Douglass Brown

Arlecia Tyus

Security Policies & Procedures

May 3, 2026

HIPAA and GDPR Compliance for enVisiAIn: A Near-Future Health Technology

I am really into the game Cyberpunk 2077, and one of the concepts that stands out to me is Trauma Team International. In the game, Trauma Team is a high-tech emergency medical service that responds to clients with advanced medical support, security, and rapid intervention. While that version is clearly exaggerated and set in a dystopian future, it made me think about how a similar health technology company could exist in a more realistic way. For this assignment, I created a fictitious company called enVisiAIn, a health technology business that uses AI-augmented computer vision to help people regain or improve their ability to see and interpret the world around them.

By 2030, health technology companies will likely operate at the intersection of artificial intelligence, wearable devices, biometric data, and emergency response. enVisiAIn would provide smart glasses, mobile applications, and clinical support software for patients with serious visual impairments. The system would process live video, eye scans, location data, patient records, and AI-generated recommendations. The goal would be to help users navigate physical spaces, identify objects, recognize approved contacts, read signs, and receive emergency support when the device detects danger. Because of this, enVisiAIn would face serious compliance obligations under both HIPAA in the United States and GDPR in the European Union.

HIPAA would apply because enVisiAIn operates in the health field and handles electronic protected health information, also known as ePHI. If the company works with hospitals, doctors, insurers, or clinics, it may be considered a business associate or

part of a covered healthcare environment. The HIPAA Security Rule requires regulated entities to protect electronic health information through administrative, physical, and technical safeguards that preserve confidentiality, integrity, and availability. For enVisiAIn, this means the company would need secure access controls, audit logs, encryption, employee training, vendor management, and clear incident response procedures.

One technological solution enVisiAIn could use for HIPAA compliance is an identity and access management platform such as Microsoft Entra ID, Okta, or Duo. This would allow the company to control who can access patient data. A clinician may need to see a patient's treatment settings, while a customer support worker may only need limited account information. An AI engineer may need anonymized model performance data, but should not be able to view identifiable patient video or medical records. This type of role-based access control would be effective because it limits unnecessary exposure of patient data. However, it would also create implementation challenges because the company would need to carefully define each role and review access regularly.

A second HIPAA-related solution would be cloud security software with encryption, audit logging, and data loss prevention. Since enVisiAIn would process video, biometric scans, and clinical data, it would need to protect data both at rest and in transit. HIPAA technical safeguards include access control, audit controls, integrity protections, authentication, and transmission security. These tools would be highly effective for reducing breach risk, but they would also be expensive. Video and AI data require large amounts of storage and processing power. The company would need to balance the usefulness of collecting detailed visual data with the privacy principle of collecting only what is necessary.

GDPR would create a different but related set of obligations. If enVisiAIn serves users in the European Union, it would be processing personal data under GDPR. More importantly, it would be processing sensitive categories of data, including health data, biometric data, visual recordings, and location information. GDPR is designed to protect personal data and applies to organizations that process the data of people in the EU, even when the company itself is not based there. For enVisiAIn, GDPR would re-

quire clear consent, data minimization, privacy notices, the ability for users to access or correct their data, and strong protections around automated decision-making.

A useful GDPR solution would be a consent and privacy rights management platform such as OneTrust, DataGrail, Transcend, or TrustArc. This type of software could help enVisiAIn track user consent, explain how data is used, manage privacy requests, and document compliance. For example, a patient may agree to let enVisiAIn use their eye scans for treatment but not for AI model training. Another user may request a copy of their data or ask the company to delete certain information. A privacy management platform would make those workflows more organized. The challenge is that healthcare data cannot always be deleted immediately because medical, safety, or legal retention requirements may apply.

Another GDPR solution would be a data mapping and data protection impact assessment tool. This would help enVisiAIn understand where data enters the company, where it is stored, who uses it, which vendors receive it, and when it should be deleted. This matters because AI computer vision creates complex data flows. A smart glasses device may capture a patient's surroundings, other people's faces, street signs, homes, workplaces, and medical information. Even if the company's goal is helpful, the privacy risk is high. GDPR would push enVisiAIn to build privacy into the design instead of adding it later.

The biggest implementation challenge for enVisiAIn would be integration. Compliance tools cannot sit outside the business like a separate checklist. They must connect to daily operations. Identity management must connect to employee onboarding and clinical systems. Encryption must connect to the mobile app, smart glasses, cloud storage, and AI model pipeline. Consent management must connect to patient onboarding and account settings. Audit logs must connect to security monitoring and incident response. If these systems do not integrate well, employees may avoid them, workflows may slow down, and compliance may become performative instead of real.

Cost would also be a major concern. enVisiAIn would need to pay for secure cloud infrastructure, compliance management software, legal review, cybersecurity staff, privacy staff, employee training, penetration testing, vendor reviews, and regular audits. These costs would be high for a startup, but they would be necessary because

the company's product deals directly with patient safety and sensitive data. In this type of business, trust is part of the product. If users believe the system is unsafe or invasive, the technology will fail no matter how advanced it is.

Overall, enVisiAIn shows how future health technology companies will need to treat compliance as part of the design process. HIPAA would require the company to protect electronic health information through strong security safeguards. GDPR would require the company to respect privacy, consent, user rights, and responsible data processing. The most effective solution would be an integrated compliance stack made of identity management, encryption, audit logging, consent management, data mapping, and AI governance. The main challenge is that these tools are expensive and difficult to implement, but for a company handling medical, biometric, video, and location data, they are not optional. In a realistic 2030 health technology environment, compliance would not just protect enVisiAIn from penalties. It would protect the people depending on the system to safely see and move through the world.