The Enemy Within: Dealing with Insider Threats
**Moderator:** Lee Kim
HIMSS

**Speakers:**
- Bruce Forman
  UMass Memorial Healthcare
- Carmine Nigro
  Federal Bureau of Investigation
- Anahi Santiago
  Einstein Healthcare Network
“Insider threat” is a term that we have heard a lot in the news.

What is your definition of who the “insider” is and what the “insider threat” is?

What insider threats do we need to be aware of? Cyber and other (e.g., physical)?

What insider threats are you most concerned about and why?

What methods do you use to detect and mitigate the insider threat (people, processes, technology)?
What can be done with the well-intentioned insider to deter them from negligent mistakes that can result in data loss or breach?

Employee snooping is a major concern for many healthcare organizations. How do you mitigate snooping? What are your policies and procedures? Technology?

Do you treat your internal network traffic the same way as your external network traffic, given the problem of insider threat?

How do you deal with low tech or no tech insider threat (e.g., stealing paper records or taking photographs of information)?
Who are the people most likely to be a malicious insider?

Behavioral profile?
Personal factors?
Organizational profile?

What are the indicators of malicious insider activity?

Technology, security, performance, etc.?  
Suspicious or irregular behavior?
Personal factors?

Can you give a few examples of malicious insiders? How about “remote” malicious insiders? (E.g., domestic or foreign consultant or contractor for an outsourced job or task)
If we suspect or know about an insider threat problem within our organization, when is it the right time to engage with the FBI?

What can organizations do to work effectively and efficiently with the FBI when there is a potential problem?

What are the best practices for deterring the insider threat?

What can you do to deter the serial insider threat actor? Background checks? Verifying credentials, etc.?
Is there as much or more of a problem of insider threat with contractors or consultants compared to employees? What about insider threat and the cloud and managed services?

What can your organization do to become more resilient to insider threats? Is there guidance and resources which you would recommend?

Bruce, Anahi, & Carmine
THANK YOU!