Below is a structured assurance case for the security of Instant Messaging (IM) software, utilizing the Goal Structuring Notation (GSN):

\*\*Goal 1: Ensure the security of Instant Messaging Software\*\*

- Strategy 1: Address Security Through Multiple Layers

- Goal 1.1: Ensure Secure User Authentication

- Solution 1.1.1: Implement Multi-Factor Authentication

- Solution 1.1.2: Utilize Strong Hashing Algorithms for Password Storage

- Goal 1.2: Guarantee Secure User Data Transmission

- Assumption 1.2.1: Users have reliable internet connectivity

- Solution 1.2.1: Implement End-to-End Encryption using AES

- Solution 1.2.2: Use Secure Socket Layer (SSL)/Transport Layer Security (TLS) protocols

- Goal 1.3: Prevent Data Leakage

- Solution 1.3.1: Employ Data Loss Prevention (DLP) Techniques

- Solution 1.3.2: Regular Audits and Vulnerability Scans

- Goal 1.4: Ensure Software Integrity

- Solution 1.4.1: Use Code Signing Certificates

- Solution 1.4.2: Implement Automatic Update Mechanism

- Strategy 2: Ensure Compliance with Relevant Security Standards and Regulations

- Goal 2.1: Comply with General Data Protection Regulation (GDPR) for EU Users

- Solution 2.1.1: Implement Features for Data Access, Correction, and Deletion

- Solution 2.1.2: Conduct Regular GDPR Compliance Audits

- Goal 2.2: Align with HIPAA for US Healthcare Data

- Solution 2.2.1: Guarantee Data Encryption both at Rest and in Transit

- Solution 2.2.2: Execute Access Controls and Audit Trails

- Strategy 3: Manage and Mitigate Security Risks

- Goal 3.1: Identify and Prioritize Potential Security Threats

- Solution 3.1.1: Perform Regular Threat Modeling Sessions

- Solution 3.1.2: Maintain an Up-to-Date Threat Database

- Goal 3.2: Implement Measures to Mitigate Identified Risks

- Solution 3.2.1: Develop and Deploy Security Patches in a Timely Fashion

- Solution 3.2.2: Provide Robust User Education and Awareness Programs

This structure maps out key goals, strategies, solutions, and assumptions required to assure the security of the IM software. Each component is integral in maintaining a comprehensive security framework, designed to mitigate a wide variety of potential threats while ensuring compliance and user trust. Regular updates and compliance checks ensure adherence to legal standards and adaptability to evolving security challenges.