CHIME & MDHIMSS

2019 Program Summary

CHIME MDHIMSS Leadership Academy

Leadership Academy

Overall Abstract

Healthcare information technology executives have been leading the way in implementing electronic health records, clinical informatics and analytics, and patient-centered care. But now healthcare is seeing disruption at every turn with the introduction of artificial intelligence, machine learning, robotics, social networking platforms and wearable technology. What will this quantum change mean to healthcare and what can health IT executives do to direct their organizations toward effective adoption and use of these powerful new capabilities? Healthcare is exploring the potential for these technologies to make services more efficient, anticipate demand and tailor treatment. Decisions can be more transparent and evidence-based, the right care can be offered to patients based on their personal needs, safety and security threats can be recognized and responded to quickly, and healthcare professionals can have data available for every action and decision.

Learning Objectives

- Investigate the new frontiers of Artificial Intelligence, machine learning, the Internet of Things and the connections between them that will transform care
- Discuss how health IT leaders can challenge themselves to be more engaged and influential as digital leaders; working with their peers and communities to develop a digital strategy for their organizations
- Examine the changes in direction necessary to create and deliver on a digital strategy for healthcare
- Describe how continued integration and alignment of health systems and digital capabilities will create the next wave of healthcare transformation
- Identify current programs that are taking on the transformation challenges
- Explore the qualities of leadership and collaboration necessary to connect with patients, peers and partners to put people ahead of technology in healthcare transformation

CMIO Leadership Academy

Overall Abstract

The CMIO role in today's healthcare organization has never been more challenging. To better equip physician leaders filling this important position, CHIME will further your education as a leader in healthcare IT with the CMIO Leadership Academy.

Designed specifically for physicians embarking on CMIO leadership roles, the curriculum will be modeled on CHIME's successful Healthcare CIO Boot Camp program, with additional content tailored to help participants gain the real-world skills necessary to become successful CMIOs.

Taught by a faculty of successful healthcare CIOs and CMIOs, the intensive program will feature a collaborative teaching methodology combining presentations, small group discussion, case study analysis, progressive problem solving, and personal mentoring.

Learning Objectives

- Create focus and energy for change in a tumultuous environment as well as a framework for change
- Create opportunities to bring stakeholders together to truly collaborate and identify adaptive changes that can help the organization move forward
- Understand the nature of strategy and discuss IT-business strategy alignment/convergence
- Review complementary strategies and strategy evolution
- Understand the value of governance and matching of your IS governance style to organizational governance style
- Understand need to define decisional rights at each level of governance as well as the roles of leadership and operations in both governance and execution of projects
- Build and maintain an active network of internal and external relationships based on shared interests and needs; developing trusting and trusted relationships
- Demonstrate effective give-and-take relationships with others, e.g., senior leaders, physicians and other stakeholders, peers, direct reports, customers
- Demonstrate an understanding of others' perspectives and agendas

Cybersecurity Academy

Overall Abstract

A top priority for every healthcare IT executive is protecting their organization from cybersecurity threats and reaches. Just one breach can cost the organization precious time and resources, and the loss of trust by patients and the community can have lasting consequences. In this executive level program, industry experts will present key components of an effective cybersecurity strategy and approaches any organization can take to gain employee support and engagement.

Learn strategies to engage key stakeholders who can become champions of the cybersecurity and risk management plan, and who can provide the support and resources needed to effectively carry out the plan. Gain insights on developing, implementing and using cybersecurity plans at the time of a breach, as well as tips on engaging the organization so cybersecurity becomes a part of every employee's role. Finally, learn how to shift your organization into a cybersecurity learning organization in order to protect valuable data and physical assets

Learning Objectives

- Discuss opportunities to incorporate cybersecurity awareness and risk management into the fabric of an organization and the employee mindset.
- Explain how to engage stakeholders to secure needed resources and funding to support the plan.
- Identify key steps in preparing an organization against cybersecurity threats and breaches including security frameworks and control measures.
- Define key components of an effective cybersecurity plan including prevention, response and recovery approaches for successful implementation and staff adoption