SOLUTION BRIEF

You cannot scan a device that is attached to a patient.

A hospital network carries infusion pumps, ventilators, imaging systems, patient monitors, lab analysers and diagnostic equipment. Almost none of it will accept an agent. Much of it runs on a validated configuration that cannot be modified without revalidation. Some of it will behave unpredictably if probed, and it is connected to a person.

The result is that the devices with the most direct path to patient harm are the least visible devices in the building, and biomedical engineering and IT security frequently hold two different lists of them.

WHAT MAKES THIS ENVIRONMENT DIFFERENT

Patient safety is the security outcome
Availability of a clinical device is not an IT metric. An interruption during a procedure is a patient safety event, which is why active techniques are not available in this environment.

Ownership is split
Biomedical engineering owns the devices, IT owns the network, and security is accountable for the risk. Any useful inventory has to be one all three can agree is accurate.

Regulated devices cannot simply be patched
Manufacturer-controlled configurations mean the standard remediation path is often unavailable, so knowing exactly what is exposed and how it is reachable matters more than a severity list.

The estate arrives continuously
Devices come in through clinical procurement, through trials, on loan and with visiting specialists. A quarterly inventory is out of date on the day it is produced.

WHAT WIRETRACE DOES HERE

WireTrace observes clinical network traffic passively from a SPAN port or TAP. It sends nothing to any device and installs nothing on any of them, so no device is touched, no validated configuration is affected, and no clinical workflow is interrupted. From traffic alone it identifies the connected estate and how it behaves.

Clinical protocols are read for their content rather than classified by port, including **DICOM** imaging exchanges and **HL7** clinical messaging, alongside the enterprise and infrastructure protocols the same devices use for management, identity and updates. That matters because a clinical device is rarely identifiable from its clinical traffic alone; the picture comes from everything it says.

QUESTION	ANSWERED FROM OBSERVED TRAFFIC
What clinical devices are connected?	A live inventory including devices that no agent reaches and no procurement record captured.
Where does each one sit?	Network position and communication relationships, which is the practical basis for segmenting clinical equipment away from general traffic.
What is it talking to?	Internal systems, management platforms and any external destination, including manufacturer support paths.
Where is it exposed?	Cleartext credentials, weak or expired certificates and reachable management interfaces, observed rather than assumed.
Has behaviour changed?	New relationships or unfamiliar activity for a device whose normal pattern is well established.

Ransomware in a hospital is a patient safety problem before it is a data problem. The practical defence is knowing which devices exist, how they are connected, and which paths would let an infection reach clinical equipment. That is an inventory and segmentation question, and it has to be answered without touching the devices themselves.

WHERE IT IS USED

USE CASE

One inventory three teams accept

Biomedical engineering, IT and security work from the same observed record instead of reconciling a maintenance database against a network scan that was never allowed to run.

USE CASE

Segmenting clinical equipment

Segmentation projects stall because nobody can say what talks to what. Observed relationships give the design a factual basis and then show whether the implemented boundary is holding.

USE CASE

Finding the undocumented arrivals

Loan equipment, trial devices and systems installed by a vendor engineer appear as soon as they communicate, rather than at the next audit.

USE CASE

Managing exposure that cannot be patched

When remediation is not available, compensating control depends on knowing precisely what is exposed and from where. Observation gives that with the evidence behind it.

USE CASE

Evidence for regulated audit

Control evidence accumulates continuously from real communications, which is a stronger position than a point-in-time assessment assembled from interviews.

USE CASE

Investigating without interrupting care

When something looks wrong, the protocol history is already there. Investigation does not require going to a ward and interacting with equipment in use.

DATA HANDLING IN A CLINICAL ENVIRONMENT

Healthcare buyers ask about data handling before they ask about capability, and correctly so. WireTrace runs **entirely on premises** with no cloud dependency, so no clinical network data leaves the hospital. The platform retains understanding of devices and their behaviour rather than the content of clinical traffic, and retention is configurable. The full data handling position is covered in the security and privacy documentation provided during evaluation, which is written for exactly this review.

REGULATORY CONTEXT

Evidence is mapped to the frameworks healthcare organisations are assessed against, including the **HIPAA Security Rule**, **NIST CSF 2.0** and **ISO 27001**, alongside the national frameworks applicable in each market. Each mapping states what can be evidenced from observed communications and what cannot.

Single hospital

Sensors at the points where clinical traffic aggregates, with the platform on site.

Healthcare group

Sensors across sites reporting centrally, giving one estate-wide clinical device picture.

No cloud, ever

Fully self-contained, which removes the data residency conversation entirely.

Start with one clinical VLAN

A scoped assessment needs a mirror port and a short window, and touches nothing. It returns the connected clinical estate on that segment, how it is communicating and where it is exposed. Biomedical engineering is usually the team most surprised by the result.

Book a demo at wiretrace.io/request-demo · or email sales@wiretrace.io