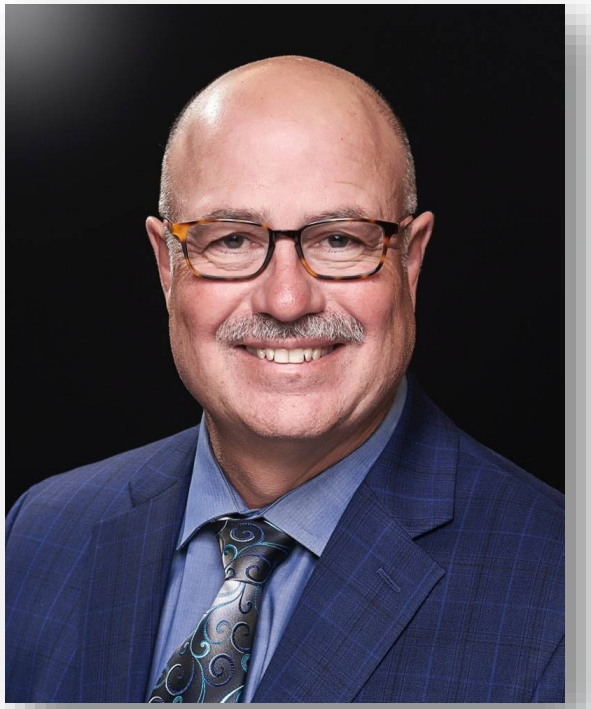
Preparing for your Future: 2021 and Beyond

College of Biomedical Equipment Technology

Committed to Delivering a World-Class Education on Demand

MDEXPO
Tampa, FL • November 8-9, 2020

Preparing for your Future: 2021 and Beyond



William Bassuk
President, College of Biomedical Equipment Technology

Monty Gonzales
Director, College of Biomedical Equipment Technology

John Schmidt
Deputy Director of Education, College of Biomedical Equipment Technology

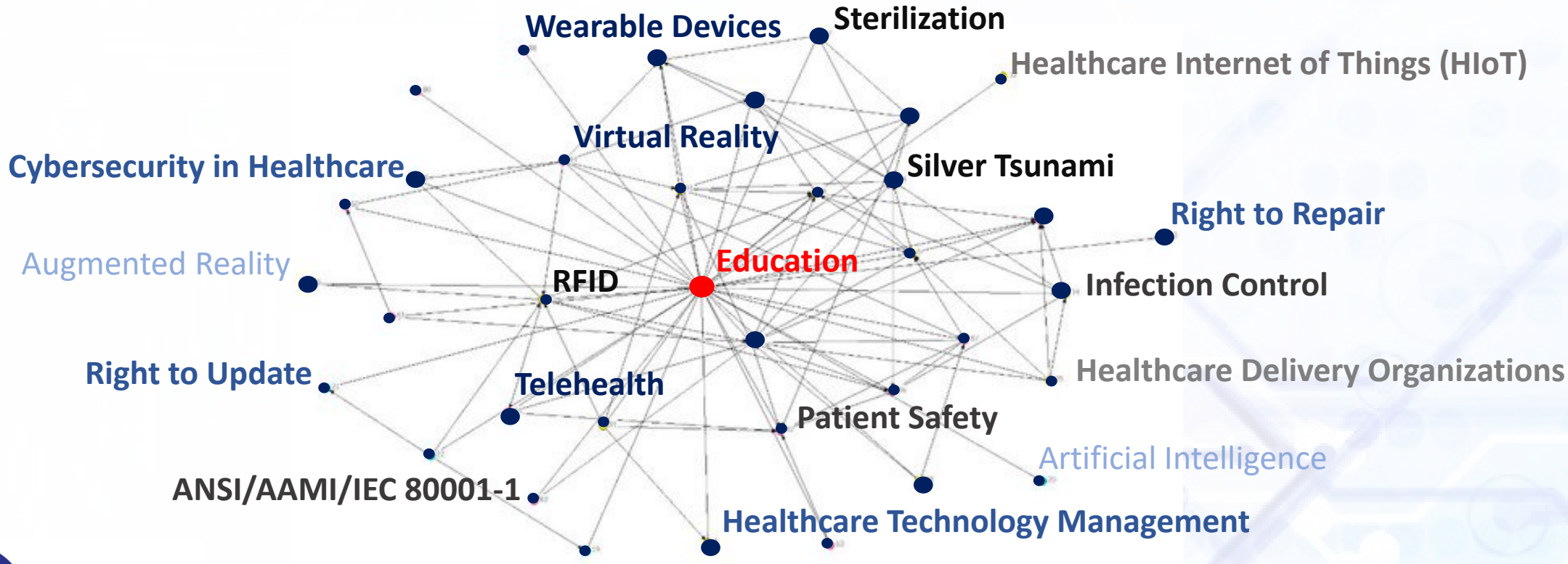
College of Biomedical Equipment Technology

Committed to Delivering a World-Class Education on Demand

MDEXPO
Tampa, FL • November 8-9, 2020

Preparing for your Future: 2021 and Beyond

The Problem Set



College of Biomedical Equipment Technology

Committed to Delivering a World-Class Education on Demand

MDEXPO
Tampa, FL • November 8-9, 2020

Preparing for your Future: 2021 and Beyond

The Human Factor

AMCA DATA BREACH

Billing services vendor, American Medical Collection Agency, experienced a data breach in 2018-2019 lasting a period of 8 months. The data breach, resulting from human error, affected 25 million patients

Source: HealthITSecurity.com, 2020

OREGON DHS

Oregon DHS was the target of a massive phishing campaign.

In total, 625,000 patients and 2.5 million emails were compromised.

Source: HealthITSecurity.com, 2020

UW Medicine

*In a recent incident, the **University of Washington Medicine** was forced to notify **974,000 patients** that their data had been exposed Online for three weeks due to a misconfigured server.*

Source: HealthITSecurity.com, 2020

Preparing for your Future: 2021 and Beyond

How are data breaches effecting Healthcare Delivery Organizations (HDO)?

- Healthcare Data breaches cost 5.6 billion annually (Forbes, 2019)
- In 2019 the top 10 healthcare data breaches affect 32 million patient records (xtelliogent Healthcare Media, 2020)
- Clinical data is a staple resource for most health and medical research:
  - Electronic health records
  - Administrative data
  - Claims data
  - Patient / Disease registries
  - Health surveys
  - Clinical trials data
    - The 5 most cyber-attacked industries in 2015: (Forbes, 2020)
      - 1. Healthcare
      - 2. Manufacturing
      - 3. Financial Services
      - 4. Government
      - 5. Transportation

Preparing for your Future: 2021 and Beyond

What's going on in our HDO industry?

- The HDO's are addressing threats to Healthcare IT with traditional IT means.
- FBI warns ransomware assault threatens US healthcare system (https://us-cert.cisa.gov/ncas/alerts/aa20-302a)
- Since April 2020 (COVID) connectivity of devices to the edge has increased 80%
- it's estimated connected medical devices could increase to roughly 50 billion, driven by innovations such as 5G, edge computing, and more
    - Medical devices are most vulnerable
        - Built to work not for security
        - No 3rd party software
    - Trained personnel
        - Network – not trained for biomed
        - Biomed - not trained for network

College of Biomedical Equipment Technology

Preparing for your Future: 2021 and Beyond

How do we connect and maintain devises safely from a HDO Perspective?

- **Patient Safety Issue - Top 3 concerns Physicians have about Cybersecurity**
  - **74% Interruptions in patient care**
  - **74% Compromised HER security**
  - **53% Threats to patient safety**
- **HIPPA and FDA Regulations**
- **Nuances of Networked Medical**
- **Archaic Systems (How do you protect a WIN 95 system/software from a 2020 Threat); many older medical devices run on old and proprietary software and cannot be updated (life cycle)**
- **Right to Repair means limited access on some devices (complicates efforts)**
- **Limited Budgets / Limited Resources**

Preparing for your Future: 2021 and Beyond

What are the effects of HDO's medical device healthcare security and data breaches?

- **According to the 2019 HIMSS Cybersecurity Survey, just over 15% of significant security issues were initially started through either medical device problems in hospitals or vendor medical devices. (Helpnetsecurity, 2020)**
- **IoT is fundamentally changing the problem set - Ramifications are life and death (loss of data = loss of life)**
- **We need to attack IT HDO's problem from an IT HDO perspective**
- **Detailed network "device" maps are not available**
    - **Cybercriminal are unleashing waves of data-scrambling techniques**
        - **Extortion**
        - **Black market - Steal and sell data**
        - **Create discord**
        - **Damage industry and the US**
        - **Knock healthcare systems offline**

Preparing for your Future: 2021 and Beyond

According to the 2019 HIMSS Cybersecurity Survey, just over 15% of significant security issues were initially started through either medical device problems in hospitals or vendor medical devices. (Helpnetsecurity, 2020)

- **Consider a particular device (Radiological or Infusion Pump)**
  - **Old Software**
  - **Limited Budget**
  - **Manual Updates**
  - **Why and how to secure**
  - **IT professionals need to be part of a solution**
  - **Interconnectivity across departments and HC IT solutions**
  - **HIPPA compliance**
  - **FDA Regulations and Guidelines**
  - **Other?**

Preparing for your Future: 2021 and Beyond

Perennial Problem (Right to Repair and the Right to Update)

- Software will always outpace hardware
- Software solutions are always an 85% solution that companies address with patches and updates
- FDA Regulations slowing the patch and update process
  - Software patches must be extensively tested to ensure no risk to patient
  - Delayed software patches leaves security vulnerabilities
- Nuances of Networked Medical
- HIPPA
- Archaic Systems (How do you protect a WIN 95 system/software from a 2020 Threat); many older medical devices run on old software and cannot be updated
- Right to Repair means limited access on some devices (complicates efforts)
- Limited Budgets

Preparing for your Future: 2021 and Beyond

AMCA DATA BREACH: 25 MILLION PATIENTS, INVESTIGATIONS ONGOING (HealthITSecurity.com, 2020)

- Billing services vendor American Medical Collection Agency was hacked for ***eight months*** between August 1, 2018 and March 30, 2019.
- ***Six covered entities have come forward*** to report their ***patient and - personal and financial data was compromised***. However, the majority of the impacted providers are still continuing to investigate the scope of the breach
  - **12 million patients** from Quest Diagnostics -
  - **7.7 million patients** from LabCorp patients
  - **422,000 patients** of BioReference.
  - **13,000 patients** form Penobscot Community Health Center in Maine
  - **2.2 Million patients** from Clinical Pathology Laboratories
  - **46,500 patients** from Austin Pathology Associates
- Shortly after, seven more covered entities reported they too were impacted: Natera, American Esoteric Laboratories, CBLPath, South Texas Dermatopathology, Seacoast Pathology, Arizona Dermatopathology, and Laboratory of Dermatopathology ADX.
  - In total, more than 774,640 patients have been added to the breach by these covered entities (Natera did not disclose how many of its patients were impacted), bringing the total number of impacted patients to more than 25 million.

❖ ***AMCA's parent company has since filed bankruptcy, while the billing services vendor, Quest and LabCorp are facing numerous investigations and lawsuits.***

Preparing for your Future: 2021 and Beyond

OREGON DEPARTMENT OF HUMAN SERVICES: 645,000 PATIENTS (HealthITSecurity.com, 2020)

- Initially announced in March, **Oregon Department of Human Services** began notifying additional patients in June of a breach caused by a **massive phishing campaign**. In total, **625,000 patients and 2.5 million emails** were compromised.

- In January, a **targeted phishing attack** caused **nine employees** to respond to the malicious emails and provide their user credentials. As a result, hackers gained full access to their **email accounts, messages and attachments**.

- It took Oregon DHS officials **three weeks to discover** the hack, when those employees reported account issues to the security team. Officials said they've continued to investigate the incident since the breach was discovered and determined protected health information was involved.

- Hackers were able to obtain or view **patient data**, which included **case numbers, Social Security numbers, and PHI**. Officials could not rule out access.

Preparing for your Future: 2021 and Beyond

UW MEDICINE: 973,024 PATIENTS (HealthITSecurity.com, 2020)

- In February, the **University of Washington Medicine** began notifying **974,000 patients** that their data was exposed online for three weeks due to a misconfigured server.
- The breach was discovered in December 2018 when a **patient conducted a search** of their own name and found a file containing their **personal information**. They notified UW Medicine, which determined an **employee error three weeks prior caused internal files to become publicly accessible**.
- "Because **Google had saved** some of the files before December 26, 2018, UW Medicine worked with Google to remove the saved versions and prevent them from showing up in search results," officials said in a statement. "All saved files were completely removed from Google's servers by Jan. 10, 2019."
- The database contained a trove of **personal data**, including the name of the lab test or the research study with the name of the health condition for some.

Preparing for your Future: 2021 and Beyond

An Educational Approach

Maintain relationships among educational providers, Healthcare Delivery Organizations, ISO's and standards (AAMI)

Expand educational programs (2+2 programs) including HTM, HISM, Infection Control, and others

Expanded certificate programs (short-term), impactful programs aimed at strengthening and broadening skills

Emphasize Prior Learning Assessment (PLA) to seasoned HTM professionals

Leverage technology to deliver world class education to anyone in the world when and where they need it

College of Biomedical Equipment Technology

Committed to Delivering a World-Class Education on Demand

MDEXPO
Tampa, FL • November 8-9, 2020

Preparing for your Future: 2021 and Beyond

Q & A

College of Biomedical Equipment Technology

Committed to Delivering a World-Class Education on Demand

MDEXPO
Tampa, FL • November 8-9, 2020