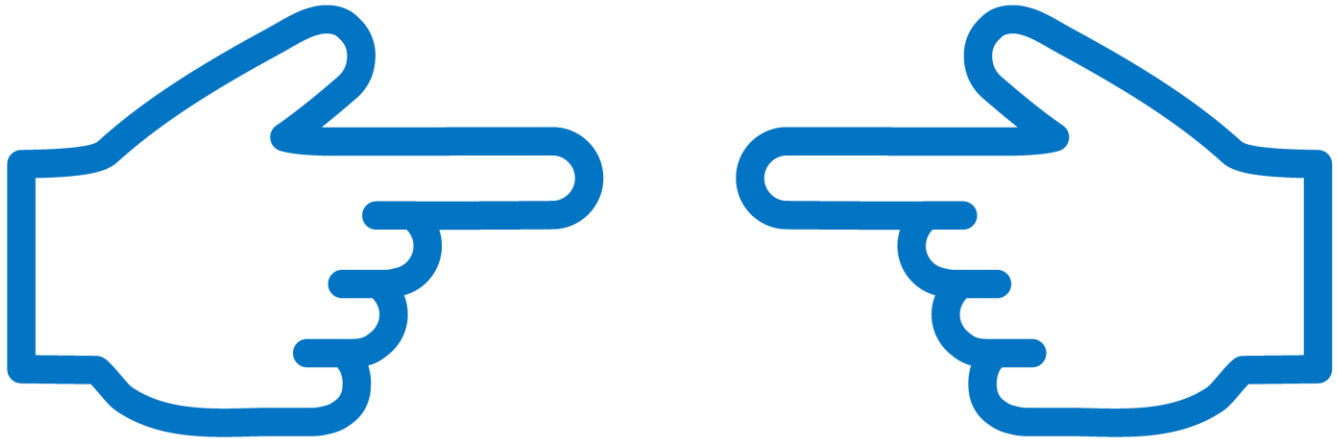
INCOSE
Healthcare Working Group
4th Annual Systems Engineering in Healthcare Conference

A Shared Responsibility

Securing Connected Medical Devices

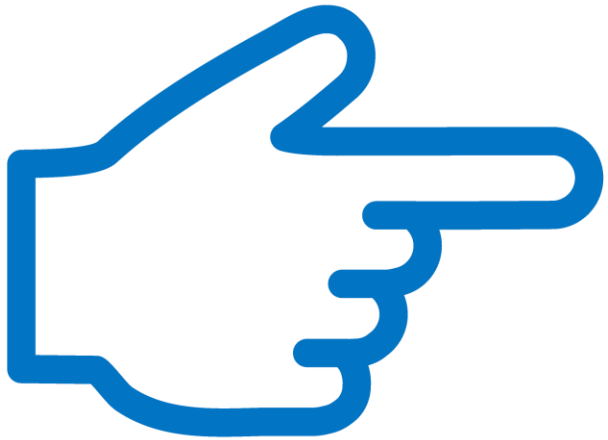
Copyright © 2018 by DigiCert.
Permission granted to INCOSE to publish and use

Evolution of Responsibility – Finger Pointing



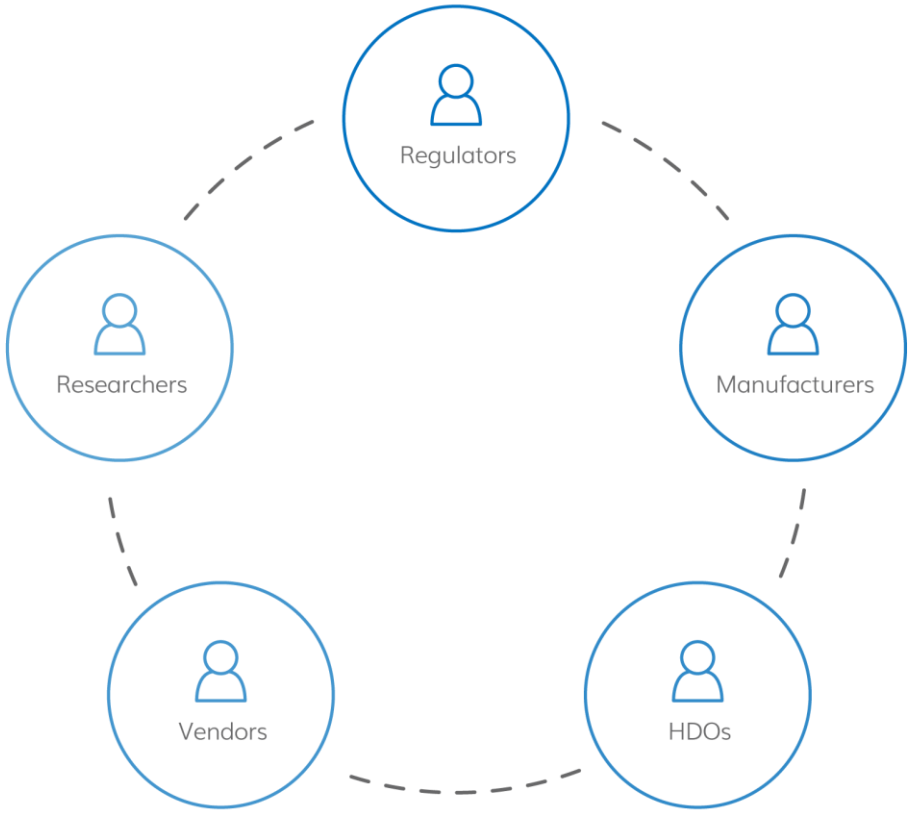
Evolution of Responsibility – Unwillingness

Evolution of Responsibility – Nowhere to be Found



Evolution of Responsibility – Collaboration

Collaboration is Essential to Success



Where Has Healthcare Seen Collaboration

American Health Information Community (AHIC)

Office of the National Coordinator for Health Information Technology (ONC)

American Health Information Community (the Community)

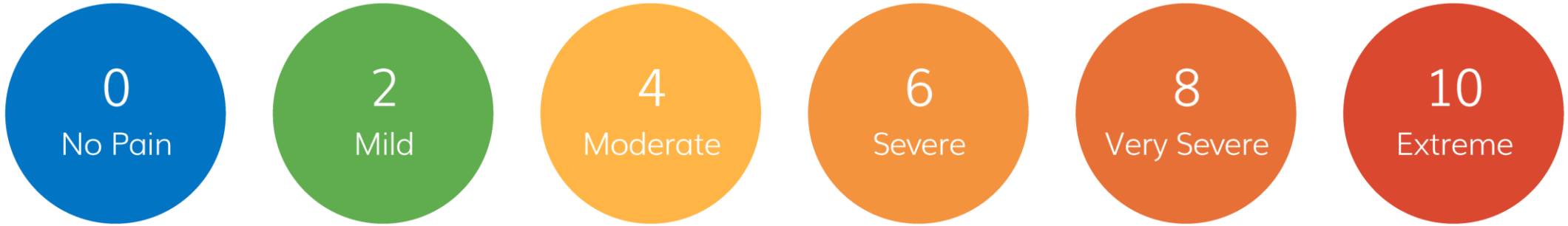
On September 13, 2005, Health and Human Services (HHS) Secretary Mike Leavitt announced t membership for the American Health Information Community (the Community). The Community is being formed to help advance efforts to reach President Bush's call for most Americans to have electronic health records within ten years.

The Community is a federally-chartered commission and will provide input and recommendations to HHS on how to make health records digital and interoperable, and assure that the privacy an security of those records are protected, in a smooth, market-led way.

The Community will have a total of 17 members including Secretary Leavitt who will serve as th Chair. The remaining 16 members selected by Secretary Leavitt represent a combination of key leaders in the public and private sectors. Selected for membership are individuals who represent stakeholder interests in advancing the mission of the Community and who have strong peer support. Members selected to serve include:

- Secretary Michael O. Leavitt

Collaboration is Triggered by Shared Pain



Where is the Pain Being Felt

The biggest healthcare breaches of 2017

Healthcare proved itself a lucrative target for hackers in 2016, and so far 2017 is unfortunately following suit.

December 06, 2017 | 05:59 AM

FDA issues recall of 465,000 St. Jude pacemakers to patch security holes

Heart patients will have to visit their doctors to have their pacemakers patched for the "voluntary" recall -- but there are risks.

By Charlie Osborne for Zero Day | August 30, 2017 -- 10:31 GMT (03:31 PDT) | Topic: Security

MAY 17, 2017 @ 09:00 AM 24,290

The Little Blac

Medical Devices Hit By Ransomware For The First Time In US Hospitals

Thomas Fox-Brewster, FORBES STAFF
I cover crime, privacy and security in digital and physical forms. FULL BIO

Advisory (ICSMA-18-058-01)

Medtronic 2090 Carelink Programmer Vulnerabilities

Original release date: February 27, 2018

Print Tweet Send Share

Advisory (ICSMA-18-037-02)

GE Medical Devices Vulnerability

Original release date: March 13, 2018

Print Tweet Send Share

Responsibility Exercise

Scenario 1

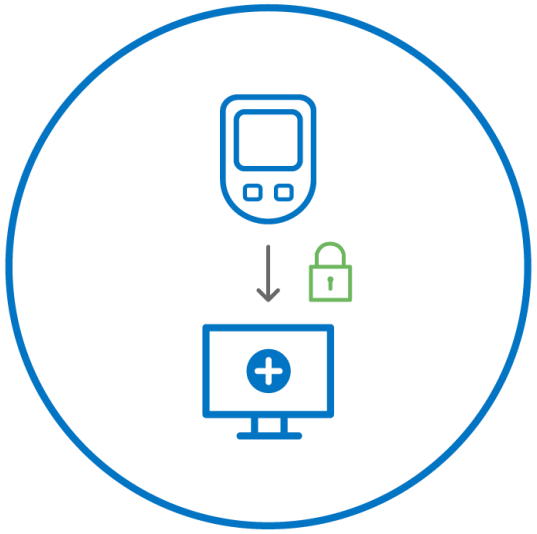
Medical Device Risk Assessment

Scenario 2

Authenticating Device to Network

Scenario 3

Encryption of Data from Device to EHR



Scenario 4

Authenticating Device Updates

Scenario 5

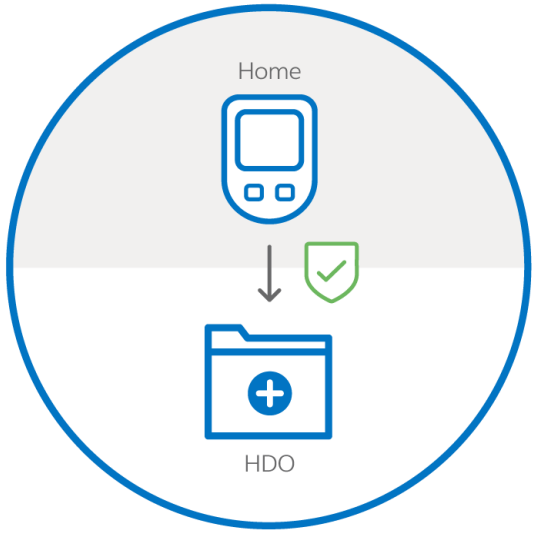
Ensuring the Integrity of Device Updates

Scenario 6

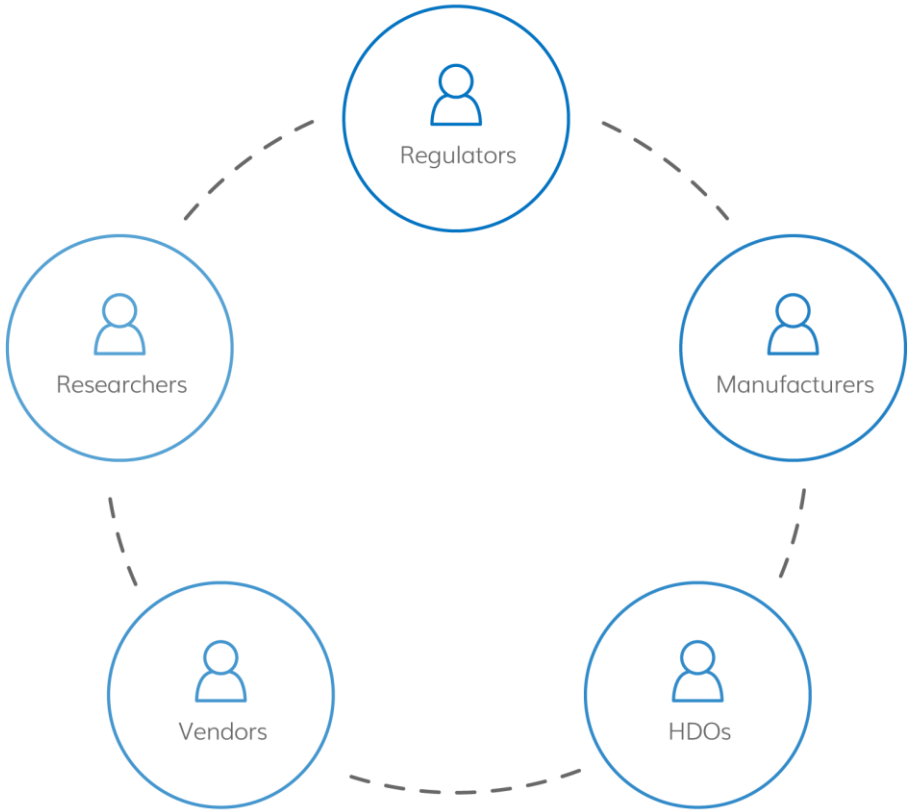
Coordinated Vulnerability Disclosure Policies

Scenario 7

Encryption of Data from Home To EHR



Key Takeaway: Collaboration is Essential to Success



Change is Coming

You can FIGHT change and lose.

You can ACCEPT change and survive.

You can **LEAD** change and prosper.

Mike Leavitt, HHS Secretary 2004-2008

Thank You!

Mike Nelson
VP of IoT Security
(801) 770-1706
mike.nelson@digicert.com

@mike_k_nelson

INCOSE
Healthcare Working Group
4th Annual Systems Engineering in Healthcare Conference

Thank you for attending!

Share your experiences at #HWGSEC