NEURAL IMPLANTS · PATIENT CARE · ENTERPRISE SECURITY

Hope, Wired In

How connected neural devices can transform patient care, and why securing them is an enterprise investment



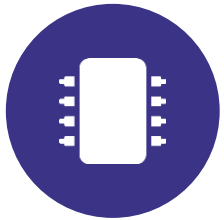
Praveen Sharma · Director, Cyber Range Center, Salem State University

Meet Maria: why this story matters



Before

Parkinson’s tremor takes away simple daily tasks; medication helps less each year



Therapy

Deep brain stimulation delivers gentle pulses to precise targets in the brain



After

She holds a cup steadily again. Quality of care means dignity

Maria is an illustrative composite patient, not a real case.

Neural implants are already therapy



Deep brain stimulation

Parkinson’s disease and movement disorders: calms the signals that cause tremor



Responsive neurostimulation

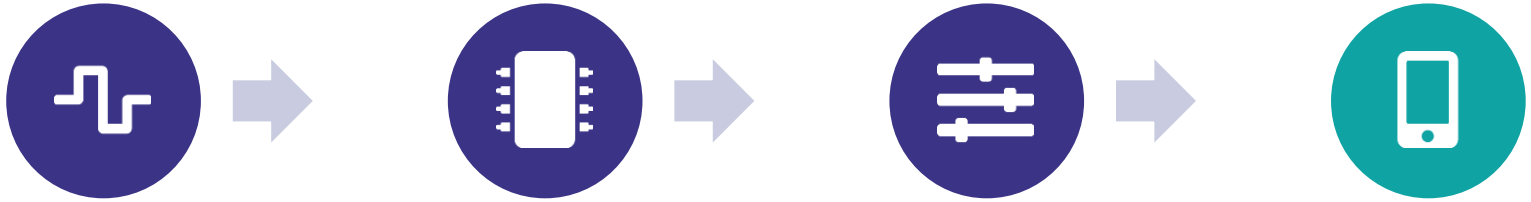
Epilepsy: detects early seizure activity and responds before it spreads



Spinal cord stimulation

Chronic pain: helps patients return to work, sleep and family life

From stimulators to systems



Sense

Read signals from brain or spine

Analyze

Interpret patterns on the device

Adjust

Tune therapy in real time

Share

Connect to apps and wearables

A closed loop: the implant now behaves like a small computer inside the body, connected to the world outside.

What connected care could unlock



Personalized therapy

Tuned to each patient’s own signals



Remote monitoring

Spot problems before they become emergencies



Fewer long trips

Less travel to specialist clinics



Better research

New insight into how these conditions behave

Benefits the technology is designed to deliver; outcomes vary by device and patient.

How secure are these devices, really?



“If I were a patient, I’d want to make sure that the privacy of my thoughts is being protected by design.”

Kevin Fu, security researcher, who tests medical devices in his “torture chamber”

Can an implant read your thoughts?



The P300 brain wave

A common signal that effectively measures surprise, such as recognizing a face. In theory, it could turn an implant into a rudimentary lie detector.



Today: coarse-grained

A grainy black-and-white photo, or an old phonograph



Not today: thought-reading

No high-definition movie of what you are thinking

Not reading thoughts, but revealing something about them

Source: Kevin Fu, in "Neural Implants Bring Hope for Treatment, But Pose New Cybersecurity Headaches"

From one bit to megabytes: the fidelity is rising



"Once we reach that point of really high-fidelity data, it's going to be too late to design the controls then."

No single threshold: the change is gradual

Source: Kevin Fu, in "Neural Implants Bring Hope for Treatment, But Pose New Cybersecurity Headaches"

Today’s risks are already real



A Bluetooth flaw

Could expose intimate details of a patient’s health and daily life



Wider attack surface

Apps, wearables and internet links add more doors to try



A long device life

Weaknesses found years later cannot be fixed by swapping hardware

For a health system: disrupted therapy, lost patient trust and regulatory exposure

Cognitive data: a new protected class?



Protected today

Health data: diagnoses, records and test results, under rules such as HIPAA



Emerging question

Cognitive data: signals about brain activity itself; a few U.S. states now treat neural data as sensitive

Act now: treat neural data as your most sensitive class, with clear rules for access, retention and sharing

Engineering within tight limits



Battery

Replacing it can mean surgery



Size

Everything must fit inside the body



Reliability

Failure can harm a patient



Patient burden

Charging and connections fall on patients

The trade-off: wireless links and strong security need power and add complexity, so they must be designed in, not added later

Secure by design starts with threat modeling



Model threats

Required by FDA for premarket approval



Design controls

Build protection into the device



Update safely

Firmware updates over 5–10 years, no device swap

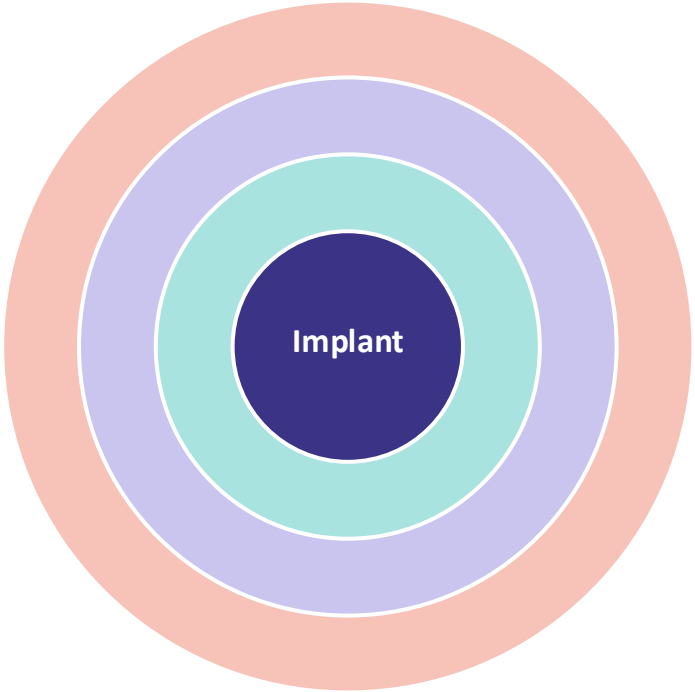


Re-assess

Agile models that change as threats change

Ask every vendor: how long will this device receive security updates, and how will they reach patients safely?

Every connection widens the attack surface



- Controller and app
- Clinician programmer and hospital network
- Cloud and internet

Most attacks start in the outer rings: phishing, stolen credentials and unpatched laptops, risks hospitals already know how to manage

The investment tension



Clinical trials and speed to market

Prove clinical benefit, satisfy regulators, reach patients sooner





Privacy, security and resilience

Protect data, therapy and trust for the life of the device

“I would not be surprised if they’re choosing where to spend their dollars on a clinical trial versus securing privacy.” Kevin Fu

Security as an investment in patient care



People

Clinicians, biomedical engineers and security share ownership, with one accountable leader



Process

Procurement requires SBOMs and update plans; playbooks treat device events as clinical safety events



Technology

Inventory every connected device, segment the network and monitor continuously

The return: avoided downtime · patient trust · regulatory readiness · confidence to adopt the next breakthrough

Innovation must not outpace protection

1. Build privacy by design into every device decision
2. Treat neural data as your most sensitive information
3. Invest in security as part of the therapy itself



Thank you · Questions?