Comm100

HIPAA Compliant Digital Engagement for Healthcare Providers

The Comm100 digital omnichannel engagement platform helps you connect with your patients and clients where and when they prefer, in full compliance with the Health Insurance Portability and Accountability Act (HIPAA). Now you can confidently safeguard electronic Protected Health Information (ePHI) from unauthorized access or distribution while delivering the personalized service that defines your organization.

When it comes to digital communications, it takes a lot more than just a Business Associate Agreement to be compliant. We help you confidently embrace all the possibilities without compromising security or privacy. Here's how.

Security and Encryption of ePHI

Data encryption is a critical aspect of PHI security, as in the event a breach were to occur, it ensures that the data would not be legible or identifiable to an individual.

- **Data 'at rest':** encrypted through Amazon Web Services (AWS) RDS encryption algorithm which utilizes AES 256-bit encryption. AWS servers feature state-of-the-art SSAE 16, CSAE 3416, and ISAE 3402 security standards. We have Business Associate Agreements (BAA) in place with Amazon hosting facilities to demonstrate their compliance with our security processes.
- **Data 'in transit':** encrypted through HTTPS and TLS 1.2 protocol, depending on which browser version your client is using at the time.

ePHI Access and Authorization

Comm100 operates an ePHI least-access principle – our people are only authorized to access information that they absolutely need to in the course of their work. User access is reviewed on a regular basis to ensure that any access granted is appropriate given the individual's responsibilities. Any requests for increased access are reviewed and approved on a case-by-case basis.

Our business systems are secured using multi-factor authentication to further reduce the risk of unauthorized access, through one-time access tokens sent to employee cellphones. Login attempts are monitored and limited. These protocols apply to laptops and mobile devices used by our staff and apply whether employees are working in Comm100 offices or remotely.

Information Security Management

Our Information Security team is responsible for enforcing all Comm100 security and privacy policies spanning our network, our software, and our people. Our Chief Information Security Officer is supported by a team with extensive experience in IT management and systems security.

Our security management policies include:

- Ensuring the secure configuration and maintenance of system environments
- Running regular risk assessments including penetration testing
- Maintaining and regularly reviewing system logs
- Monitoring file integrity
- Management of intrusion detection and prevention systems
- Completion of risk analysis and management reports
- Management and configuration of firewalls
- Administering the security awareness program
- Reviewing and qualifying partners and third-party relationships

- Responding to customer security-related inquiries
- Reviewing exception reports and audit logs

We continuously review and update all policies to keep pace with evolving business and regulatory changes.

People Security Management

HIPAA compliance includes security protocols for our employees, partners, and independent contractors we may employ. Every group receives HIPAA training at the commencement of their employment or contract, and every subsequent year as a refresher. Training includes content that describes security controls and details workforce responsibilities in the event of security incident.

HIPAA training takes place within a broader backdrop of security-conscious processes at Comm100. Best practices are regularly reinforced through a wide-ranging security awareness program that provides employees with reminders and tips throughout the year.

We also provide extra training to employees who have a high degree of data access to ensure that they are aware of job-specific privacy and security procedures that apply to their day-to-day work.

We take HIPAA compliance very seriously, so our people are required to acknowledge in writing that they have understood and will follow our HIPAA and security policies. Our policies themselves state that where they are not followed, consequences are serious and formal sanctions will apply, up to and including termination of employment.

Workplace Security Management

Physical security systems at our office locations include keycard-controlled access, surveillance cameras, and fully encrypted workstations with up-to-date anti-malware protection.

Incident Response

Comm100 has a detailed Incident Response process that all employees must follow in the event of a security incident. This process ensures that Comm100 appropriately identifies and responds to suspected or known security incidents, that the harmful effects of security incidents are mitigated to the fullest extent possible, and that security incidents and their outcomes are fully documented and properly disclosed according to HIPAA and other compliance, regulatory, or voluntary requirements.

We also undertake test scenarios to evaluate the responsiveness and actions of our incident response team. These test scenarios are evaluated annually by our third-party assessor to ensure that the actions recommended by team members and the timeframes in which the scenarios were (hypothetically) resolved are acceptable under HIPAA.

Third-party HIPAA Compliance Assessment

Each year, we undergo a third-party HIPAA Compliance Assessment. While some patient engagement software vendors perform internal assessments, we contract a third party to ensure that we are appropriately protecting our network infrastructure and data communications from compromise.

Our last two assessments were performed by SecurityMetrics, a global leader in data security and compliance, headquartered in Orem, Utah. Assessment take place onsite over a number of days, during which time the assessor performs a number of different activities:

- Observe systems and compare results with documented diagrams and inventory
- Analyze policy and procedure documentation
- Evaluate security tools and controls
- Examine system configurations
- Interview personnel regarding skills, knowledge, and training
- Assess operating procedures
- Observe physical security controls

We would be pleased to share a copy of our most recent assessment report with you.

Comm100

Let's chat

Comm100 is a leading global provider of omnichannel customer experience solutions with a mission to make online service and support delivery more genuine, more personalized, and more productive through meaningful conversations. Let us show you how.

Learn more

@comm100 letschat@comm100.com 1-877-305-0464 comm100.com