Glossary of Terms

Access Control - The process of granting or denying specific requests for access to information, related information processing services, and specific physical facilities.

Antivirus Software – A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents.

Business Case - A documented, structured proposal for business improvement that is prepared to facilitate a selection decision for a proposed investment.

Business Needs Statement - A statement identifying the business need for a proposed investment or project.

Capital Planning and Investment Control (CPIC) - A structured approach to managing IT investments.

Centralized Patching - A centralized system that allows an agency to remotely and automatically deploy critical security patch updates to computers on the network.

Continuous Monitoring - The process of maintaining a current security status for one or more information systems or for an entire suite of information systems.

Data-At-Rest - All data in computer storage.

Data-In-Motion - The transfer of data between all copies and versions of the original file.

Develop, Modify, Enhance (DME) – In the arena of IT activity, any project that involves development, modification, or enhancement to a process or a product.

Digital Divide – The gap between those with IT access and those with limited access or no access at all.

Earned Value Management (EVM) – An objective measurement of how much work has been accomplished on a project in relation to the project's schedule and budget.

Electronic Health Record (EHR) - A software product that uses a computer graphical user interface to display various clinical functions.

Encryption – The process of changing plain text into cipher text for the purpose of security or privacy.

Enterprise Performance Life Cycle (EPLC) – A framework to enhance IT governance through application of sound investment and project management principles and industry best practices.

Health Information Technology (HIT) - The use of computers and technology in a healthcare setting.

ICD-10 - Standard diagnostic classification for all general epidemiological, many health management purposes, and clinical use.

Information Systems Advisory Committee (ISAC) - develops priorities and provides guidance to the Director of the IHS.

Information Technology Investment Review Board (ITIRB) – The official IHS reviewing body for IT investments, including all major initiatives, funding, and expenditures.

Interoperability – The ability to share patient health information with external systems.

Intrusion Detection – The process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents.

Intrusion Prevention - Monitoring the events occurring in a system, analyzing for signs of possible incidents, and attempting to stop detected possible incidents.

IT Governance – An IHS process focused on IT investments and their performance and risk management.

IT Investment - An organizational initiative to employ or produce IT assets. It incurrs costs, realizes benefits, has a schedule of project activities and deadlines, and involves risks associated with engaging in the initiative.

Lines of Business - A set of one or more highly related products which service a particular customer transaction or business need.

Master Person Index - A computerized version of the traditional paper model used to store patient medical information.

Meaningful Use (MU) - Meaningful use of certified EHR technologies.

mHealth Services - The practice of medical and public health, supported by mobile devices.

Multi-dimensional Database - A type of database that is optimized for data warehouse and online analytical processing applications.

Penetration Testing – A test methodology in which assessors attempt to circumvent the security features of an information system.

Personal Health Record (PHR) - A functionality that allows patients to manage their health information in an on-line format.

Resource and Patient Management System (RPMS) - The IHS integrated solution for management of clinical, business practice, and administrative information in healthcare facilities.

Secure Socket Layer (SSL) – A protocol used for protecting private information during transmission over the Internet.

Steady-State Operations - An operational variable that does not change with time.

Store and Forward Telehealth - The ability to acquire, store, and forward digital images for healthcare reporting.

Technical Review Board (TRB) – A board responsible for evaluating and scoring the technical soundness of proposed projects and identifying opportunities to leverage and reuse existing projects.