ISACA®
*Trust in, and value from, information systems*
**San Francisco Chapter**

## Expert Panel: Understanding and Securing Electronic Medical Records

## GRC Track – Session G22

Mark Seward, CISA
Director of Security and Compliance Solutions
Splunk, Inc.

Bill Pankey
Consultant
Tunitas Group

Blair Bautista
Director for the IT Audit and Assurance Practice
Moss Adams

Patrick Roberts
Vice President and CISO
Elan Pharmaceuticals

Jeffrey D. Blevens
IT Compliance , Program Manager
Kaiser Permanente

## Session Abstract

Current access management systems do not support the healthcare system.  The all or nothing approach lacks the subtlety to balance privacy, patient safety and operations.  Access can be broken down into qualities that can be measured by collecting and correlating specific data types over time.

Healthcare insurance fraud ranges from $68 to $120 billion depending on the data source.  Organized crime sees insurance fraud as profitable.  Claims typically must be paid in seven days or be flagged for fraud.  No real-time data analytics system currently exists to monitor claims pre-adjudication.  Log correlations will be discussed as a possible way to mitigate fraud risk.

## Target Audience

Occupational Experience – Entry to Senior level Auditors, Managers, and Directors in Health Care industries, and Non-Health Care industries.

## COBIT Objectives

PO1, PO3, PO9, DS5, DS7, DS10, DS11, ME3.

## Speaker Bios

**Mark Seward:**
Mark Seward CISA, is currently Director of Security and Compliance Solutions at Splunk Inc. He has over 10 years of experience in the IT security management profession as a security practitioner and product manager with experience in log management and vulnerability management including extensive security work for the US Treasury Department.  Mark has a Master of Science in Information Technology and a Federal CIO certification from the University of Maryland.

**Bill Pankey:**
Bill Pankey has been involved in security issues of EMR /EHR for the past 15 years.  He is currently involved in the development of security architectures to support the Veterans Health Administration's next generation electronic health record.  He is an active participant in healthcare standards development and is currently engaged in ONC's S & I (standards and interoperability) collaboration.  Bill is a CISA, CISM, CGEIT, CISSP and holds numerous technical security certifications.  For the past four cycles, he has organized and taught portions of the SF ISACA Chapter's online CGEIT Exam Prep course.

**Patrick (Paddy) Roberts:**
After 20 years working in the information risk management and security arena, prior to leaving Ireland four years ago, Patrick Roberts was one of Ireland's most experienced information risk management and security professionals.  He has recently relocated to the Bay Area with Elan Corporation where he operates as their CISO and Head of the IT Governance & Control group.

Prior to joining Elan, Patrick ran one of Ireland's largest information security teams at first-e, the

Internet banking group.  As Head of Risk Management for the bank, his responsibilities spanned technical risk, operational risk and fraud management.

Before joining first-e, Paddy worked in the Global Risk Management Solutions group at PricewaterhouseCoopers for four years.  During this time, Paddy worked on assignments across Europe for a number of multinational clients spanning technical risk, operational risk and computer audit.  Paddy left PwC as Head of Technical Risk Services.

In addition to his Elan responsibilities, Paddy is the founding president of the Irish chapter of the Information Systems Security Association where he served as President from 2003 until late 2008.

**Blair Bautista:**
Blair is a healthcare advisory consultant with over 25 years experience primarily serving provider clients in the west coast.  He worked for the largest healthcare provider in the US, as has been involved as a team member in the development clinical applications (e.g. pharmacy, radiology, occupational medicine, ambulatory, and inpatient).  Blair specializes in reviews of electronic medical records implementation assessments, pre-post implementation assessments and focused reviews of specific EMR modules.  As an internal auditor within the healthcare industry, Blair performed detailed process reviews of clinical operations that involved evaluating complex clinical workflows.

**Jeffrey Blevens:**
Jeffrey Blevens is currently a Principal Program Manager within Kaiser Permanente's (KP) IT Compliance Department.  He has over 11 years combined compliance experience with focusses on HIPAA, SOX and PCI.  In his current role on the KP HIPAA Application Security Program, his focus is on HIPAA application security remediation and HIPAA sustainment of all layers for security and minimum necessary.