embin

MEDICAL · USA

Connected Medical Treatment Device Controller

Custom Hardware Design | Embedded Firmware | Graphical Display Interface | Remote Monitoring & Updates | Secure Access Control | Encrypted Communication

CLIENT

A US-based medical device company.

THE PROBLEM

The client's device prepares medicines using a precise electrical treatment process — precise enough that staff needed a proper graphical interface to operate it correctly, not just a few buttons and lights. But beyond the device itself, the client needed to know what was happening to every unit they'd shipped: whether it was running correctly, whether it needed a software update, and whether anyone other than authorized staff and devices could operate it. Without that, supporting a fleet of deployed devices meant relying entirely on customers to report problems.

WHAT WE BUILT

On the device itself, we built a high-resolution graphical display as the primary interface for staff, with the electrical treatment process driven by dedicated control hardware to keep the precision the application demanded. The bigger piece of engineering was everything around the device: a remote interface that lets the manufacturer monitor each unit's status and push software updates over the internet, encrypted so updates can't be tampered with in transit. Every operation, event, and error gets logged locally on the device first — so the record exists even if connectivity drops — and then synchronizes to a central database once the device is back online. To stop the system being operated by unauthorized devices or components, we built in secure hardware keys that the system checks before it will run at all.

WHAT IT DOES

- ✓ Provides a high-resolution graphical display as the primary on-device interface for staff
- ✓ Drives the electrical treatment process using dedicated control hardware for precise, repeatable operation
- ✓ Can be monitored remotely over the internet, giving the manufacturer visibility into the status of every deployed unit
- ✓ Receives software updates remotely, encrypted in transit so updates can't be tampered with en route
- ✓ Logs every operation, event, and error locally first, then synchronizes to a central database once online — so nothing is lost if connectivity drops
- ✓ Checks for a secure hardware key before operating, preventing use by unauthorized devices or components

OUTCOME

The client gained ongoing visibility into their entire deployed fleet — status, errors, and usage — plus the ability to push updates remotely and securely, turning what would otherwise be a "wait for the customer to call" support model into one where problems and update needs can be seen and acted on proactively.

Embin Technologies Pvt. Ltd.

Unit 507, Sarita B, Prabhat Industrial Complex,
W.E. Highway, Dahisar (E), Mumbai – 400 068, India

www.embin.com
contact@embin.com