MITRE

PIONEERING A HEALTHIER FUTURE

MITRE is transforming data into insights to improve the health system and reinvent the healthcare experience.

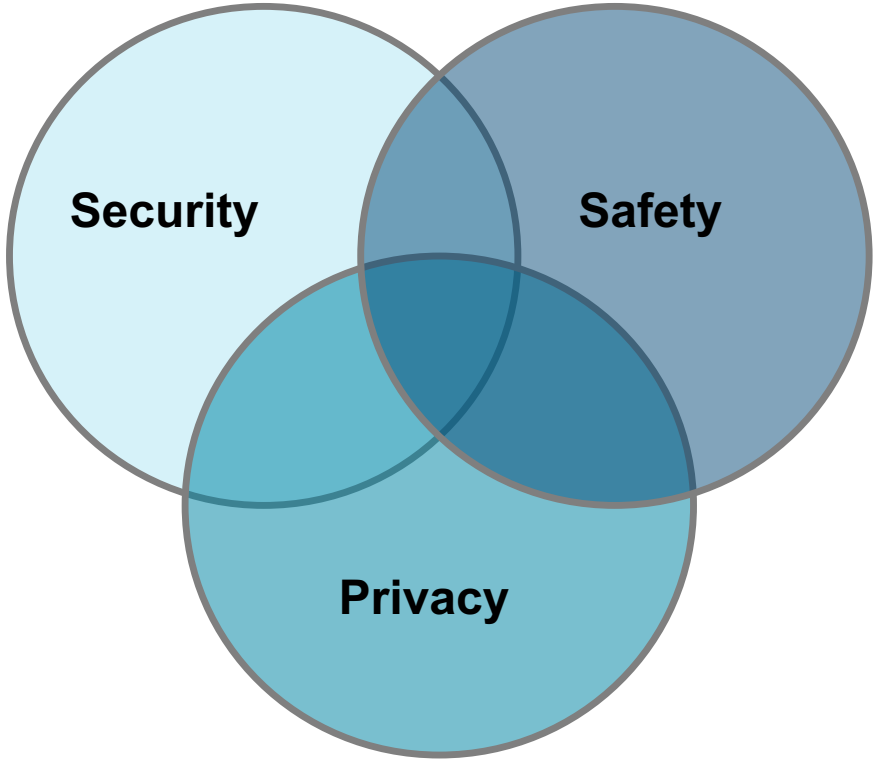
health.mitre.org

Rubric for Applying CVSS to Medical Devices

Penny Chase

Steve Christey Coley

The Delicate Balance of Security, Privacy, and Safety



- **"Everything is a priority"**
- **Varying risks to patient, device, clinical environment**
- **Different regulatory requirements**
- **Different prioritization depending on context of risk assessment**
- **Each can interfere with the other**
  - Don't want anti-virus to fire during surgery
  - Security can erode privacy
- **Our focus: safety and security**

MITRE

Challenges in Scoring Real World Vulnerabilities

- **Can be difficult to determine safety impact of a technical finding**
  - Safety regulations already require separation and indirect defense-in-depth
  - Fail-safe operations
- **Vulnerable applications might not directly interact with physical actions**
  - Depends on the functionality and work/data flow
- **Traditional information technology (IT) often prioritizes integrity and confidentiality over availability**
- **For patient safety, availability is often extremely important**
  - "You can't reboot a patient"
- **The clinical environment varies widely**

MITRE

Hospira LifeCare PCA3 and PCA5 Infusion Pump

- **Technical vulnerability(ies)**
  - Remote telnet root access without password
  - CVSSv2: 10.0 (ICS-CERT)
- **Healthcare impact**
  - Change drug libraries, including min/max allowed dosage
  - (unproven?) change actual dosage delivered
- **Defense-in-depth:**
  - Human still needs to manually confirm dosage change
- **Environmental considerations**
  - Pump may be on separate, "trusted" network
  - The vulnerable interface might not even be in use
- **Scoring implications**
  - In a hospital performing due diligence, risk may be minimal
- **References**
  - FDA Safety Communication: https://www.fda.gov/safety/medwatch/safetyinformation/safetyalertsforhumanmedicalproducts/ucm446828.htm
  - ICS-CERT Advisory: https://ics-cert.us-cert.gov/advisories/ICSA-15-125-01B

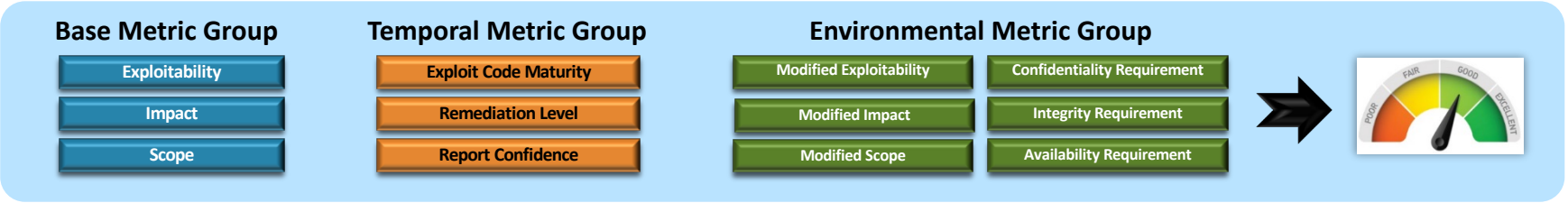
Image from: https://www.hospira.com/en/products_and_services/infusion_pumps/Lifecare

MITRE

Desired Features for a Healthcare Vulnerability Scoring System

- **Minimal complexity**
- **Usable by – and meaningful to – healthcare practitioners**
- **Accepted by diverse stakeholders**
  - Manufacturers, hospitals, security researchers, patients, regulators
- **Flexible for different clinical environments**
- **Flexible for different device classes**
- **Repeatable, reproducible**
- **Validated**
- **Provide common "language" for centering discussion and keeping disagreements focused**

Common Vulnerability Scoring System (CVSS)



- **CVSS is an open framework developed by the Forum of Incident Response and Security Teams (FIRST) for communicating the characteristics and severity of software vulnerabilities**
  - Base Metric Group: vulnerability's intrinsic qualities
  - Temporal Metric Group: vulnerability's characteristics that change over time
  - Environmental Metric Group: vulnerability's characteristics unique to a user's environment
- **Each vector element is assigned a value and a single score is computed as a weighted sum of those values**

MITRE

Approach

- **Established a cross-stakeholder working group: medical device manufacturers, healthcare delivery organizations (HDOs), cybersecurity researchers, FIRST CVSS Special Interest Group, National Cybersecurity Communications & Integration Center (NCCIC), FDA**
- **Reviewed how some manufacturers and healthcare delivery organizations currently use CVSS**
  - Concluded that CVSS is a suitable scoring system, but requires better guidance for use in healthcare settings
- **Developed draft rubric through a series of telcons and email**
- **Conducted initial pilots with manufacturers to validate approach**
- **Submitted a proposal to FDA to qualify as a Medical Device Development Tool (MDDT) and asked to submit a pre-qualification package**
  - A previously validated, scientific tool for use in regulatory decision-making

CVSS Rubric and Extended Vector for Medical Devices

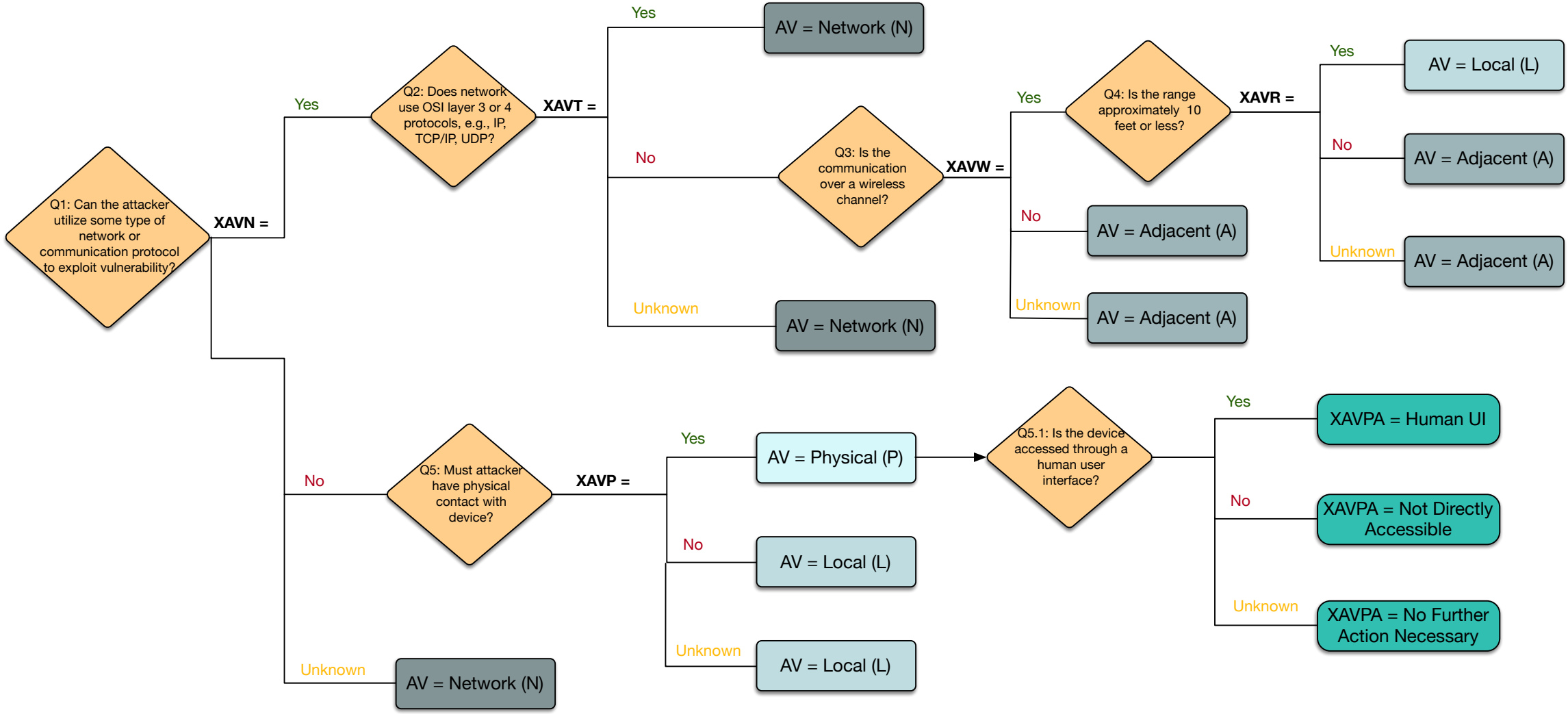
- **The rubric is structured as a series of questions at various decision points for each vector element, and includes**
  - Customized, HDO-specific guidance that is not included in the original specification
  - Device-specific examples
  - Discussion of difficulties in (1) repeatability of the rubric and/or (2) conformance to the spirit of the original CVSS v3 specification
  - Consideration of many perspectives that would be relevant to a medical device manufacturer or an HDO, including (1) patient safety, (2) patient/clinician privacy, and (3) cybersecurity risk from an enterprise vulnerability-management perspective
- **Extended vector records the decisions behind the CVSS vector element**

Rubric: Base Metric Group (Attack Vector) – Questions

- **Q1 (XAVN). Can the attacker utilize some type of network or communication protocol to exploit this vulnerability? Note: Do NOT consider firewall or other access restrictions for this question (see "Working Group Discussion" section).**
- **Yes: Q2 (XAVT). Does the network use OSI layer 3 or 4 protocols, e.g. IP, TCP/IP, or UDP?**
  - **Yes: AV = "N" (Network)**
    - Whether from the Internet or anywhere within the environment's Intranet
    - If there is any access from at least one Internet location
    - Includes access from third-party networks (e.g. manufacturer systems with access to hospital-internal network)
  - **No: Q3 (XAVW). Is the communication over a wireless channel?**
    - **Yes: Q4 (XAVR). Is the range approximately 10 feet or less?**
      - **Yes: AV = "L" (Local). Attacker is physically close to the victim or target, and is presumed to have implied authorization, using short-range communications such as:**
        - Bluetooth LE
        - Zigbee
        - Inductive communication
        - Near Field Communications (NFC)
      - **No: AV = "A" (Adjacent). Attacker is on wireless channel, possibly with a relatively wide range, e.g. network across an entire physical facility or building.**
        - 802.11b

MITRE

Rubric: Base Metric Group (Attack Vector) – Flow Chart



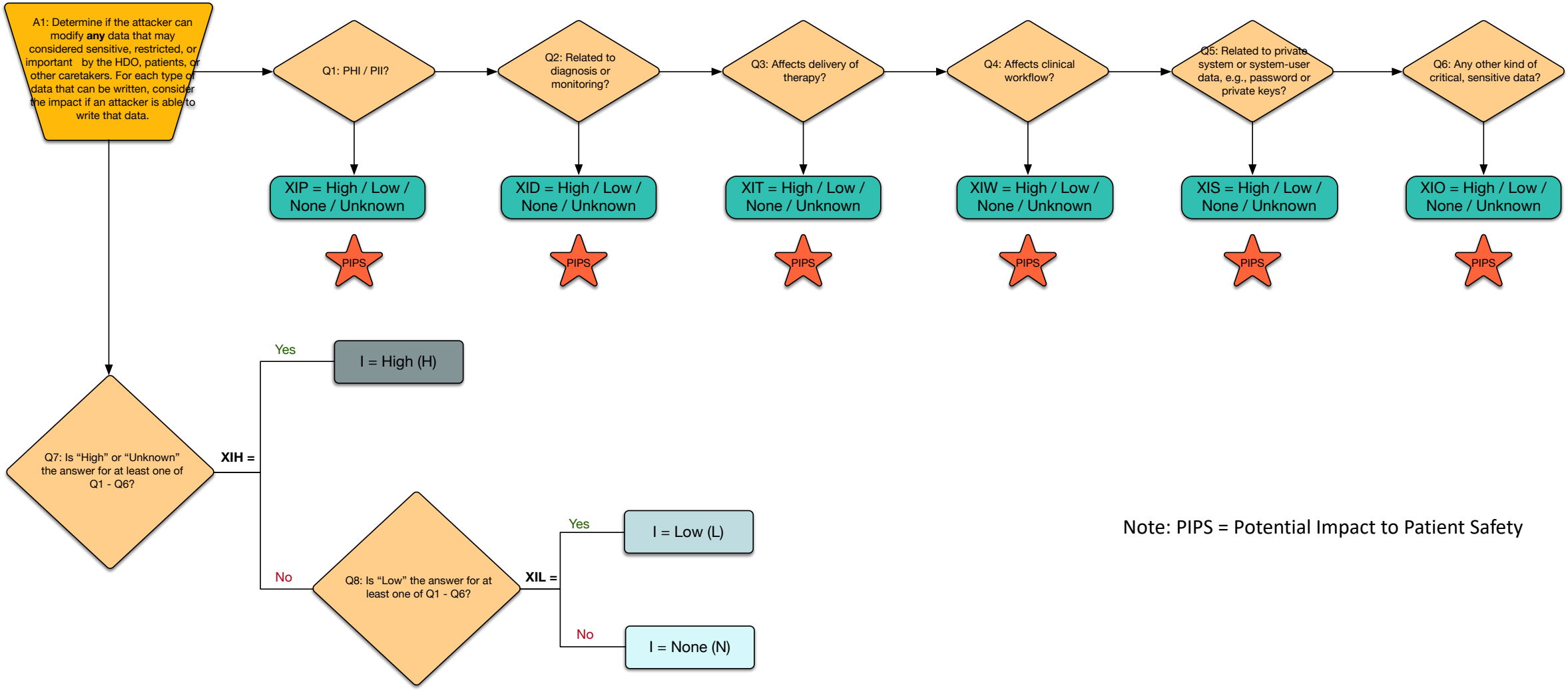
MITRE

Rubric: Base (Attack Vector) – Extended Vector

Question	Element	Values
Q1: Can the attacker utilize some type of network or communication protocol to exploit this vulnerability?	Extended Attack Vector Network (XAVN)	Yes (Y) No (N) Unknown (U)
Q2: Does the network use OSI layer 3 or 4 protocols, e.g. IP, TCP/IP, or UDP?	Extended Attack Vector TCP/IP or UDP (XAVT)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q3: Is the communication over a wireless channel?	Extended Attack Vector Wireless (XAVW)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q4: Is the range approximately 10 feet or less?	Extended Attack Vector Range (XAVR)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q5: Must the attacker have physical contact with the device?	Extended Attack Vector Physical (XAVP)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q5.1: Through an intended human UI?	Extended Attack Vector Physical Access Type (XAVPA)	Human UI Not Directly Accessible No Further Action Necessary

MITRE

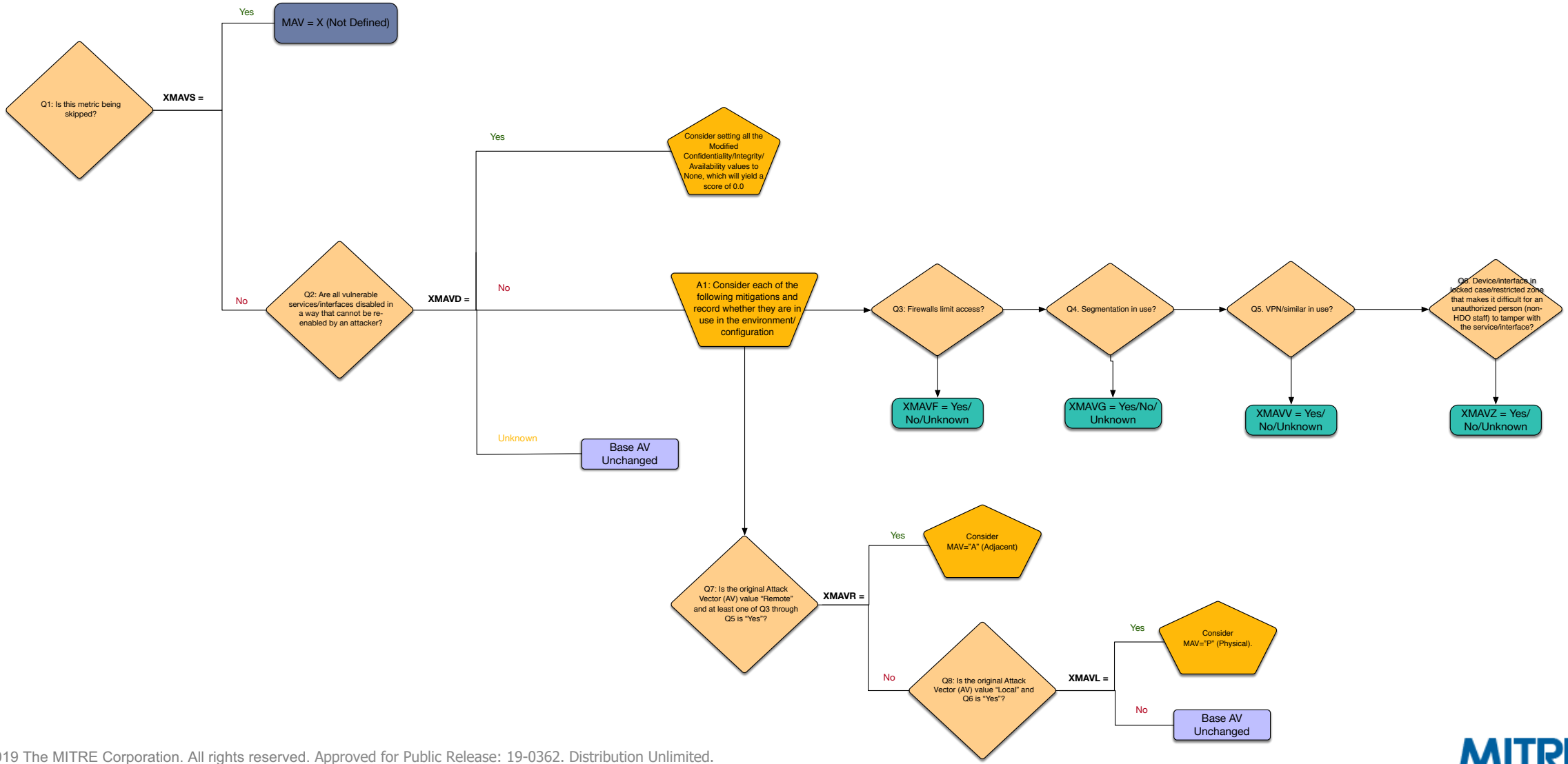
Rubric: Base Metric Group (Integrity Impact)



Note: PIPS = Potential Impact to Patient Safety

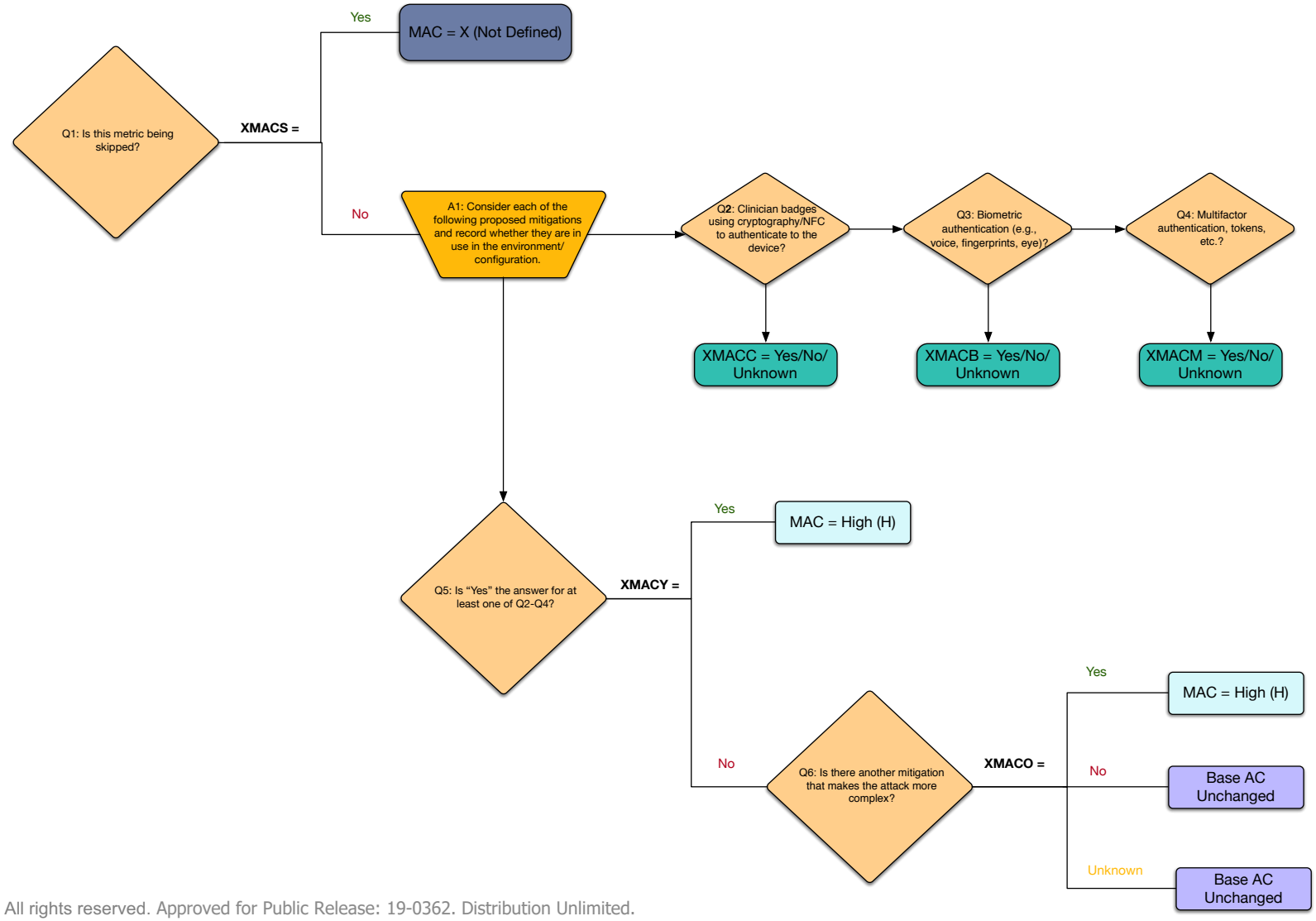
MITRE

Rubric: Environmental Metric Group (Modified Attack Vector)



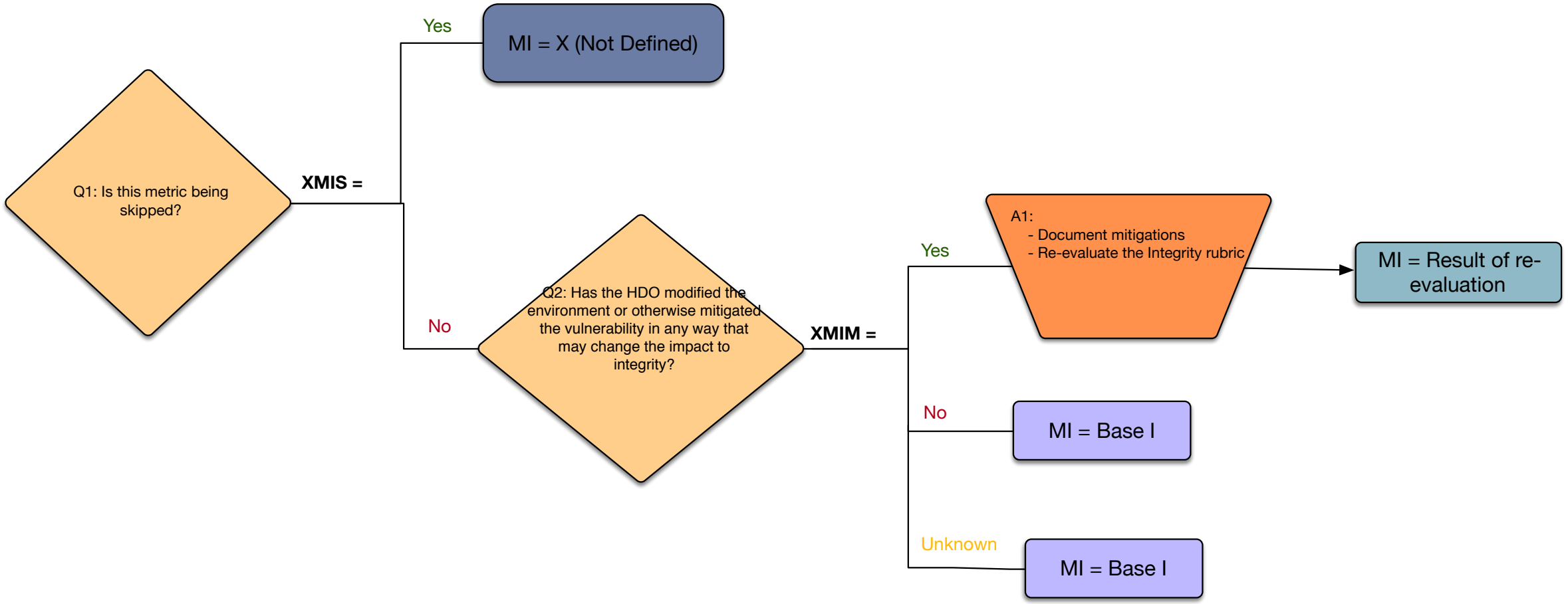
MITRE

Rubric: Environmental Metric Group (Modified Attack Complexity)



MITRE

Rubric: Environmental Metric Group (Modified Integrity)



MITRE

www.mitre.org/md-cvss-rubric

MITRE

Next Steps

- **Develop the MDDT pre-qualification package**
  - Conduct pilots with additional medical device manufacturers to gather additional evidence
    - Demonstrate applicability of rubric to a wider range of devices
    - Assess consistency in scoring
    - Compare rubric vs existing non-rubric scoring process
  - Complete and submit pre-qualification package
- **Develop a calculator**

Presentation Data Rights Notice

NOTICE

This presentation was produced for the U. S. Government under Contract Number HHSM-5000-2012-00008I, and is subject to Federal Acquisition Regulation Clause 52.227-14, Rights in Data-General.

No other use other than that granted to the U. S. Government, or to those acting on behalf of the U. S. Government under that Clause is authorized without the express written permission of The MITRE Corporation.

For further information, please contact The MITRE Corporation, Contracts Management Office, 7515 Colshire Drive, McLean, VA 22102-7539, (703) 983-6000.

MITRE

MITRE

PIONEERING A HEALTHIER FUTURE

MITRE is transforming data into insights to improve the health system and reinvent the healthcare experience.

health.mitre.org

Join us to advance the nation's progress toward an integrated health system with improved access and quality at a sustainable cost.

Learn more at health@mitre.org

pc@mitre.org

coley@mitre.org