

# ALLHEALTHLOGIC, LLC

## CADX<sup>®</sup>

### CLAIMS ATTACHMENT DOCUMENT EXCHANGE

#### INFORMATION SECURITY REQUIREMENTS

##### **A. General Requirements**

All AHL Clients are required to implement and maintain appropriate safeguards and controls and exercise due diligence to protect patient data against unauthorized access, use and/or disclosure. The degree of such protection is determined by:

- Federal and State legal or regulatory requirements
- Industry "best practices"
- Sensitivity of the data
- Relative level of risk
- AHL's Baseline Protection Requirements (listed below)

In the event that additional security procedures are reasonably requested by Client, upon prior written approval by Client of any additional costs or charges, AHL shall perform such additional security procedures. Client shall have the right to audit such security procedures once each year during the term of the Agreement. Other CADX<sup>®</sup> responsibilities include

- Maintain the Certificate Authority under which secure digital certificates, logons and passwords are issued
- Maintain the overall security of the CADX<sup>®</sup> portal
- Maintain the Client access profiles to control which staff has access to which Clients.
- Transaction logging of all activity on the CADX<sup>®</sup> portal to protect the privacy and confidentiality of patient health information.

##### **B. Information Security Requirements Relationship to Confidentiality Addendum**

These requirements are in addition to any requirements which are set forth in the Privacy and Confidentiality Addendum Exhibit I1 between the Client and AHL.

##### **C. Definitions**

The following definitions apply to these Information Security Requirements:

1. "AHL Data" is data provided or made available to a Client by AHL, data collected, created, or derived by a Client on behalf of AHL or data pertaining to AHL internal operations, infrastructure, or business functions.
2. "AHL Processing" is information processing performed using AHL Data, information processing performed on behalf of AHL or information processing which directly or indirectly supports AHL contracted functions.
3. "AHL Processing Resources" are Client-supplied or Client-operated information processing resources (e.g., systems, storage media, hardcopies, network infrastructures, etc.) which are used, either directly or indirectly, in support of AHL Processing.
4. "Outsourced Processing" occurs if an agreement requires a Client to perform any form of information collection or processing on behalf of AHL. Examples include, but are not limited to:
  - Clearinghouses other than AHL
  - Data collection websites

#### **D. Security Requirements for Type of Agreement**

1. Licensing or Purchase of Software Products. The Client will notify AHL if any software product maintenance, patches, revisions, or upgrades materially change the security control mechanisms originally implemented by CADX®.
2. Software Development. Any software developed for AHL is required to be developed and implemented in accordance with the same standards and criteria required of software developed "in-house" by AHL. The software must satisfy the appropriate AHL Information Security Policies and Guidelines, copies of which will be provided to the Client if a procurement agreement requires software development.

## E. Baseline Protection Requirements for Outsourced Processing

All Outsourced Processing Clients must meet the following Baseline Protection Requirements:

**Data Transmission** The Client will implement encryption, in accordance with standards mutually agreed upon between AHL and the Client, for all transmission of AHL Data via public networks (e.g., the Internet). Such transmissions include, but are not limited to:

- a) Sessions between web browsers and web servers
- b) Email containing AHL Data (including passwords)
- c) Transfer of files via the Internet (e.g., FTP)

Acceptable encryption algorithms and keylengths:

Type	Minimum keysize
3DES	112
CAST	128
DSS/DH	1024
IDEA	128
RC2	128
RSA	1024
SSL (V3 or higher)	
May also be referred to as TLS (V1.0 or higher)	128

Such other types as may be specified by AHL from time to time.

### Access Control

- 1) The Client will implement appropriate access control mechanisms to prevent all access to AHL Data and/or Processing Resources, except by:
  - a) Authorized users,
  - b) Client personnel who have a "need to access" to perform a particular function in support of AHL CADX<sup>®</sup> Processing.The access and privileges granted shall be the minimum necessary to perform the assigned functions.
- 2) The Client will maintain and use mechanisms and processes for detecting, recording, analyzing, and resolving unauthorized attempts to access AHL Data or CADX<sup>®</sup> Processing Resources. AHL will be notified of all actual or suspected instances of deliberate unauthorized attempts (both successful and unsuccessful) to access AHL Data or Processing Resources.

### Identification and Authentication

- 1) All access to AHL Data and CADX<sup>®</sup> Processing Resources must be identified and authenticated. AHL will issue a digital certificate to each Client for (I&A) authentication to the secure access areas of CADX<sup>®</sup>. In addition, AHL will issue an individual, unique user ID and an individual password for authentication.

Once connected to the secure site the user will have the option of resetting their password.

- 2) The Client will implement procedures to ensure the protection, integrity, and soundness of passwords.

**Account Administration**

- 1) The client will implement formal processes for requesting, approving, and administering accounts and access privileges for AHL Processing Resources.  
These processes are required for both AHL-related accounts and Client internal accounts for AHL CADX<sup>®</sup> Processing Resources.

- 2) AHL must approve account requests from AHL employees or on-site contractors.

**Physical Security**

The Client will implement appropriate physical security controls (including facility and environmental) to prevent unauthorized physical access to AHL Processing Resources. Media containing AHL Data (e.g., paper, tapes, removable media, etc.) must be protected against unauthorized physical access. This protection must be maintained before, during and after use, storage, transportation, and/or disposition/destruction, as applicable.

**Personnel Security**

- 1) All Client employees, contractors and agents who have, or may be expected to have, access to AHL Data shall be required to comply with the provisions of any Confidentiality Agreement to which the Client and AHL are parties.
- 2) The Client will ensure that its employees and contractors remain aware of industry standard security practices, and of its and their responsibilities for protecting AHL Data.

**Infrastructure Protection**

The Client will implement industry standard procedures to protect the Client's processing infrastructure. Example include, but are not limited to:

- a) Formal security program (policies, standards, processes, etc.)
  - b) Processes for being aware of, and implementing, security patches and fixes.
  - c) Router filters, firewalls, and other mechanisms to restrict access to the Client's information processing infrastructure
- Processes to prevent, detect, and eradicate malicious code (e.g., viruses, etc), and to notify AHL of instances of malicious code detected on AHL Processing Resources or affecting AHL Data.

## Requirements of All Payer Contracts Involving Medicare

In addition to the provisions above, in the event Client in the performance of its obligations under the Agreement will have access to information concerning Medicare beneficiaries whose health care benefits are provided by or through Client, Client shall comply with the Internet Security Policy issued on November 24, 1998 by the Centers for Medicare and Medicaid ("CMS") [formerly, Health Care Financing Administration ("HCFA")] of the U.S. Department of Health and Human Services (the "CMS Internet Security Policy"). Under the CMS Internet Security Policy, if the Client is to use the Internet to transmit "CMS Privacy Act Protected and/or other sensitive CMS information", the following conditions must be met:

1. An acceptable method of encryption must be used to provide for the confidentiality and integrity of the data;
2. Acceptable authentication procedures must be used to assure that the sender and recipient of the data are authorized to receive and decrypt the information; and
3. Acceptable identification procedures must be used to assure that both the sender and recipient of the data are known to each other.

**CMS Privacy Act Protected and/or other sensitive CMS information** includes, but is not limited to, (a) **all individually identifiable data** held in systems of records, (b) information for which unauthorized disclosure would constitute a clearly unwarranted invasion of personal privacy, (c) payment information used to authorize or make cash payments, (d) proprietary information, and (e) highly sensitive computerized correspondence and documents.

The currently acceptable encryption, authorization and identification approaches are set forth on **Attachment A** hereto. Needless to say, CMS has reserved the right to increase these levels as technology advances.

In addition to the foregoing, it should be noted that local site networks which may be accessed via the Internet (whether or not they transmit information) must also be protected against attack and penetration from the Internet through the use of firewalls.

It should also be noted that, under CMS's Internet Security Policy, organizations desiring to use the Internet for the transmission of protected information must notify CMS.

In summary, a Client who uses a site which is accessible via the Internet must have firewalls in place. A Client who is going to transmit protected information over the Internet must utilize encrypted transmittals, and must satisfy CMS's minimum standards for encryption, authentication and identification. CMS must be notified.

## ATTACHMENT A

### ACCEPTABLE ENCRYPTION APPROACHES

Note: As of November 1998, a level of encryption protection equivalent to that provided by an algorithm such as Triple 56 bit DES (defined as 112 bit equivalent) for symmetric encryption, 1024 bit algorithms for asymmetric systems, and 160 bits for the emerging Elliptical Curve systems is recognized by CMS as minimally acceptable. CMS reserves the right to increase these minimum levels when deemed necessary by advances in techniques and capabilities associated with the processes used by attackers to break encryption (for example, a brute-force exhaustive search).

#### **HARDWARE-BASED ENCRYPTION:**

1. Hardware encryptors - While likely to be reserved for the largest traffic volumes to a very limited number of Internet sites, such symmetric password "private" key devices (such as link encryptors) are acceptable.

#### **SOFTWARE-BASED ENCRYPTION:**

2. Secure Sockets Layer (SSL) (Sometimes referred to as Transport Layer Security - TLS) implementations - At a minimum SSL level of Version 3.0, standard commercial implementations of PKI, or some variation thereof, implemented in the Secure Sockets Layer are acceptable.
3. S-MIME - Standard commercial implementations of encryption in the e-mail layer are acceptable.
4. In-stream - Encryption implementations in the transport layer, such as pre-agreed passwords, are acceptable.
5. Offline - Encryption/decryption of files at the user sites before entering the data communications process is acceptable. These encrypted files would then be attached to or enveloped (tunneled) within an unencrypted header and/or transmission.

### ACCEPTABLE AUTHENTICATION APPROACHES

**AUTHENTICATION** (This function is accomplished over the Internet, and is referred to as an "in-band" process.)

1. Formal Certificate Authority-based use of digital certificates is acceptable.
2. Locally-managed digital certificates are acceptable, providing, all parties to the communication are covered by the certificates.

3. Self-authentication, as in internal control of symmetric "private" keys, is acceptable.
4. Tokens or "smart cards" are acceptable for authentication. In-band tokens involve overall network control of the token database for all parties.

### **ACCEPTABLE IDENTIFICATION APPROACHES**

**IDENTIFICATION** (The process of identification takes place outside of the Internet connection and is referred to as an "out-of-band" process.)

1. Telephonic identification of users and/or password exchange is acceptable. Exchange of passwords and identities by U.S. Certified Mail is acceptable.
2. Exchange of passwords and identities by bonded messenger is acceptable.
3. Direct personal contact exchange of passwords and identities between users is acceptable.
4. Tokens or "smart cards" are acceptable for identification. Out-of-band tokens involve local control of the token databases with the local authenticated server vouching for specific local users.