THE HEALTH CARE IMPROVEMENT FOUNDATION

2020-2021
Delaware Valley
Patient Safety & Quality Award
Top 10 Submission

Partnership for Patient Care
15th Anniversary
2006 – 2021

Jefferson Abington Hospital

Cyber Security Readiness - Stress Testing Digital Darkness Downtime Procedures with in-situ Simulation-based Failure Modes Effects Analysis

Background

- In October 2020, the Federal Bureau of Investigation and Department of Health and Human Services contacted Jefferson Health with a "credible and imminent cyber-security threat" that would disable all network machines, software, and devices in the health system.
- Downtime procedures were identified as inadequate to maintain normal operations, which is a threat to patient safety.

Goal

- To discover, quantify and mitigate latent safety threats (LST) that would occur in total digital darkness.

Approach

- Assembled an inter-professional and inter-disciplinary care team.
- Set up Patient Safety-Nursing Education Dyads in the in-situ simulation Failure Modes Effects Analysis (FMEA) methodology.
- Mobilized the dyad teams to conduct in-situ simulation which followed a patient from their entry to the ED, during their time in the ED, and to the floor for every possible scenario.
- Applied a human factors-based approach.

Results & Takeaways

- Stress testing the reliability and resiliency of critical clinical care systems revealed a number of gaps, hazards, and threats in downtime processes, which enabled the development of more effective risk mitigation strategies.
- First application of an in-situ simulation FMEA to a cyber-security threat.
- Building on the existing culture of safety allowed for access to the resources needed to accomplish the initiative.