January 19, 2016

An Open Letter to the Healthcare Stakeholder Communities: Safer, Sooner, Together

Leaders of the healthcare stakeholder communities,

We request that you unite with us in a joint commitment to patient safety between the healthcare and cyber security communities.

Healthcare has been evolving for thousands of years. Care givers' ability to preserve, improve, and extend life has never been greater than it is today. Modern healthcare is the product of systemic improvement through evidence, rigor, and discipline.

The latest medical advances lay at the intersection of patient care and connected technology. Integration of new technology enables innovations that improve patient outcomes, reduce cost of care delivery, and advance medical research. The forefront of modern healthcare brings us personalized and precision medicine, real-time remote diagnostics, and greater patient involvement in their own treatment, among other revolutions.

New technology introduces new classes of accidents and adversaries that must be anticipated and addressed proactively. Remote malicious attackers, software flaws, and privacy concerns are the potential inadvertent side effects of transplanting connected technology into care delivery. The once distinct worlds of patient safety and cyber security have collided. In kind, now is the time for the healthcare and cyber security communities to connect and collaborate toward our common goals.

When the technology we depend on affects public safety and human life, it commands our utmost attention and diligence. Our medical devices command this level of care. We entrust our lives and the lives of those we love to medical devices in our times of greatest need, and in some cases every day.

The goal of our outreach effort is to catalyze greater teamwork between the cyber security and the healthcare communities *for the benefit of patients*. Our combined expertise will ensure that the consequences of connected technologies are treated with the same diligence as other classes of patient safety issues.

Will you join us in this endeavor to become safer, sooner, together?

The Hippocratic Oath is a symbolic attestation by physicians to provide care in the best interest of patients. Medical devices are key instruments of delivering this care. It stands to reason that the design, development, production, deployment, use, and maintenance of medical devices should also follow this symbolic spirit. What follows is an attempt to merge shared values of both domains, to achieve safer outcomes sooner, together.

Our Hippocratic Oath for Connected Medical Devices describes commitments to capabilities that preserve patient safety, as well as trust in the process of care delivery itself. The text is written from the perspective of a medical device, though phrased so that anyone in the chain of care delivery may see how it fits their role. The content was developed jointly with leading cyber security researchers and others working in and around the healthcare ecosystem. The capabilities were intended to be objectively defined, lasting, and to allow for adaptation and innovation within each function.

We urge healthcare stakeholders to adopt, develop, enhance, and promulgate these capabilities. Patients, care givers, and others have a right to inform themselves of potential consequences of

treatment options. Manufacturers and others involved in the chain of care delivery may demonstrate their commitment to cyber safety by attesting to the way they fulfil this oath. We commit to help you diagnose and treat cyber safety issues to continue your ability to provide greater patient care benefits with fewer side effects.

Hippocratic Oath for Connected Medical Devices

Further detail and explanation at https://iamthecavalry.org/oath

I will revere and protect human life, and act always for the benefit of my patients. I recognize that all systems fail; inherent defects and adverse conditions are inevitable. Capabilities meant to improve or save life, may also harm or end life. Where failure impacts patient safety, care delivery must be resilient against both indiscriminate accidents and intentional adversaries. Each of the roles in a diverse care delivery ecosystem shares a common responsibility: As one who seeks to preserve and improve life, I must ***first do no harm****.*

To that end, I swear to fulfill, to the best of my ability, these principles.

1. Cyber Safety by Design: *I respect domain expertise from those that came before.* ***I will inform design with security lifecycle, adversarial resilience, and secure supply chain practices****.*
2. Third-Party Collaboration: *I acknowledge that vulnerabilities will persist, despite best efforts.* ***I will invite disclosure of potential safety or security issues, reported in good faith****.*
3. Evidence Capture: *I foresee unexpected outcomes.* ***I will facilitate evidence capture, preservation, and analysis to learn from safety investigations****.*
4. Resilience and Containment: *I recognize failures in components and in the environment are inevitable.* ***I will safeguard critical elements of care delivery in adverse conditions, and maintain a safe state with clear indicators when failure is unavoidable****.*
5. Cyber Safety Updates: *I understand that cyber safety will always change.* ***I will support prompt, agile, and secure updates****.*

We are eager to work with you and to promote your current and future capabilities to the public. These capabilities establish a foundation and serve to catalyze an ongoing collaboration to improve patient care and trust. Given our research and experience to date, we are encouraged to see some early investments toward these capabilities. Technical capabilities will take time to bring to market, valuable policy commitments can begin now. On this journey, the challenges will be many and they will be significant, but together and through collaboration we can rise to meet them. Let's start now.

Respectfully,

I Am The Cavalry, members of the security research community, and concerned citizens

Signatures and instructions on for signing can be found at https://iamthecavalry.org/oath, are solely the opinion of the individual.

⚕ Cyber Safety by Design

> *I respect domain expertise from those that came before.* ***I will inform design with security lifecycle, adversarial resilience, and secure supply chain practices.***

Safe outcomes are the product of systematic intent throughout the device lifecycle; they cannot be left to chance. Those whose lives and livelihoods depend on the reliability of the medical device should be able to evaluate for themselves the extent to which safety is assured - or neglected - in its design and development. Greater maturity and consistency in software design, development, testing, and maintenance leads to higher quality, and improved patient outcomes.

- **Cyber security standards based.** Existing International and industry standards for secure design and development of software components are highly mature. Manufacturers who use these can accelerate the security of their software development, baselines, and processes. While there is no single consensus standard, common practices can help mature a program and lay the groundwork for adoption of a preferred standard or framework later.
- **Adversarial resilience analysis.** All other things equal, a component and system that has been more rigorously tested has fewer unknown flaws or defects. Adversarial threat modeling, fault testing, and other cyber security practices build on safety engineering to consider failure and misuse caused by adversaries. Assessments should be carried out by qualified personnel, independent of design and development.
- **Avoid unmitigated remote access.** Capabilities to save lives in the hands of qualified caregivers, can put life at risk when guided by accident or adversaries. Non-unique credentials (passwords, keys, etc.) and undisclosed access may allow untrusted commands, information, or individuals to influence treatment. Open, remote access may facilitate widescale harm from accidents and adversaries. Where such exposures must exist, mitigations must also exist to prevent harm.
- **Supply chain rigor.** Well-governed, traceable hardware and software supply chains establish predictable quality and provenance of device components. A more trustworthy supply chain enables better resilience and a more agile response to accidents and adversaries. Off-the-shelf hardware and software, acquired with appropriate rigor, can increase reliability, reduce cost, and speed time to market compared to other alternatives.
- **Avoid known flaws.** Avoid third-party software components with known vulnerabilities when less vulnerable alternatives are available and will not compromise required functionality. Consider providing a bill of materials for third-party software packages, including their versions, so stakeholders can make their own risk decisions, even beyond the expected lifetime of the device.
- **Shared responsibilities.** The outcome of any course of treatment is a union of the device's inherent capabilities, the care giver's operation in its environment. The best care possible is achieved when the device and operator do what each is best poised to do. In the absence of clear statements of design assumptions and expectations for care delivery, the ability of care givers to replicate assumed environments and processes will be fortunate coincidence, rather than inherently systemic. Communicate expected deployment conditions, known failure conditions, operational requirements, design assumptions, architectural elements, reference implementation guidance, specific warnings or prohibitions, and other considerations.

⚕ Third-Party Collaboration

> *I acknowledge that vulnerabilities will persist, despite best efforts.* ***I will invite disclosure of potential safety or security issues, reported in good faith.***

Software flaws identified before they become safety issues give defenders an advantage. Manufacturers with the capability to receive and investigate flaws quickly increase this advantage. Those who encourage and act on reporting from independent sources can also reduce cost and exposure beyond what is possible with internal review alone. Value from researcher-manufacturer collaborations has led to manufacturers incentivizing research via recognition and reward programs.

- **Standards based**. Published policies and programs in the software industry can serve as effective examples for medical device manufacturers. Use of vetted standards (such as those in the FDA Consensus Standards, including ISO 30111 and ISO 29147) and practices accelerate an organization's maturity and ensure predictable, normalized interfaces to those who report issues.
- **Existing mechanisms.** Use of existing processes and structures reduces time to develop an effective program, increases participation, and reduces administrative burden. Processes and policies already in place to accept and respond to reports of safety concerns – such as complaint handling – may also be used to handle reports of potential safety or security issues.
- **Known interfaces.** External vulnerability reporting coordinators have normalized interfaces between manufacturers and third-party researchers. This brokers trust on all sides and reduces effort required.
- **Incentives focused.** Patient safety should be in everyone's best interest. Positive incentives, such as outreach, recognition, and financial incentives, drive earlier, higher quality reporting. This reduces cost, time, and negative perception to eliminate flaws, at the same time gives defenders an edge on adversaries by disrupting their ability to monetize attacks. Negative incentives deny these benefits to patients and to the healthcare ecosystem.

⚕ Evidence Capture

> *I foresee unexpected outcomes.* ***I will facilitate evidence capture, preservation, and analysis to learn from safety investigations***.

Safety investigations and records of device operations give visibility into unexpected outcomes. This evidence can plainly show the sources of error, be they malfunctions, design defects, human error or deliberate attack. Without evidence, causes of adverse events will be opaque and corrective actions will be speculative.

- **Independently reviewable.** Independent reviews of device failure or safety reports allow stakeholders to investigate adverse events in a timely manner, to improve transparency of findings, and to support lines of accountability. Manufacturers should provide guidance to support investigations by healthcare facilities, specialized service providers, researchers, and agencies.
- **Tamper resistant, forensically sound evidence capture.** Mechanisms should provide a legal standard of care for preserving logs and other information about the event, including tamper resistance, tamper evidence, and chain of custody.
- **Privacy sensitivity.** The benefits of safety investigations are intrinsically linked to records that demonstrate the impact of failure. However, these benefits can be realized without creating privacy and surveillance concerns by decoupling security and integrity logs from patient records.
- **Reapplication of knowledge.** Understanding causes of vulnerability, failure and harm are a precursor to addressing them, not the end in itself. Insights must inform all aspects of the medical device and patient care cycles. Share lessons learned with the broader healthcare community where it can improve the public good.

⚕ Resilience and Containment

> *I recognize failure in components and in the environment are inevitable.* ***I will safeguard critical elements of care delivery in adverse conditions, and maintain a safe state with clear indicators when failure is unavoidable.***

Medical devices deliver patient care through an interdependent system of systems. The strength this complexity brings should not put patients at undue risk of harm. Systems must operate safely independent of the operating states of other systems or components. Failures should be apparent, dependent inputs validated, and outputs protected.

- **Minimal elective exposure.** Connectivity can provide critical capabilities to medical devices. It also increases exposure to hazardous conditions and adversaries. Exposure that does not meaningfully improve capabilities adds attack surface. (eg. NFC versus Bluetooth for changing treatments in implantable devices.) As such, more secure and lower cost designs seek to minimize these types of exposure.
- **Isolation and segmentation.** Unexpected or hostile interactions between devices and their environment are more likely to lead to harm than well-understood interactions. A more secure design and implementation seeks to shield components and systems from adversaries or unexpected conditions.
- **Fail safe and visibly.** Failure conditions should not cause undue harm to patients and should clearly indicate that the device is not operating normally. Unexpected modes of operation or known failures should trigger a "fail safe" or "safe mode" that can prevent a failure in one device or software component from spreading. Communicate indications and known conditions of failure to stakeholders.
- **Trusted input.** Tamper resistant, tamper evident techniques safeguard against life-critical decisions or actions from untrustworthy information or instructions (ie. Drug libraries, HL7 codes, treatment plans, etc.), ideally with real-time feedback.
- **Patient record integrity.** Decisions about patient care rely on accurate records of patient history and treatment. These records should be protected against tampering, manipulation, loss, and gaps. Capabilities such as ample storage, confirmation after transfer, integrity validation, and privacy protection allow informed patient care decisions.

⚕ Cyber Safety Updates

> *I understand that cyber safety will always change.* ***I will support prompt, agile, and secure updates.***

Once an issue is known that could affect patient care, a faster response improves care delivery. Software updates are faster and less expensive than hardware replacement; and automated, remote software updates are most efficient. Increases in exposure are compensated for by the speed and scale of addressing flaws or weaknesses that could lead to negative outcomes.

- **Automation and documentation.** Update processes that are more automated and better controlled are less prone to error, delay, malice, misinterpretation, or other issues. Process documentation should outline clear roles and responsibilities for relevant stakeholders and allow development of corresponding processes inside stakeholder groups.
- **Secure update process.** Processes should verify the authenticity and integrity of software updates to prevent adversarial, malicious, or accidental tampering. Remote update capability can give cost, reputational, and speed advantages if implemented in KNOWN good ways.

- **Stakeholder communication.** Communication to stakeholders should be prompt, transparent, and forthright. Manufacturers should notify relevant stakeholders when and where flaws exist, their severity, contents of the update, and instructions for each role. Updates may be exclusively communication about workarounds, warnings, unsafe conditions, labeling, instructions for use, or other relevant information.
- **Support dependency security updates.** Medical device safety depends on the integrity of third-party software dependencies. Patient safety must not be undermined by vulnerabilities in these platforms, nor in applying updates to fix them. Verification processes specific to off-the-shelf software security updates can enable a more agile response.