ABBREVIATIONS LIST

ADPS  Automated Data Processing System
AES  Advanced Encryption Standard
DES  Data Encryption Standard
DLP  Discrete Logarithm Problem
ECC  Elliptic Curve Cryptography
EDI  Electronic Data Interchange
EHDMa  E-Health Decision Making Algorithm
HIC  Health Insurance Card
HIPPA  Health Insurance Portability and Accountability Act
HS  Hospital Server
HSPS  Health Services Portal Server (HSPS).
HTTPS  Hyper Text Transport Protocol Secure
IC  Insurance Company
IOT  Internet of Things
JAR  Java Archive
JDBC  Java DataBase Connectivity
JSP  Java Server Pages
MASDMA  Multi-Attribute Secure Decision Making Algorithm
RFID  Radio Frequency Identification
RSA  Rivest Shamir Adleman
RSA  Rivest Shamir Adleman (Cryptographic System)
S²FRSA  Selective Secure Field RSA
TP  Third Party
$V_k$        Verification Key

WAR        Web Archive

AES – is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001, AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits

Authorization—it is the process by which an entity such as a user or a server gets permission to perform a restricted operation.

Authentication—it verifies the identity of a user or service

Asymmetric Cryptosystem—is cryptography in which a pair of keys is used to encrypt and decrypt a message so that it arrives securely.

Security—it is the combination of confidentiality (the prevention of the unauthorized disclosure of information), integrity (the prevention of the unauthorized amendment or deletion of information), and availability (the prevention of the unauthorized withholding of information).

Cryptography—it is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.

Cryptanalysis—refers to the study of ciphers, ciphertext, or cryptosystems (that is, to secret code systems) with a view to finding weaknesses in them that will permit retrieval of the plaintext from the ciphertext, without necessarily knowing the key or the algorithm. This is known as breaking the cipher, ciphertext, or cryptosystem.

Data authenticity – A security property indicating that data originates from the claimed source.

Data Remanence – is defined as the residual representation of data that has been in some way nominally erased or removed. This residue may be due to data being left intact by a nominal delete operation, or through physical properties of the storage medium. Data remanence may make inadvertent disclosure of sensitive information possible, if any storage media is released into an uncontrolled environment such as thrown in the trash or given to a third party.

Data confidentiality—A security property indicating that data cannot be viewed by an unauthorized entity.
**Data integrity**— A security property indicating that data has not been altered by an Unauthorized entity.

**Decryption** — mechanism of converting cipher text to plain text

**Digital Signature** — it is a mathematical scheme for demonstrating the authenticity of a digital message or document

**DoS** — Denial of Service; a security attack on a system that results in its temporary unavailability and inability to perform its normal services. The most common type of DoS attacks is flooding the system with excessive traffic to prevent it from servicing normal and legitimate requests.

**DES** — Data Encryption Standard is a widely-used method of data encryption using a private (secret) key. DES applies a 56-bit key to each 64-bit block of data for encryption, both sender and receiver should use same private key for encryption and decryption.

**Encryption** — mechanism of converting plain text to cipher text

**e-Medical Health Insurance System** — Electronic Medical Health Insurance System; a set of treatments and commercial transactions performed over a communication network, such as the Internet.

**e-Medical-diagnosis** — Electronic Medical-diagnosis; any Medical-diagnosis product that is possible to represent in electronic form and transmit over the Internet. For example, MRI, ECG and X-ray.

**e-Payments** — Electronic Payments; a set of commercial transactions performed over communication network, such as the Internet.

**e-Medical transactions** — A security property that guarantees that each of the parties involved in an transaction receives its expected information/item or no party receives anything valuable.

**Health Insurance** - relates to a type of insurance that essentially covers your medical expenses. A health insurance policy like other policies is a contract between an insurer and an individual / group in which the insurer agrees to provide specified health insurance cover at a particular “premium” subject to terms and conditions specified in the policy.
Internet of Things – is a computing concept that describes a future where every day physical objects will be connected to the Internet and will be able to identify themselves to other devices.

SSL/TLS – Secure Socket Layer/Transport Layer Security protocol; a network security protocol providing authenticated, confidential and integrity-protected communication over the Internet. It is supported by current Web browsers and widely accepted by e-commerce community for securing e-commerce applications.

Symmetric Cryptosystem – cryptographic technique that uses the same cryptographic keys for both encryption of plaintext and decryption of ciphertext.