same time, medical professionals operate under immense pressure. Physicians, clinicians, nurses, and healthcare administrators must balance patient care, regulatory requirements, insurance systems, and rapidly evolving technologies. These challenges deserve recognition and respect. However, because medicine deals directly with the health, dignity, and personal autonomy of individuals, the medical industry must also be held to the **highest ethical and security standards in the United States**.

Patients must be able to trust that their data, images, and personal histories are protected with the utmost care. Yet many individuals feel that medical negligence cases are difficult to

pursue successfully, leaving patients with limited recourse when errors, data breaches, or improper practices occur. This perception contributes to growing public concern about transparency and accountability within the healthcare system.

For this reason, greater **public scrutiny and policy attention** may be necessary. National security advisors, lawmakers, and regulatory bodies may need to examine whether existing legal frameworks sufficiently protect patients in a digital medical environment. Potential reforms could include stronger consent requirements for biometric data collection, stricter limitations on the sharing of patient images, clearer disclosure of data-handling practices, and stronger penalties for negligent handling of medical records.

Patients themselves also play an important role in protecting their autonomy. Individuals should feel empowered to ask how their information will be stored, who will have access to it, and whether alternative identification methods exist when biometric verification is requested. Transparency between providers and patients strengthens trust and reduces the risk of misunderstanding or exploitation.

Ultimately, the question is not whether digital tools belong in medicine—they undoubtedly do. Rather, the question is how these technologies can be implemented **without compromising patient dignity, privacy, or safety**. When medical systems require intrusive data collection without clear safeguards, they risk crossing into the type of structural pressure that the Union of Saints identifies as OSIRAM.

The risk is real, but so is the opportunity to address it responsibly. Mitigating these dangers requires open discussion, regulatory vigilance, and an informed public willing to examine the systems that govern their healthcare. By encouraging transparency, ethical accountability, and patient empowerment, society can ensure that medical technology serves humanity rather than undermines it.

In the Saintly way, the path forward is one of awareness, scrutiny, and principled reform—protecting both the dignity of patients and providers, and the integrity of the medical profession.