2. Presentation: Healthcare Data Networking
Facilitators: Brian Welch and Cyrus Bulsara, Scripps Health (or designee)
Discussion on data security and why building management systems should be on the hospital network.
• Approach used by Scripps Health for network security
• Discussion and public input
Hospital Building Safety Board
OSHPD

Technology Committee Meeting
June 23, 2020
Presenters:

Cyrus Bulsara
Chief Information Security Officer (CISO) - Scripps Health
XX years in information security in healthcare.

Clark Kegley
Asst. Vice President, Information Services – Scripps Health
26 years in healthcare information technology.
Scripps Health Overview:

- Scripps Health is a 96 year old, $2.9 billion private, nonprofit, integrated health system in San Diego, California that is ranked among the top 15 health systems in the nation. Scripps treats 700,000 patients annually.

- Scripps is a member of CHIME’s Most Wired Healthcare organization.

- Comprised of four hospitals across five campuses.

- Scripps Clinic and Scripps Coastal Medical Center, a network of integrated facilities with specialists from more than 60 medical and surgical specialties at more than 28 outpatient centers and clinics.

- More than 3,000 affiliated physicians and 15,000 employees.
Executive Summary:

HIPAA Overview:

• HIPAA or the Health Insurance Portability & Accountability Act of 1996 is a series of national standards that health care organizations must have in place in order to safeguard the privacy and security of protected health information (PHI).

• HIPAA includes 2 significant rules that articulate requirements for protecting PHI. They include the Privacy Rule and the Security Rule.
Executive Summary:

HITECH Act Provisions:

• The Health Information Technology for Economic and Clinical Health Act (HITECH), enacted as part of the American Recovery and Reinvestment Act (ARRA) of 2009, strengthened the privacy and security protections of HIPAA.

• Under HIPAA, Covered Entities such as healthcare providers have a written agreement with Business Associates who may access protected health information.

• Exceptions to Business Associate requirements include entities that act as a conduit for the information or who do not specifically access protected health information.
Executive Summary:

- Building Management System vendors could avoid the Business Associate agreement requirement with a Covered Entity.

- This could expose protected health information as defined by HIPAA to inappropriate disclosure.

- The normal shared risk between Covered Entities and Business Associates is transferred entirely to the Covered Entity in the absence of a Business Associate Agreement.

- Without ITs involvement issues could be introduced that negatively impact the Building Management System.
Rings Of Security:

• Sound security practices create multiple layers of security designed to thwart attempts to access protected health information.

• Your home is a good example of Rings of Security:
  1. Your garage door is secured by an automatic door opener.
  2. Your door going from your garage to your house is locked.
  3. Your house has an alarm that you turn off when entering.
  4. Your valuables are in a safe in your bedroom.
  5. Your safe is locked.

• Well designed corporate data networks follow similar practices on an enterprise scale.
Today’s Data Networks:

• Present day technology allows for significant safeguards in data network security.

1. Firewalls at the perimeter

2. Physical security controlling access to the network

3. Active monitoring protect the network from intrusion 24/7/365

4. Network professionals oversee corporate data networks

5. Modern data networks are designed with redundancy and seek to eliminate all single points of failure

6. Robust data networks allow for segmentation to isolate network traffic based on business, clinical and security needs
Today’s Data Networks: Staffing

• Network technology experts support today’s corporate data networks.

1. Education includes undergrad and certifications

2. Modern corporate data networks dictate redundancy of people, process and technology

3. Major manufacturers support network teams in healthcare (Example: Cisco)

4. When a failure occurs on a vendor-installed network it is often the healthcare provider’s phone that rings first, not the vendors.
Vendor Implemented Systems – Concerns:

- Vendors follow a different business model than healthcare provider organizations.

- Their model includes selling and supporting systems, not enhancing the security posture of the corporate data network.

- They routinely install “back door” access into their installed base to address issues. Often outside the knowledge of the healthcare organization.

- They generally do not have the number of staff or the skill sets typically found in IT shops of healthcare organizations.

- They will often ask to have a separate data network because it is easier for them to install their systems.

- They generally do not subscribe to the levels of security of healthcare organizations.
Vendor Implemented Systems – The Solution:

• When external vendors work directly with Information Services teams to implement their systems the best outcomes are achieved.

• IT and the vendor work jointly on the implementation requirements, including appropriate security measures, and establish protocols for support, outages and maintenance.

• This creates clear separation of duties and expectations for normal operations of the installed system. More importantly, it establishes protocols for outages in terms of response, remediation and recovery.

• These are shared accountabilities.
Modern networks are architected such that a wide range of options are available to observe and control traffic…

It starts with basic visibility:
- Aggregate descriptive metadata (ports, protocols, IPs, etc).
- Understand the network. Who is talking, and why?
- Review metadata and develop a “baseline” of normal.

Once we understand the network, we can control it:
- Control who can connect to the network by deploying Network Access Control technologies.
- Control who can talk to who on the network by deploying segmentation and Access Control Lists (ACLs).
- Detect and respond to indicators of compromise.
- Control how data flows between hosts, within and outside the network perimeter.
...but “modern” is a moving target.

New challenges emerge constantly:
- The rise of connected systems (IoT). Everything has an IP.
- Remote work extends the network perimeter into the home.
- ...

Cybersecurity functions are challenged to develop approaches that balance security with the needs of our customers.
- Building systems and biomedical devices demand connectivity, but often lack host-based security. Applying appropriate network-based security controls is delicate.
- Our userbase is hungry for data and services, delivered to the location and device of their choosing.
Technology is the least of our problems. People, processes, and strategic leadership must be the focus.

Understand the needs of your customer. Understand the risk appetite of your business. Understand the regulatory environment. Develop a threat model. Create a cybersecurity approach that strikes the right balance. Continuously monitor it, measure it, improve it. Iterate.

“The best cybersecurity technology you can hope to implement is whatever you can afford, staffed by good cybersecurity personnel.”
• Understand the lifecycle of an attack through the Unified Killchain framework.

Recon
Discover our network and probe for vulnerabilities.

Foothold
Gain an initial foothold on the network. Map targets.

Pivot
Move on from the initial foothold to higher-value targets on the network. Position for endgame.

Endgame
Action to achieve objectives.

• Understand the tactics, techniques, and procedures (TTPs) used by attackers to migrate through the attack lifecycle with the MITRE ATT&CK framework.
• Choose a framework of internal controls to adopt/benchmark.

**Basic**
1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

**Foundational**
7. Email and Web Browser Protections
12. Boundary Defense

• The CIS CSC Top 20 is a good start. Account for your regulatory requirements.

• Choose a framework to measure maturity by. **Iterate.**

**Visibility**
Continuous awareness of the hardware/software on our network, and how it behaves.

**Control**
React to what we see with our own TTPs and controls.

**Standardize**
Respond consistently to what we see with transparent, repeatable processes.

**Automate**
Deploy automation to react at machine speed and free valuable human resources for value-add work.

Continuous Improvement
Develop a virtuous cycle of performance measurement and improvement.
Physical Cybersecurity

• Physical access = root access!

• Just as we segment the network, so too must we segment real life.
• Deny physical access by default.
• Authenticate personnel physically using an appropriate mix of identifiers (badges, biometrics, etc.).
• Implement environmental controls that promote access control and operations.
• Continuously monitor it, measure it, improve it. Iterate.
Vendor Management

• Hold your vendors to the same standards as you would yourselves.

• Build expectations into enforceable legal agreements.

• Verify relevant third-party certifications (e.g., SOC2).

• Continuously monitor compliance with expectations.
Conclusions:

- Vendors will generally follow a pathway that best supports their business model.

- Healthcare IT departments follow a pathway that best supports clinical and business operations.

- HIPAA and the HITECH Act directly impact healthcare providers and hold them accountable for the security of corporate data networks. Building Management System vendors are generally not governed by HIPAA and the HITECH Act.

- Vendor resources do not possess the knowledge of the healthcare data network on which they install their systems. The providers IT staff do.

- That same provider staff support multiple vendor systems on the corporate data network.
Recommendations:

• We appreciate all that OSHPD and their supporting entities do for healthcare organizations.

• OSHPD can rest assured that we’ve got the best interests of our patients, those that care for them, and our vendor partners in mind when we design and implement all systems. No one is as invested as IT shops in healthcare to deliver critical systems.

• We know what regulations require and manage to those outcomes when designing and implementing systems.
Thank You For Your Time Today!

We welcome your questions.

Bulsara.Cyrus@ScrippsHealth.Org
Kegley.Clark@ScrippsHealth.Org
3. Presentation: Fuel Cells for Normal Power
Facilitator: Sri Raghavan, Bloom Electric (or designee)
Discuss proposal to consider fuel cells as a normal power source in hospitals.
• Discussion and public input
FUEL CELL AS A NORMAL SOURCE

June 23, 2020

Sri Raghavan, P.E
Daniel Huang, P.E
### SOME CHALLENGES FACED BY HEALTHCARE TODAY

<table>
<thead>
<tr>
<th>Economics</th>
<th>Reliability</th>
<th>Air Quality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy costs significant; utility</td>
<td>Greater focus on reliability</td>
<td>Poor air quality increases acute respiratory</td>
</tr>
<tr>
<td>rates rising</td>
<td>during the surge</td>
<td>illnesses in people</td>
</tr>
<tr>
<td>Revenue loss from cancelled</td>
<td>Preparedness for future pandemics</td>
<td></td>
</tr>
<tr>
<td>procedures</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PSPS and weather related outages</td>
<td></td>
</tr>
</tbody>
</table>
Bloomenergy®

We Deliver Clean, Reliable and Resilient Onsite Power

Over 660 sites protected
Designed and Manufactured in US
Traded on NYSE: BE

Microgrid Provider for Business Resiliency

AlwaysON 24x7 Electricity
Over 85 microgrids installed worldwide

Generates Electricity without Combustion

99%+ Reduction in Smog-Forming Pollution
Displaces Diesel Generators

COMCAST  Intel  verizon®  ebay inc.  THE HOME DEPOT  Walmart  IKEA  EQUINIX
Anode and cathode are made from special inks that coat the electrolyte and require no precious metals, corrosive acids or molten materials. As long as there is fuel, air and heat, the process continues producing clean, reliable and affordable energy.

Chemical reaction produces electricity when connected to a circuit.

THE SOLID OXIDE FUEL CELL: HOW IT WORKS

Natural Gas (CH₄ – Methane)

Ambient Air

Fuel Passes Over Anode

Steam Reformation

O₂

Air Passes Over Cathode

Anode and cathode are made from special inks that coat the electrolyte and require no precious metals, corrosive acids or molten materials.

Anode

O₂⁻

Cathode

O₂⁻

O₂

CO + H₂ → CO₂ + H₂O

Reformation

Fuel Passes Over Anode

Oxygen Ions React with Fuel in Fuel Cell

CO → CO₂

H₂ → H₂O

Anode

Electrolyte

Cathode

Reaction Produces Electricity

[ e⁻ ]
MICROGRID OPERATION OVERVIEW

- Primary generation for base load and backup generation for business critical loads
- Load following functionality for standalone operation
  - Voltage and current
  - Manage step changes in load
- Advanced functionality
  - No momentary loss of power during utility outage or restoration

Feature for grid-connected customers to use for business critical loads during grid outages
FUEL CELL AS NORMAL SOURCE MICROGRID

**Status Quo Architecture**

- Normal Source
- Alternate Source

When Utility is down, Hospital runs on Alternate Source

No Elective Procedures allowed on Alternate Source

Postponement of elective procedures can cause revenue loss and threaten patient care

**Fuel Cell Based Architecture**

- Normal Source
- Alternate Source

When Utility is down, Hospital **stays** on Normal Source

Elective Procedures can Proceed

when utility is down, hospital runs on alternate source...
CONVENTIONAL OSHPD MODEL

Type 1 & 2 EES – Essential Electrical System for Health Care
PROPOSED BLOOM MICROGRID SOLUTION

Type 1 & 2 EES – Essential Electrical System for Health Care
<table>
<thead>
<tr>
<th><strong>Resiliency</strong></th>
<th><strong>Elective Procedures</strong></th>
<th><strong>Fuel Supply</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional standalone power source</td>
<td>Ability to continue elective procedures</td>
<td>Works off underground natural gas pipeline</td>
</tr>
<tr>
<td>Resiliency solution for PSPS/long outages</td>
<td>Mitigating elective procedure backlog coinciding with PSPS/long outages</td>
<td>Diesel will continue to be ‘last line of defense’</td>
</tr>
<tr>
<td>Business as usual across OR, ER, SNFs, clinics etc.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mitigating Covid surge coinciding with PSPS/long outages</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
MICROGRID FEATURE: BASELINE SITE

Grid Tied Inverter Output

200 kW Energy Server

380V DC Bus

Hospital Load

Grid

Load
MICROGRID INVERTER WITH STEP-LOAD MODULE

Grid Tied Inverter Output

380V DC Bus

200 kW Energy Server

Microgrid Inverter Output

Hospital Load

Protected Load

99.99+ %

Power Continuity

OSHPD Standard Transfer Switch
MICROGRID INVERTER: WITH GRID OPERATION

Grid

40 to 200 kW

Grid

Hospital Load

OSHPD Standard Transfer Switch

99.99+ % Power Continuity

380V DC Bus

200 kW Energy Server

0 to 160 kW (Total Output de-rated by 20% for N+1 redundancy)

Protected Load 160kW

MICROGRID INVERTER: WITH GRID OPERATION

Primary power source is the Microgrid Inverter
UPM: WITHOUT GRID OPERATION

200 kW Energy Server

380V DC Bus

160 kW

0 kW

Protected Load 160kW

99.99+ % Power Continuity

Load unaffected by grid outage

OSHPD Standard Transfer Switch
Key Features:

• Business as usual even during long outages
• Elective procedures can proceed
• Insurance against PSPS/long outages coinciding with pandemic surge or elective procedure backlog
• Provides hospital loads with a 3rd reliable source of power which can remain in service even in the event of a grid outage
• Does not replace normal (utility) or alternate sources (emergency generator)
• Modular approach – allows for synchronization, coordination

For more information please contact - BloomEnergy.Information@bloomenergy.com
Thank You

Bloomenergy®
4. Presentation: OSHPD Technology-Driven Programs
Facilitators: Joe LaBrie and Richard Tannahill, OSHPD (or designee)
Discuss the following electronic plan review and training programs being developed by the Facilities Development Division:
- Testing, Inspection and Observation (TIO)
- eCheck List
- Electronic Comment and Process Review (eCPR)
- Inspector of Record Academy
- Electronic Plan Review (ePR)
- Discussion and public input
OSHPD Technology-Driven Programs

- Testing, Inspection and Observation (TIO)
TIO Current Practice

- OSHPD Form (XL or PDF)
- Plan Approval
- Permitting
- Incremental / Phased Projects
- Field Maintenance
  - Updates
  - Changes
  - Workflow
TIO Form Current Limitations

- Real Time Sign-Offs / Updates / Changes
- Distribution
- Access
- Original / Master
- Back Up Documents (Archiving, Certs, VCRs etc)
- Authorization
- Authentication
eTIO

- Objective: Create an electronic TIO tool that is designed to improve the quality assurance documentation that overcomes the current TIO limitations.
- PDF Issues: Basically the same as paper
- XL Format Issues: Great for one time use but then its PDF
- Platform Options:
  - Stand alone online
  - Accela / eSP Integration
OSHPD Technology-Driven Programs

- Testing, Inspection and Observation (TIO)
- eCheck List
OSHPD Technology-Driven Programs

- Testing, Inspection and Observation (TIO)
- eCheck List
  - Delayed
From this…

To this
OSHPD Technology-Driven Programs

- Testing, Inspection and Observation (TIO)
- eCheck List
- Electronic Comment and Process Review (eCPR)
### eComment and Review Process

#### Projects

<table>
<thead>
<tr>
<th>Date</th>
<th>Project Number</th>
<th>Project Type</th>
<th>Project Name</th>
<th>Status</th>
<th>Related Records</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/09/2018</td>
<td>I140004-21-00-ACD0225</td>
<td>Post Approval Document</td>
<td>Increment Master - Marin General - Hospital Replacement Building</td>
<td>Approved</td>
<td>531</td>
<td></td>
</tr>
<tr>
<td>04/06/2018</td>
<td>S180761-21-00-AMC0001</td>
<td>Alternate Method of Compliance</td>
<td>Patient Monitor System</td>
<td>Denied</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>04/06/2018</td>
<td>I140004-21-00-ACD0223</td>
<td>Post Approval Document</td>
<td>Increment Master - Marin General - Hospital Replacement Building</td>
<td>Approved</td>
<td>531</td>
<td></td>
</tr>
<tr>
<td>04/03/2018</td>
<td>S180761-21-00</td>
<td>Application for New Project</td>
<td>Patient Monitor System</td>
<td>Field Operations in Progress</td>
<td>8</td>
<td>Amendment</td>
</tr>
<tr>
<td>03/29/2018</td>
<td>S180712-21-00</td>
<td>Application for New Project</td>
<td>MGH- Recycle Yard</td>
<td>Closed</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>
eComment and Review Process

Select an Amendment Type

Choose one of the following available amendment types. For assistance or to apply for an amendment type not listed below please contact us.

- Alternate Method of Compliance
- Comment and Process Review
- Post Approval Document

Continue Application »
Comment and Process Review

APPLICATION

* Issue Under Appeal:

* Reason for Appeal:

* Proposal of Appellant:
eComment and Review Process

**Step 3: Attachments > Supporting Documents**
Upload any plans, documents, photographs or data that you believe supports your appeal or that you believe would assist the reviewer in determining if this appeal should be upheld.

* indicates a required field.

**Attachment**

The maximum file size allowed is 300 MB.
html;htm;mht;mhtml;exe;com;pif;scr;vbs;shs;chm;bat;cmd;hta;reg are disallowed file types to upload.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Virtual Folders</th>
<th>Action</th>
<th>Size</th>
<th>Description</th>
<th>Latest Update</th>
<th>Upload Date</th>
</tr>
</thead>
</table>
Routing through Accela

- First Level Review (OSHPD staff who made the decision, ruling, order, or act)
- Second Level Review (Manager of first level person)
- Third Level Review (Deputy Division Chief)
- Fourth Level Review (Deputy Director)

- Appeals go to HBSB
OSHPD Technology-Driven Programs

• Testing, Inspection and Observation (TIO)
• eCheck List
• Electronic Comment and Process Review (eCPR)
• Inspector of Record Academy
IOR Academy

- Create an IOR Academy for Focused Training by OSHPD ISU through On-The-Job Mentoring and Rigorous Technical Curriculum for a Select Group of Next Generation of IORs
IOR Academy Structure

- On the job apprentice program
- Weekly academic training
  - Administrative Regulations
  - Technical Knowledge
- Academy Duration
- Examination Milestones
IOR Academy Structure

• Business Plan
• Curriculum Development
• Strategic Partnerships for Apprenticeships
  • Associations
  • IOR Groups
  • Healthcare groups
OSHPD Technology-Driven Programs

• Testing, Inspection and Observation (TIO)
• eCheck List
• Electronic Comment and Process Review (eCPR)
• Inspector of Record Academy
• Electronic Plan Review (ePR)
OSHPD Technology-Driven Programs

- Testing, Inspection and Observation (TIO)
- eCheck List
- Electronic Comment and Process Review (eCPR)
- Inspector of Record Academy
- Electronic Plan Review (ePR)
5. Update: Robotic Courier (TUGS) Technology
   Facilitator: Nanci Timmins, OSHPD (or designee)
   • Discussion and public input
AGVS-
Automated Guided Vehicle System
2020

Nanci Timmins
Chief Fire and Life Safety Officer
Automatic Guided Vehicle Systems
### AGVS PIN

**Why we need this PIN**

- The CBC does not include provisions for the installation of robotic systems that share means of egress systems and elevators with building occupants.

**Why is that a concern**

- Obstruction of the usable width of egress.
- Transportation of combustible materials in egress systems.
- Delay of operation of smoke and draft control assemblies and fire assemblies.
- Cause inappropriate operation of activated fire control assemblies.
- Cause installation of equipment in egress systems.
- Interference with operation of elevators.

Many of the items transported by an AGVS are now transported by other means. The other means are operational. **However,** an AGVS requires some construction and/or remodeling and is therefore within the scope of the CBC, per CEBC 302A.7. An AMC will be required for each AGVS project.
Code Requirements

CBC 1003.6, 1018.1, 1020.3, 1024.2, 1028.4.1 and 1028.5 require minimum egress widths be maintained and unobstructed.

Title 19, Section 3.11 Prohibit the obstruction of the required width of an exit; prohibits the installation or placement of equipment in, or exposed to, any exit, and; prohibits storage in a corridor.

CBC 716.5.9 describes requirements for automatic closing of fire assemblies.

CEBC 302A.7 requires existing buildings to be maintained in safe and sanitary conditions. Safeguards are required to be maintained in conformance with the code edition under which they were installed.
• California Code of Regulations, Title 19, Division 1, § 3.11(a) through (d)] Exits, Aisles, Ramps, Corridors and Passageways.
  • (a) No person shall install, place or permit the installation or placement of any bed, chair, equipment, concession, turnstile, ticket office or anything whatsoever, in any manner which would block or obstruct the required width of any exit.
  • (b) No person shall install, place or permit the installation or placement of any combustible material or equipment in or exposed to any exit.
  • (c) No person shall install, place or permit the installation or placement of any storage material of any kind in any exit regardless of the required width of such exit.
20 x 20 x 20 Room Experiment

- A single dime sized hole in a rated barrier
- The 8,000 sq ft room will fill with smoke in under 4 minutes
- So that you cannot see your hand 18 inches in front of you
- Source: International Firestop Council 2004
He who moves not forward, goes backward.

Johann Wolfgang von Goethe
Guidelines
(Some items may change prior to PIN approval)

• AGVS units should not be parked in corridors or corridor alcoves.

• AGVS units should be autonomous. Staff responsibility is patient safety. Added time in moving equipment in addition to equipment already requiring relocation, can be detrimental to patient safety.

• Restricted use in corridor systems serving the general public and patient care areas.

• The minimum egress width required by the building code to be provided.

• Where AGVS units may pass each other, additional corridor width may be required to maintain the minimum egress width.

• Corridor systems and adjacent rooms containing the AGVS guide path system should be provided with a complete automatic smoke detection system.

• AGVS unit storage/recharging home room should be provided with a complete automatic smoke detection system. It should be demonstrated how the AGVS will be programmed to not open the door to the storage/recharging home room if smoke detection in the room has been activated. The door to the room should be equipped with auto-openers/auto-closers connected to the building Essential Electrical System.
Guidelines
(Some items may change prior to PIN approval)

• To allow the passage of AGVS units, the activation of the automatic closure or reclosure of smoke and draft control assemblies and fire assemblies should not exceed a delay of more than 10 seconds.

• A closure or reclosure delay of 20 seconds may be permitted with a reduction in the spacing of required smoke detector protection.

• Care should be taken to avoid corridor widths or areas that become too wide. Excessive corridor widths encourage the storage of materials in the corridor system. When service corridor widths are limited to the widths necessary for the passage of AGVS carts and the movement of staff, the operation of an AGVS may actually keep corridors clear of materials and commodities that would otherwise be stored or parked in these areas.

• Where AGVS carts pass through exit doors or exit access doors, such doors should be provided in pairs. An AGVS cart should not obstruct more than one half of the required opening width of such openings, and it should not obstruct the doors from completely closing.

• The status of AGVS carts during a fire alarm condition should be addressed. It should be demonstrated how AGVS carts will be programmed to proceed to holding rooms equipped with smoke detection and auto openers and auto closers connected to the building Essential Electrical System, and whether they will remain in elevators or vacate elevators. It should also be demonstrated how the AGVS unit is programmed to return to its designated holding room and not pass through cross corridor doors in response to the fire alarm when approaching cross-corridor doors that have been released by activation of smoke detection at the cross-corridor doors.
Guidelines
(Some items may change prior to PIN approval)

• When AGVS carts stop at a fire door that has closed in response to a fire alarm, a clear zone should be maintained at the approach to the closed fire door/s, and the AGVS should proceed to its designated holding room within the smoke compartment.

• It should be demonstrated how the AGVS units are programmed to discontinue travel if fire is within the contents of the AGVS units.

• An AGVS cart should not be capable of opening a fire door at a location where a smoke detector has activated.

• An AGVS should not interfere with the operation of elevator recall.

• An AGVS cart should not exceed the weight limitations of an elevator.

• The strength of structural load bearing members should be evaluated when an AGVS is considered.

• In accordance with California Fire Code, Section 808, the operation of an AGVS with cart capacities greater than 32 gallons (4.3 cu. ft.) is not permitted in a Group I-2 or I-3 occupancy.

• In accordance with Title 19, CCR, Section 2.02, a review of alternate designs or methods of construction or alternate means of protection involving fire and life safety issues, requires a local fire authority approval.
THERE'S MORE TO THIS STORY THAN MEETS THE EYE.

Lisa Goehle
THANK YOU!
6. Discussion: Items for future Committee Meetings
Facilitator: David Bliss, Committee Chair (or designee)
• Cybersecurity, ransomware, network backup
• Emerging technologies to reduce carbon footprint/sustainability in healthcare
• Discussion and public input
7. **Comments from the Public/Committee Members on issues not on this agenda**

Facilitator: David Bliss, Committee Chair (or designee)

The board will receive comments from the Public/Committee Members. Matters raised at this time may be taken under consideration for placement on a subsequent agenda.