MediClarus

SECURITY MEASURES

Website : www.mediclarus.com

MediClarus

SECURITY MEASURES AT MediClarus

At MediClarus, we take security very seriously. Our protocols adhere to HIPAA standards, ensuring the highest levels of protection for healthcare data.

As our healthcare customer, you can rest assured that your data privacy is safeguarded. We maintain rigorous standards for data security, network security, site security, and personnel security.

Our comprehensive security policies, internet usage policies, and software/hardware protocols ensure that all our employees uphold these standards. Partner with us for reliable, secure healthcare services, and rest assured your data remains confidential and protected.

We maintain detailed audit trails for all employees who have access to patient or healthcare data. Our processes and technology strictly follow HIPAA regulations concerning the security and confidentiality of patient health information. At the start of every project, we sign confidentiality and service agreements to guarantee complete data protection for our clients.

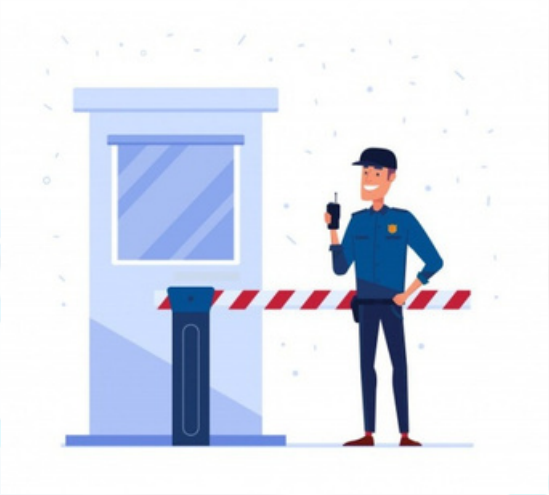
Website : www.mediclarus.com

MediClarus

SECURITY MEASURES AT MediClarus

1. Data Security

- Every MediClarus employee signs a confidentiality agreement before working on any project.
- Regular security audits and penetration tests are conducted to ensure compliance at all levels.
- Any security breaches, if they occur, are reported to our clients immediately.
- Our experienced IT team implements appropriate security infrastructure tailored to each project's requirements.
- Daily data backups are performed to safeguard against data loss.



2. Personnel Security

- Employee ID cards are verified upon entry into the premises.
- No physical documents are allowed to be taken in or out of the office.
- The use of personal laptops, CDs, and external devices (e.g., floppies) is strictly prohibited.
- Spot checks are conducted when personnel exit the premises.
- Employees are trained regularly on the importance of safeguarding customer data.
- All personnel with access to sensitive healthcare information must sign confidentiality and non-disclosure agreements.

SECURITY MEASURES AT MediClarus

MediClarus

3. Network Security

- System access is restricted to authorized personnel only.
- All external drives (e.g., USB, floppy disks) are disabled on every computer.
- Spot checks are conducted regularly to monitor compliance.
- Firewalls and antivirus software are installed and maintained up to date.
- All systems operate on secure servers using 128-bit SSL encryption.
- Password protection is implemented at multiple levels to prevent unauthorized access.
- In the event of an emergency, all network data is backed up and stored securely.
- We follow a strict network access policy and ensure best practices in password security.

MediClarus

SECURITY MEASURES AT MediClarus

4. Site Security

- Electronic security doors control and limit office access.
- Only authorized personnel can access customer data.
- Our premises are equipped with smoke alarms and fire extinguishers.
- Surveillance cameras operate 24x7 to monitor office activity.
- Security personnel are stationed 24x7 to prevent burglary or vandalism.