Welcome to today's NH-ISAC & MDISS Webinar

Medical Device Vulnerability Intelligence Program for Evaluation and Response (MD-VIPER)

NH-ISAC
NATIONAL HEALTH - ISAC

MDISS
MEDICAL DEVICE INNOVATION, SAFETY & SECURITY CONSORTIUM

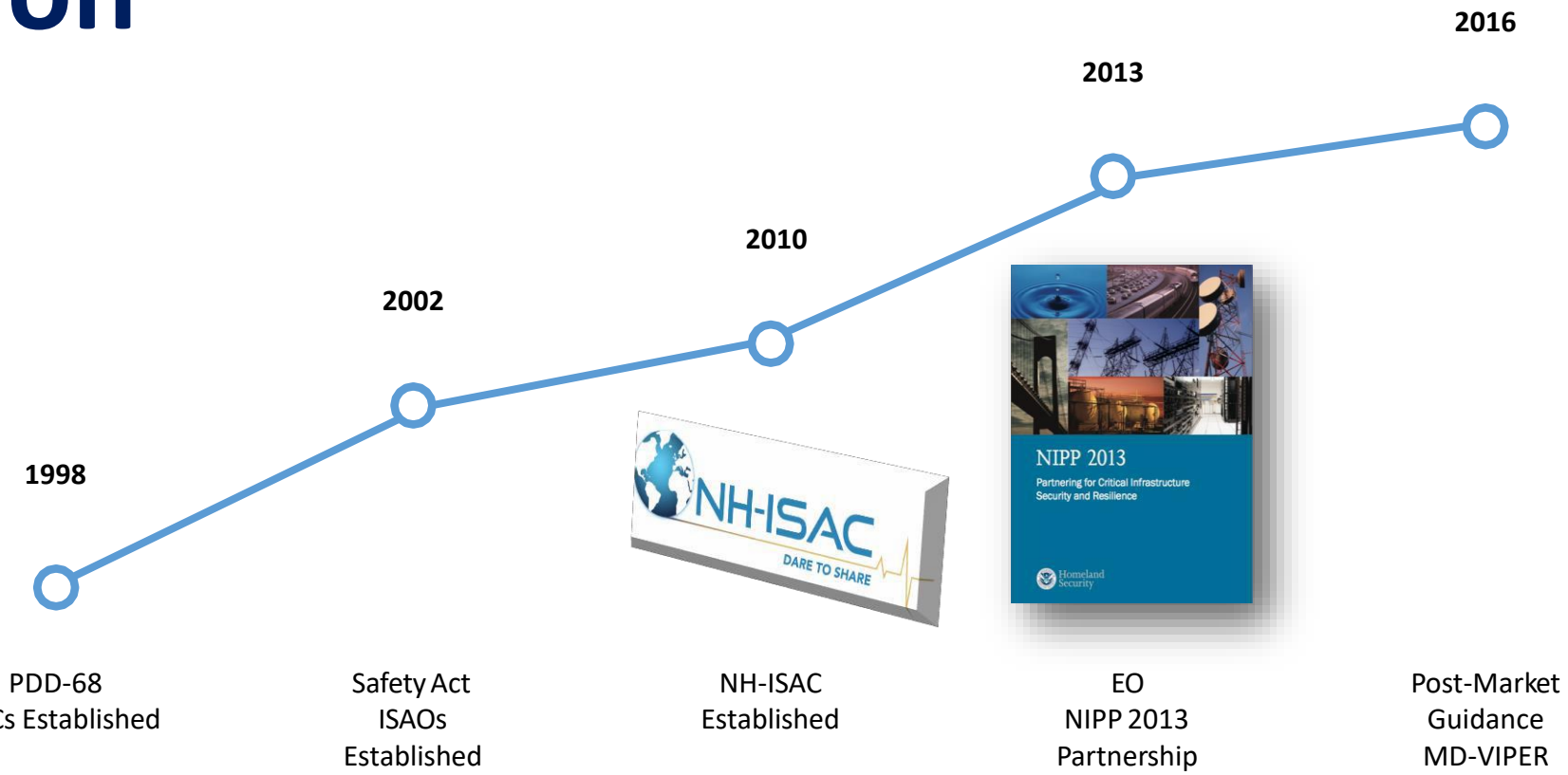
Agenda

Speaker Name	Speaker Institution	Topic
Everyone		• Speaker check- in • Sound check • Recording on
Denise Anderson	NH-ISAC	• NH-ISAC and ISAO • Standardized (ISAO) procedures overview • MOU overview Participation
Jon Crosson	NH-ISAC	• Using the site • Finding help • Reporting process • Event tracking

Dale Nordenberg	MDISS	• MD-VIPER
		  • Description
		  • Attributes
		  • Outcomes

Michelle Jump	Stryker	• Decision to report flow diagram
Steve Abrahamson	GE Health	• Report process flow diagram
Michael McNeil	Philips Health	• Coordinated disclosure
All speakers **Ken Hoyme** **Roberta Hansen** **Steve Grimes**		• QA

Evolution



- The original ISACs are almost 20 years old
- Most ISACs are private sector formed and led
- ISACs are non-profit

NIPP 2013 Glossary

- **Information Sharing and Analysis Centers (ISACs).** Operational entities **formed by critical infrastructure owners and operators** to gather, analyze, appropriately sanitize, and disseminate intelligence and information related to critical infrastructure. ISACs provide 24/7 threat warning and incident reporting capabilities and have the ability to reach and share information within their sectors, between sectors, and among government and private sector stakeholders. (Source: Presidential Decision Directive 63, 1998)
- **Information Sharing and Analysis Organization (ISAOs).** Any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of:
- (a) Gathering and analyzing
- (b) Communicating or disclosing
- (c) Voluntarily disseminating

Appendix A – National Partnership

Information Sharing and Analysis Organizations

Several private sector information sharing and analysis organizations have been established in the last decade. **ISACs are examples of successful information-sharing organizations.**

ISACs – ISACs serve as operational and dissemination arms for many sectors and subsectors, and facilitate sharing of information between government and the private sector. ISACs work closely with SCCs in the sectors where they are recognized. They are designed to provide in-depth sector analysis and help coordinate sector response during incidents, including information sharing within sectors, between sectors, and among public and private sector critical infrastructure stakeholders. Government agencies also may rely on ISACs for situational awareness and to enhance their ability to provide timely, actionable data to targeted entities.

Call to Action

Memorandum of Understanding **(MOU)**
October 2016
FDA & NH-ISAC & MDISS

- Create an environment that fosters **stakeholder collaboration and communication**
- Develop timely awareness of the Framework for Improving Critical Infrastructure Cybersecurity **(NIST CSF)**
- Develop innovative strategies to **assess and mitigate** cybersecurity vulnerabilities before hazard
- Build a **foundation of trust** within the HPH community
- Establish a mechanism by which information regarding **cybersecurity vulnerabilities and threats can be shared**

NH-ISAC

- **Founded in 2010**

Sharing Community
Intelligence and Alerts
Newsletter
Exercises
Webinars/Threat Calls
Conferences & Workshops
White Papers
Working Groups/Committees
Tools – Symphony, Soltra, Brightpoint
Playbook & Threat Level
CyberFit
Special Interest Groups

MDSISC

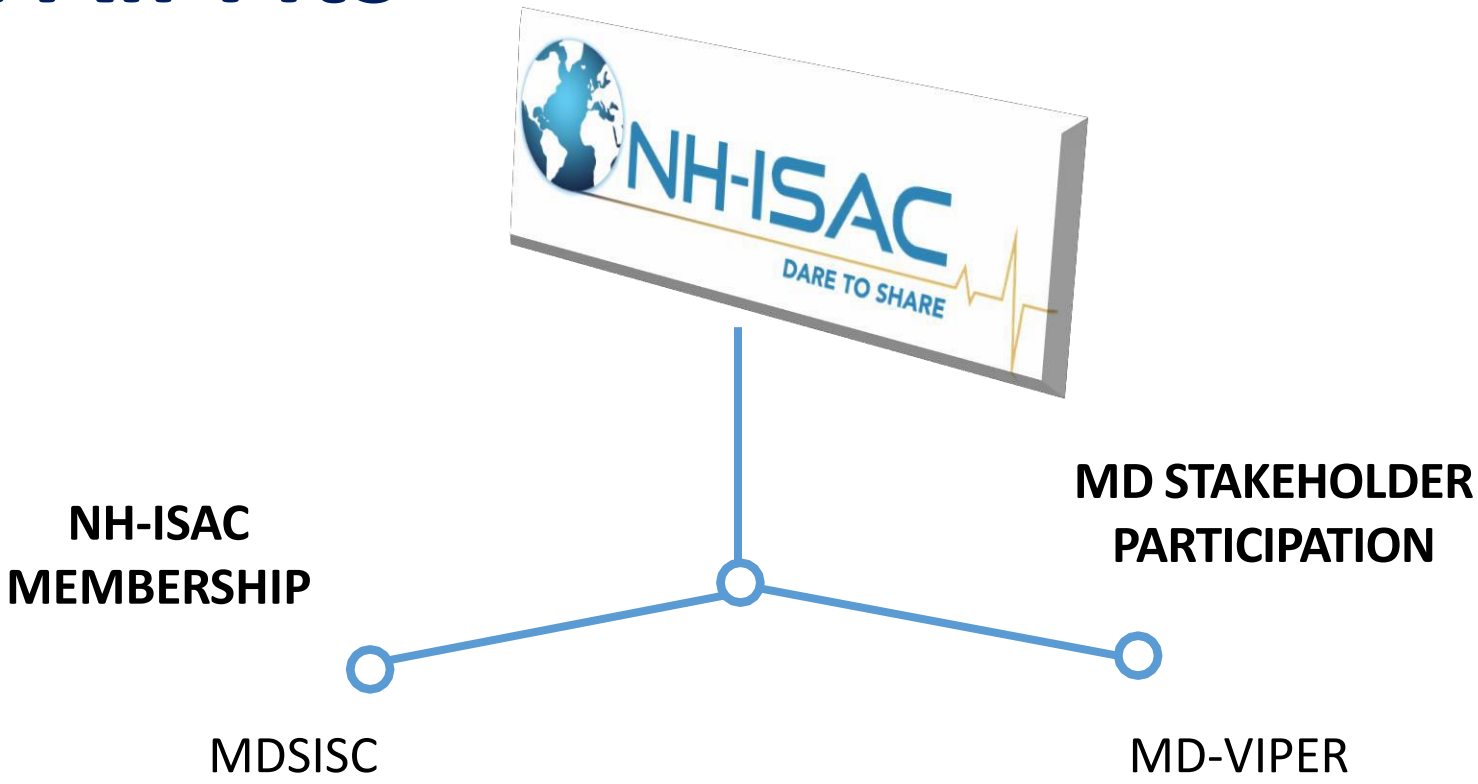
- Listserver to share and exchange information
- Monthly meetings
- Threat briefings
- White papers on threats and best practices
- Medical device track at NH-ISAC fall & spring summits
- Medical device security workshops

Participation in MD-VIPER

- Open to all medical device security stakeholders
- Free and voluntary*
- Tracking each event (submissions, data sharing event, communication event, etc.)
- Each event is triggered by the manufacturer
- Collaboration with manufacturer
- Responsible sharing of information regarding vulnerabilities and threats in light of specified vulnerabilities for stakeholder awareness

**Need to register and sign NDA*

How It All Fits

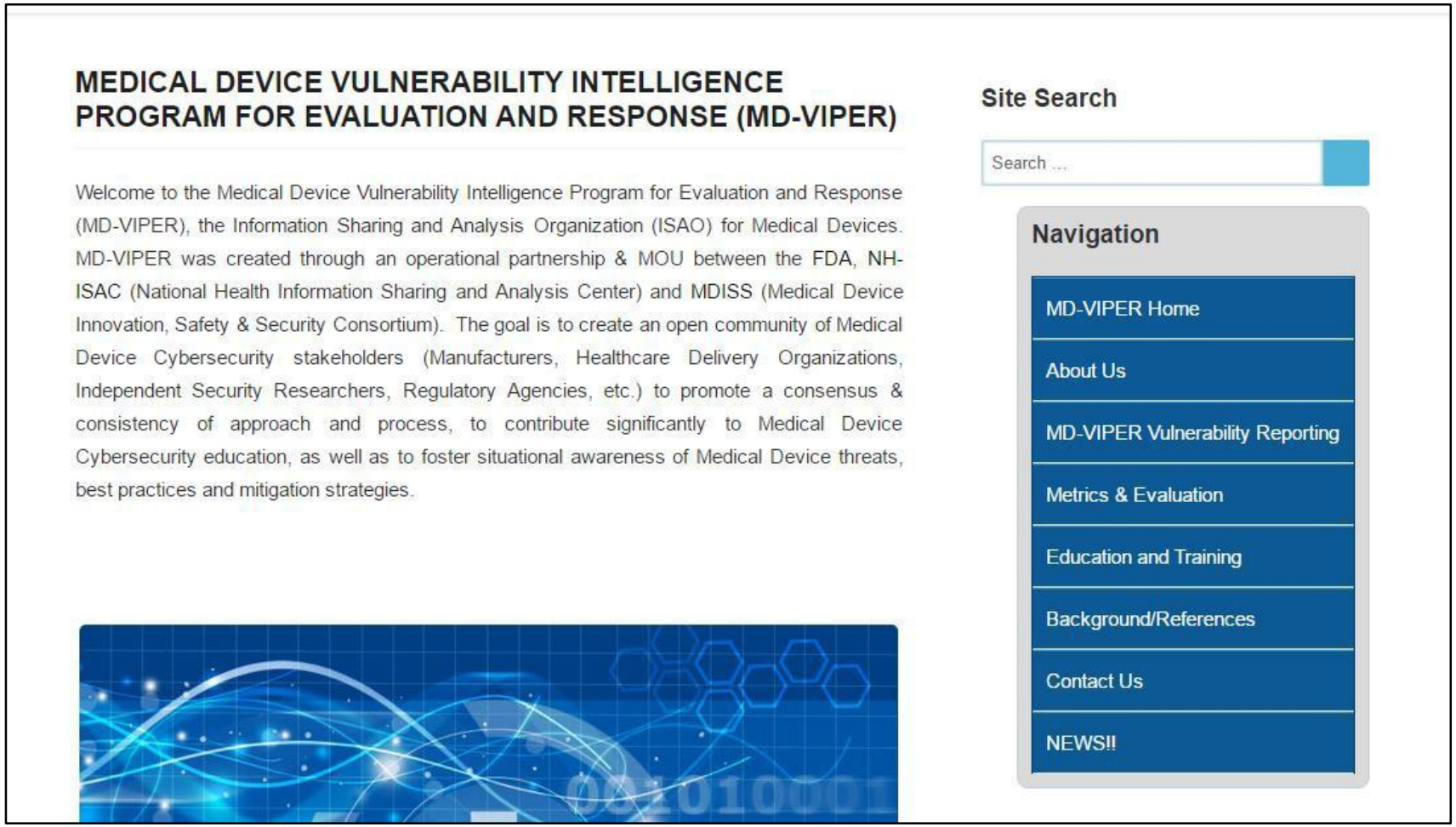


- NH-ISAC Membership is dues based and open to organizations that meet membership criteria.
- MDSISC is a special interest Council under the NH-ISAC co-led by MDISS. Open to NH-ISAC and MDISS members..
- MD-VIPER is a NH-ISAC /MDISS initiative open to medical device security stakeholders.

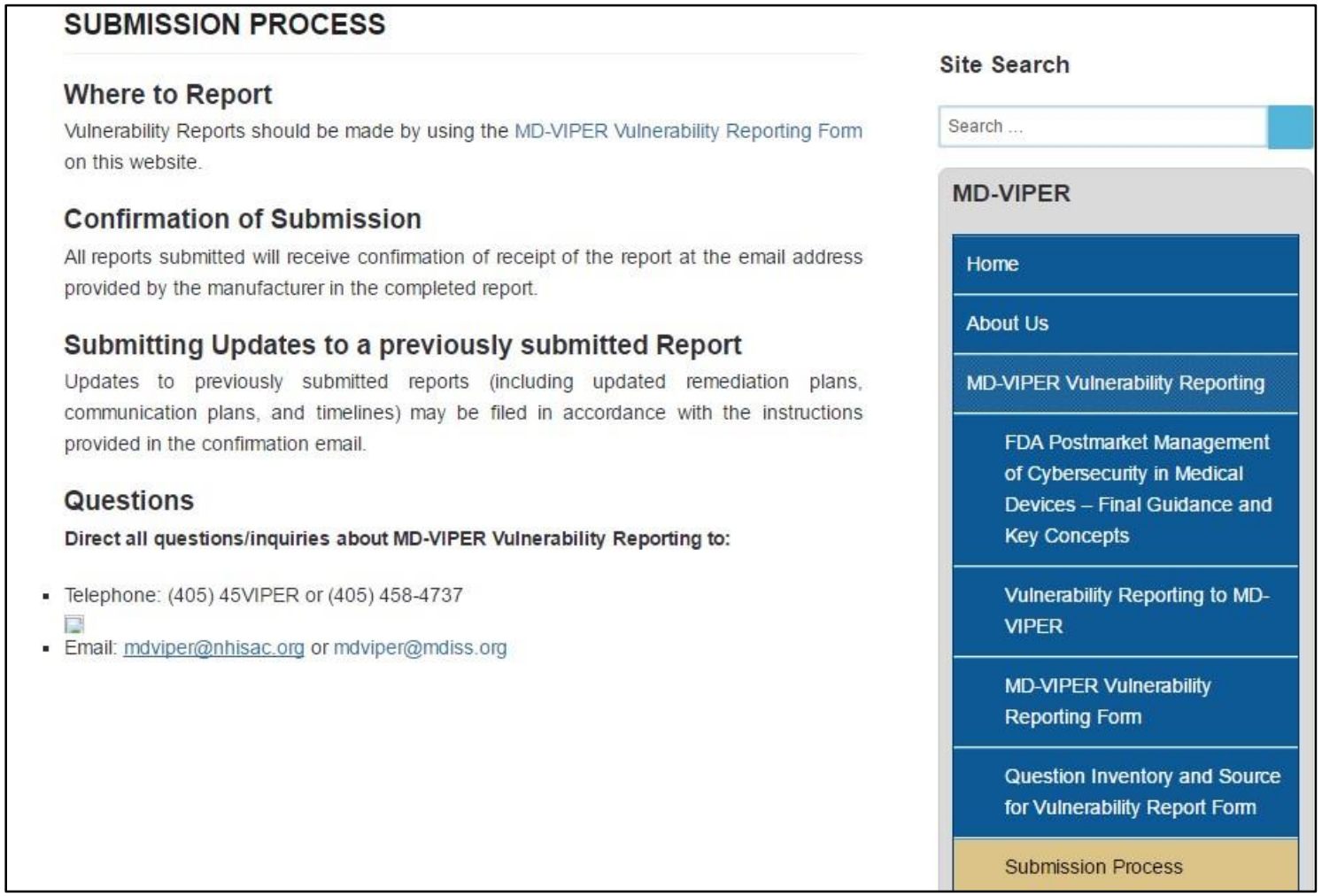
MD-VIPER

- Goal:
  - A medical device vulnerability sharing evaluation and response service
  - Support FDA Postmarket Cybersecurity in Medical Devices Guidance
  - Create open community of Medical Device Cybersecurity stakeholders
  - Promote a consensus & consistency of approach and process
  - Contribute to Medical Device Cybersecurity education and understanding
  - Foster situational awareness of medical device threats, best practices and mitigation strategies

MD-VIPER Site Information



MD-VIPER Submission Process



SUBMISSION PROCESS

Where to Report

Vulnerability Reports should be made by using the MD-VIPER Vulnerability Reporting Form on this website.

Confirmation of Submission

All reports submitted will receive confirmation of receipt of the report at the email address provided by the manufacturer in the completed report.

Submitting Updates to a previously submitted Report

Updates to previously submitted reports (including updated remediation plans, communication plans, and timelines) may be filed in accordance with the instructions provided in the confirmation email.

Questions

Direct all questions/inquiries about MD-VIPER Vulnerability Reporting to:

- Telephone: (405) 45VIPER or (405) 458-4737
- Email: mdviper@nhisac.org or mdviper@mdiss.org

Site Search

Search ...

MD-VIPER

- Home
- About Us
- MD-VIPER Vulnerability Reporting
  - FDA Postmarket Management of Cybersecurity in Medical Devices – Final Guidance and Key Concepts
  - Vulnerability Reporting to MD-VIPER
  - MD-VIPER Vulnerability Reporting Form
  - Question Inventory and Source for Vulnerability Report Form
  - Submission Process

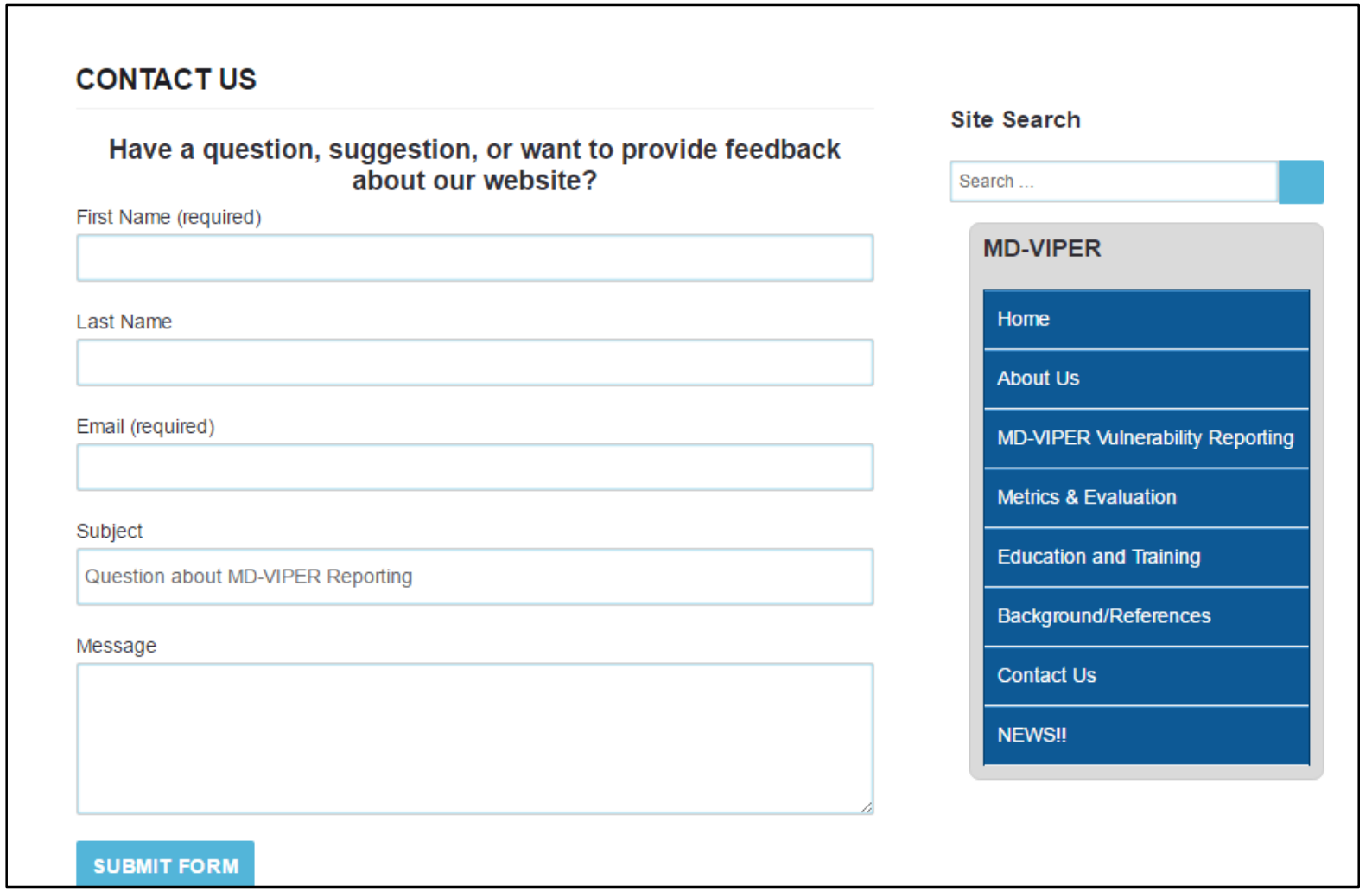
MD-VIPER Reporting Process

- Vulnerability reporter contacts MD-VIPER
- Conversation between reporter and MD-VIPER
- Reporter proceeds with sharing of vulnerability
- Once reported, all data is stationary until a data owner, manufacturer, advises in writing to share the data
- If a third party (non-manufacturer) shares the vulnerability data then
  - Information is shared with the manufacturer. they should be able to advise us, in writing, to share the data
  - Reporter directed to the manufacturer website and coordinated disclosure process
  - If needed, MD-VIPER will facilitate the connection between reporter and the manufacturer

MD-VIPER Event Log Tracking (Draft)

EVENT#	DATE	COMPANY	POC NAME	PHONE NUMBER	EMAIL	PURPOSE OF EVENT	FOLLOW UP ACTION

MD-VIPER Feedback



Vulnerability Information Sharing* in Support of FDA Guidance

System Description

- Medical device vulnerability information sharing system
- Based on 21 CFR 806 reporting processes
- Web-based system
- Current submission of vulnerability information is via secure unloadable PDF file
- Vulnerability information will be shared by manufacturer with MDVIS after it has evaluated the vulnerability
  - *MDVIS may assist in connecting third parties with manufacturers, if needed, to help ensure vulnerabilities are evaluated appropriately before sharing.*
- All vulnerability information shared with MDVIS will be embargoed until coordinated disclosure is executed by manufacturer, ICS-CERT and FDA

*This work is executed under Memorandum of Understanding (MOU) 225-16-024 between FDA, NHISAC and MDISS; Published October 06, 2016

Vulnerability Information Sharing* in Support of FDA Guidance

Key Attributes

- Collaboratively developed service
- Introduces new type of initiative
  - Cybersecurity-related content
  - Reporting guidance
- Familiar process and format for reporting
- Coordinate processes, e.g. ICS-CERT and coordinated disclosure
- Public health best practices
- Service driven
- Scientific foundation
- Safety and privacy impact

*This work is executed under Memorandum of Understanding (MOU) 225-16-024 between FDA, NHISAC and MDISS; Published October 06, 2016

Vulnerability Information Sharing* in Support of FDA Guidance

Key Outcomes

- Improve understanding of vulnerabilities in medical devices
- Improve stakeholder community's solution development work
- Harmonize best practices for device security information sharing
- Improve efficiency to market while improving security, safety and privacy profiles for devices and associated networks

*This work is executed under Memorandum of Understanding (MOU) 225-16-024 between FDA, NHISAC and MDISS; Published October 06, 2016