Streamline EHNAC and HITRUST Assessments for Reduced Redundancy, Cost and Complexity

Lee Barrett: Executive Director, EHNAC
Mark Krapels: Chief Operating Officer, Chief Security and Compliance Officer, InstaMed
Managing Vendor/Contractor Risk

Healthcare: Sample headlines involving Third Parties

$81.55 million settlement underscores the importance of executing HIPAA business associate agreements
OCR’s investigation indicated that the hospital failed to have in place an appropriate business associate agreement, as required under the HIPAA Privacy and Security Rules, so that its business associate could perform certain payment and health care operations activities on its behalf.
– U.S. Dept of HHS on March 16, 2016

Improper disclosure of research participants’ protected health information results in $3.9 million HIPAA Settlement
A laptop computer containing the electronic protected health information (ePHI) of approximately 13,000 patients and research participants was stolen from an employee’s car.
– U.S. Dept of HHS on March 17, 2016

Vendor mistake causes breach of 32,000 patients’ data.
The vendor was hired to transcribe care notes on what was supposed to be a secure website. However, the information remained publicly accessible because the vendor apparently failed to activate a firewall.
– Healthcare Business & Technology, August 2013

$875,000 HIPAA settlement underscores the need for organization-wide risk analysis
90,000 individuals ePHI was access after an email attachment with malicious malware was downloaded. Affiliated covered entities must have in place appropriate policies and processes to assure HIPAA compliance with respect to each entities that are a part of the affiliated group.
– U.S. Dept of HHS on December 14, 2015

FTC Data Security Settlement Highlights Need for Third Party Vendor Management and Oversight
Federal Trade Commission (FTC) announced a settlement with a translation services provider following the public exposure of thousands of medical transcript files containing personal medical information.
– HL Chronicle of Data Protection, January 2014
Program Governance

Third Line of Defense
- Independent assurance
- Independently test, verify and evaluate risk management controls against internal policies
- Report upon effectiveness of the program

Second Line of Defense
- Independent compliance framework, policy & oversight
- Business partners work with the BU’s to identify, assess and mitigate all risks
- Design and assist in implementing company-wide risk framework and oversee enterprise risks
- Provide independent risk oversight across all risk types, business units and locations
- Perform quality assurance reviews and other targeted oversight practices to ensure that the line of business is compliant with internal policies/external regulations

First Line of Defense
- Primary responsibility for compliance and owner of risk
- BU managers and third party relationship owners are responsible for identifying, assessing and mitigating risk associated with their business
- Implement internal controls and practices are consistent with company-wide policies & procedures
- Promote a strong risk culture and sustainable risk-return decision making
A High-Level Perspective on Managing Third Parties

- Governance Framework
- Policy & Procedures
- Inventory Stratification
- Issues Management

Risk Considerations:
- Reputational
- Operational
- Credit/Financial
- Business Continuity and Resiliency
- Strategic/Country
- Subcontractor
- Technology
- Info Security & Privacy
- Compliance

Third parties:
- Vendors
- Suppliers
- Joint Ventures
- Business Channels
- Marketing Partners
- Affiliates
- Business Associates
- Regulated Entities
Ongoing Monitoring

Results of the inherent risk should drive the nature, timing and extent of activities used to monitor, oversee, and re-assess third party relationships. Due to the higher costs associated with more in-depth assessment activities, a risk based approach should be leveraged ensuring higher risk relationships receive more active risk management than lower risk relationships.
Challenges

- Expanding Perimeter
- Internet of Things
- Cloud Services
- Third Parties / 1099
- Encryption
- Monitoring
HITRUST CSF Certification

The HITRUST CSF certification – when attained in conjunction with the industry-specific EHNAC accreditation demonstrates to business partners and prospects a commitment to the highest standards of data privacy and security.

The HITRUST CSF provides a comprehensive HIPAA privacy and security review, including HITECH and other applicable regulatory drivers such as PCI DSS, FTC Red Flags Rules and the FDA, etc.

The process includes a review of an organization’s risk management program and cyber readiness, and ensures consistency and accuracy of reporting on requirements for covered entities and business associates.

*EHNAC is the only organization with the ability to provide both EHNAC accreditation and HITRUST CSF certification.*
Why Choose EHNAC as Your HITRUST CSF Assessor?

• Using EHNAC for your HITRUST CSF assessment provides consistency between both certification and accreditation programs for HIPAA privacy and security compliance.
• Organizations achieving HITRUST certification will have 100% of their privacy and security credited to their EHNAC accreditation.
• Organizations that already have EHNAC accreditation will have developed the majority of their HIPAA-related HITRUST CSF privacy and security to apply to that certification.
• EHNAC site reviewers are also HITRUST practitioners, making it easier for organizations to undergo audits.
• Obtaining both HITRUST CSF certification and EHNAC accreditation at the same time significantly reduces the time, expense and redundancy needed to prepare documentation and undergo required site visits.
• EHNAC is participating on key HITRUST workgroups, advocating strong continuing education and industry requirements regarding privacy and security are communicated and included in future HITRUST CSF versions.
The Road to HITRUST: How EHNAC Supported InstaMed With a Clear Path to Certification
About InstaMed

Every healthcare clearinghouse and payment transaction, all in one place

Delivering healthcare payments to over 2/3 of the market

Processes tens of billions of dollars in healthcare payments annually

Over 99.99% uptime with 24/7 customer service support

Compliant, certified and audited at the highest levels for both healthcare and payment processing
Payment Channels in Healthcare

- Digital Wallets
  - Apple Pay
  - Android Pay

- Online Banking

- Online Portals

- Point of Sale
  - 40,000+ Retail Locations

- Automated Phone Pay
- Mobile and Tablet
- Mail-In Pay
The Healthcare Industry is at Greater Risk Than Ever Before

- Healthcare data breaches caused by hacking/IT incidents increased by 98% from 2015-2016
- 2016 saw the most healthcare data breaches than any other year on record
- 47% of healthcare organizations claim they are not confident in their ability to keep cloud data secure
- Ransomware increased 35% in 2015
- The healthcare industry is targeted by criminal attacks more than any other industry
- Over half a billion personal records were stolen or lost in 2015
- $6.2 billion is the estimated annual cost to healthcare of data breaches
Protecting You and Your Patients’ Data

• EHNAC Accredited Since 2006 – HNAP and FSAP
• Certified by HITRUST 2016
• First in healthcare to achieve PCI validation for P2PE v2.0
• Fully P2PE compliant solution – Coalfire Whitepaper
• Audited and certified at highest levels in industry
Healthcare Payments Milestones

- 2004: InstaMed founded by industry pioneers Bill Marvin and Chris Seib
- 2006: Payment processing launched with EHNAC Certification
- 2009: Certified for CAQH CORE Phase I & II
- 2010: Completed first SSAE16 SOC 1
- 2012: First company to achieve EHNAC Healthcare and Financial Accreditations
- 2013: First company to achieve CAQH CORE Phase III
- 2015: First in healthcare to launch EMV solution in compliance with the October 2015 regulation
- 2016: HITRUST Certification
  - First in healthcare to achieve PCI P2PE v2.0
  - Completed first SSAE16 SOC 2
EHNAC as a Foundation for HITRUST

• 100% of the EHNAC controls for privacy and security are covered within HITRUST
• About 70% of all EHNAC controls overlap with HITRUST controls
• EHNAC security controls completely cover HITRUST section 3 portable media security
• EHNAC covers many controls across HITRUST'S 19 domains
Planning

• EHNAC – 3 Months
  – 1 Month Document and Evidence Collection
  – 1 Month On-site visits (Offices, Data Centers, Service Providers)
  – 1 Month Review, Clarifications and Follow-up

• HITRUST
  – 3 Months Provide Domain Evidence
  – 1 Month Review and Further Requirements
  – 2 Months Submission, QA Fixes and Finalize Certification
HITRUST Acceptance?

• Contractual Requirements
  o Payors
  o Providers (ex: Texas)
• Accepted as a Standard
• Partially Accepted in Lieu of Other Documents
• Own Security Program – HITRUST and EHNAC not recognized yet
Healthcare’s Most Trusted Payments Network
Lee Barrett
Executive Director
EHNAC

Mark Krapels
Chief Operating Officer
Chief Security and Compliance Officer
InstaMed
Streamline EHNAC & HITRUST Assessments for Reduced Redundancy, Cost & Complexity

Debbie Hutchinson, Availity
Jay Trinckes, Coalfire
AGENDA

• Introductions
• About Availity & Coalfire
• Scenario
• Q&A
Who is Availity?

As an industry-leading health care information technology company, Availity serves an extensive network of health plans, providers, and technology partners nationwide through a suite of dynamic products built on a powerful, intelligent platform.

Availity integrates and manages the clinical, administrative, and financial data needed to fuel real-time coordination between providers, health plans, and patients in a growing value-based care environment.

Availity has been HITRUST certified since 2011.
EHNAC Accreditation

- Availity has been EHNAC certified since 2008 Healthcare Network Accreditation Program (HNAP) Electronic Healthcare Network (EHN) https://www.ehnac.org/accredited-organizations/.
- HNAP recognizes companies that perform claims clearinghouse or EDI gateway functions, including third-party administrators, billing services, payer-owned networks and other types of electronic health networks.
- Both Maryland and New Jersey require EHNAC accreditation for EHNs to conduct business in their states.
Mapping HITRUST and EHNAC

- In December 2015, Availity completed a joint SOC 2 and HITRUST assessment based on synergies between AICPA SOC 2 Trust Service Principles and HITRUST CSF version 7.
- Mapping the CSF to the SOC2 simplified the audit process resulting in reducing both costs and internal resource efforts.
- In December 2015, Availity started their EHNAC HNAP-EHN version 10.8 Self Assessment.
- Coalfire assisted with mapping controls between HITRUST and EHNAC.
Leveraging CSF with EHNAC Accreditation

- After mapping the EHNAC controls identified overlap between our HIPAA-related Privacy and Security criteria with HITRUST CSF.
- Additional EHNAC controls are used to determine compliance such as technical performance criteria include transaction monitoring and processing capacity, response timeliness and accuracy etc.
- April 2017, preparing for stacking the assessments with SOC reporting, HITRUST certification with CSF version 8.1, and EHNAC accreditation version 11.0.
Leveraging CSF with EHNAC Accreditation (cont’d)

- Streamlined the EHNAC accreditation process utilizing the HITRUST CSF helped reduce redundant assessments and associated costs and complexities.
- Reduced internal resources time spent managing repetitive and duplicative control testing HIPAA-related Privacy and Security criteria.
- Assisted with driving internal resource efficiencies.
Benefits of EHNAC and HITRUST Collaboration

“Coming from an organization that maintains both EHNAC Accreditation and HITRUST CSF Certification, this collaboration not only benefits us directly, but the entire industry by establishing the precedent for greater alignment of leading accreditation and certification organizations to eliminate redundancies which will reduce costs.”

Karin Lindgren, Senior Vice President and Chief Compliance Officer, at Availity.
JAY TRINCKES, COALFIRE
Practice Director, Healthcare & Life Sciences Practice

10+ years experience in cybersecurity, risk management, audit, vulnerability/penetration testing, business continuity, disaster recovery, and regulatory compliance.

Certifications

HITRUST Certified De-Identification Associate (CDA)

HITRUST CSF Practitioner (CCSFP)

Certified Information Systems Security Professional (CISSP)

Certified Information Systems Manager (CISM)

Certified in Risk and Information Systems Control (CRISC)

National Security Agency (NSA) – INFOSEC Assessment Methodology (IAM)/INFOSEC Evaluation Methodology (IEM)

Experience/Accomplishments

Former CISO, law enforcement officer, and founding member of an information security consulting firm

Author

The Definitive Guide to Complying with the HIPAA/HITECH Privacy and Security Rules

How Healthcare Data Privacy Is Almost Dead ... and What Can Be Done to Revive It
COALFIRE AT A GLANCE

- 500+ security professionals
- Pure-play cybersecurity firm for more than 16 years
- More than 1,500 clients in US and Europe
- Technologists and innovators
- Industry- and client-focused advisors and partners
STREAMLINING ASSESSMENTS
HITRUST CSF Maps to Other Frameworks/Regulations

- AICPA
- COBIT
- CSA
- CMSR
- ISO
- CORE
- HIPAA
- TAC
- MA
- IRS
- NIST
- NIST CSF
- DE-ID FRAMEWORK
- PMIDSP
- FEDERAL
- PCI
- CIS
- THSC
- REDFLAGS
- NRS
- JCAHO
Efficiency

• Availility HITRUST Certified
• Needed EHNAC Certification
• Although Coalfire doesn’t provide EHNAC Certifications, assisted Availility in prep work
• Able to leverage existing controls for HITRUST to demonstrate compliance for EHNAC
Q & A

“Cybersecurity is everyone’s concern, but it’s our business.”

Deborah.Hutchinson@Availity.com
Jay.Trinckes@Coalfire.com
Visit www.HITRUSTAlliance.net for more information

To view our latest documents, visit the Content Spotlight