Indiana All Payer Claims Database (IN APCD)

IN APCD Security and Certifications

Jonathan Handsborough, MBA, MBB-6σ
Executive Director, APCD, Indiana Department of Insurance

IN APCD Security and Certifications

HIPAA: The **Health Insurance Portability and Accountability Act (HIPAA)** of 1996 establishes federal standards protecting sensitive health information from disclosure without patient's consent. The US Department of Health and Human Services issued the HIPAA Privacy Rule to implement HIPAA requirements. The HIPAA Security Rule protects specific information cover the Privacy Rule.

Source - cdc.gov

IN APCD Security and Certifications

QE: **Qualified Entity** Certification program (also known as the Medicare Data Sharing for Performance Measurement Program) enables organizations to receive Medicare claims data under Parts A, B, and D for use in evaluating provider performance.

Source - cms.gov

IN APCD Security and Certifications

ISO: The **International Organization for Standardization (ISO)** is an independent, non-governmental international organization that develops and publishes international standards. International standards ensure that the products and services you use daily are safe, reliable, and of high quality. They also guide businesses in adopting sustainable and ethical practices, helping to create a future where your purchases not only perform excellently but also safeguard our planet. In essence, standards seamlessly blend quality with conscience, enhancing your everyday experiences and choices.

Source - iso.org

IN APCD Security and Certifications

NIST: **National Institute of Standards and Technology** develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies and the broader public.

Source - nist.gov

IN APCD Security and Certifications

HITRUST: HITRUST stands for **Health Information Trust Alliance**. HITRUST is a healthcare-specific common security framework covering the relevant components of security frameworks from the International Organization for Standardization (ISO), the Payment Card Industry (PCI), NIST, HIPAA, and others.

Source - in.gov/idoi

IN APCD Security and Certifications

PCI: The **Payment Card Industry Data Security Standard** (PCI DSS) is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures associated with credit card account data. This comprehensive standard is intended to help organizations proactively protect customer credit card account data that is either stored, processed, or transmitted.

Source - osc.nc.gov

IN APCD Security and Certifications

AWS Data Center: **Amazon Web Services (AWS) data center** is a physical location that stores computing machines and their related hardware equipment. It contains the computing infrastructure that IT systems require, such as servers, data storage drives, and network equipment. It is the physical facility that stores any company's digital data.

Source - aws.amazon.com

IN APCD Security and Certifications

AICPA/SOC: **System and Organization Controls (SOC)** reports are intended to provide user organizations with reasonable assurance that controls within the service organization are accurately described, properly designed, and operating effectively based on the overall operating environment.

Source - ignet.gov

IN APCD Security and Certifications

FedRAMP: **FedRAMP (Federal Risk and Authorization Management Program)** is an assessment for 3rd Party cloud computing service providers that are contracted to provide their services to Government Agencies.

Source - ignet.gov

IN APCD Security and Certifications

FIPS Cryptography: **Federal Information Processing Standards (FIPS)** are standards for federal computer systems that are developed by the National Institute of Standards and Technology (NIST) and approved by the Secretary of Commerce in accordance with the Information Technology Management Reform Act of 1996 and Computer Security Act of 1987. These standards are developed when there are no acceptable industry standards or solutions for a particular government requirement. Although FIPS are developed for use by the Federal Government, many in the private sector voluntarily use these standards.

Cryptography refers to **cryptographic** modules that meet specific security requirements set by the U.S. government. These standards are developed by the National Institute of Standards and Technology (NIST) and are used to protect sensitive information in federal computer and telecommunication systems.

Source - nist.gov

IN APCD Security and Certifications

Defense Information Agency: The **Defense Information Systems Agency (DISA)** provides a global infrastructure for information sharing and communication across the Department of Defense, from the President on down.

Source - usa.gov

Contact Us

Indiana All Payer Claims Database
Indiana Department of Insurance
IDOI Website: www.in.gov/idoi/apcd/
IN APCD Website: apcd.idoi.in.gov
Email: apcd@idoi.in.gov
317-232-3619

Indiana APCD Team

Jonathan Handsborough MBA, MBB-6σ
Executive Director

Diana Ou
Project Manager

Michele Miller
Outreach Liaison

Stacy French
Administrative Assistant

Suraksha Adhikari
Data Scientist

D. Alex Hoyte
Sr Data Analyst – Health

Laura Yahya
Sr Data Analyst - Intake