HEALTH CARE FINANCING ADMINISTRATION (HCFA)
7500 SECURITY BOULEVARD
BALTIMORE, MARYLAND 21244

DATE OF ISSUANCE: November 24, 1998

HCFA INTERNET SECURITY POLICY

SUBJECT: Internet Communications Security and Appropriate Use Policy and Guidelines for HCFA Privacy Act-protected and other Sensitive HCFA Information.

1. Purpose.

This bulletin formalizes the policy and guidelines for the security and appropriate use of the Internet to transmit HCFA Privacy Act-protected and other sensitive HCFA information.

2. Effective Date.

This bulletin is effective as of the date of issuance.

3. Expiration Date.

This bulletin remains in effect until superseded or canceled.

4. Introduction.

The Internet is the fastest growing telecommunications medium in our history. This growth and the easy access it affords has significantly enhanced the opportunity to use advanced information technology for both the public and private sectors. It provides unprecedented opportunities for interaction and data sharing among health care providers, HCFA contractors, HCFA components, State agencies acting as HCFA agents, Medicare and Medicaid beneficiaries, and researchers. However, the advantages provided by the Internet come with a significantly greater element of risk to the confidentiality and integrity of information. The very nature of the Internet communication mechanisms means that security risks cannot be totally eliminated. Up to now, because of these security risks and the need to research security requirements vis-a-vis the Internet, HCFA has prohibited the use of the Internet for the transmission of all HCFA Privacy Act-protected and other sensitive HCFA information by its components and

Medicare/Medicaid partners, as well as other entities authorized to use this data.

The Privacy Act of 1974 mandates that federal information systems must protect the confidentiality of individually-identifiable data. Section 5 U.S.C. §552a (e) (10) of the Act is very clear; federal systems must: "...establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." One of HCFA's primary responsibilities is to assure the security of the Privacy Act-protected and other sensitive information it collects, produces, and disseminates in the course of conducting its operations. HCFA views this responsibility as a covenant with its beneficiaries, personnel, and health care providers. This responsibility is also assumed by HCFA's contractors, State agencies acting as HCFA agents, other government organizations, as well as any entity that has been authorized access to HCFA information resources as a party to a Data Release Agreement with HCFA.

However, HCFA is also aware that there is a growing demand for use of the Internet for inexpensive transmission of Privacy Act-protected and other sensitive information. HCFA has a responsibility to accommodate this desire as long as it can be assured that proper steps are being taken to maintain an acceptable level of security for the information involved.

This issuance is intended to establish the basic security requirements that must be addressed for use of the Internet to transmit HCFA Privacy Act-protected and/or other sensitive HCFA information.

The term "HCFA Privacy Act-protected Data and other sensitive HCFA information" is used throughout this document. This phrase refers to data which, if disclosed, could result in harm to the agency or individual persons. Examples include:

- All individually identifiable data held in systems of records. Also included are automated systems of records subject to the Privacy Act, which contain information that meets the qualifications for Exemption 6 of the Freedom of Information Act; i.e., for which unauthorized disclosure would constitute a "clearly unwarranted invasion of personal privacy" likely to lead to specific detrimental consequences for the individual in terms of financial, employment, medical, psychological, or social standing.
- Payment information that is used to authorize or make cash payments to individuals or organizations. These data are usually stored in production application files and systems, and include benefits information, such as that found

at the Social Security Administration (SSA), and payroll information. Such information also includes databases that the user has the authority and capability to use and/or alter. As modification of such records could cause an improper payment, these records must be adequately protected.

- Proprietary information that has value in and of itself and which must be protected from unauthorized disclosure.

- Computerized correspondence and documents that are considered highly sensitive and/or critical to an organization and which must be protected from unauthorized alteration and/or premature disclosure.

5. Policy

This Guide establishes the fundamental rules and systems security requirements for the use of the Internet to transmit HCFA Privacy Act-protected and other sensitive HCFA information collected, maintained, and disseminated by HCFA, its contractors, and agents.

It is permissible to use the Internet for transmission of HCFA Privacy Act-protected and/or other sensitive HCFA information, as long as an acceptable method of encryption is utilized to provide for confidentiality and integrity of this data, and that authentication or identification procedures are employed to assure that both the sender and recipient of the data are known to each other and are authorized to receive and decrypt such information. Detailed guidance is provided below in item 7.

6. Scope.

This policy covers all systems or processes which use the Internet, or interface with the Internet, to transmit HCFA Privacy Act-protected and/or other sensitive HCFA information, including Virtual Private Network (VPN) and tunneling implementations over the Internet. Non-Internet Medicare/Medicaid data communications processes (e.g., use of private or value added networks) are not changed or affected by the Internet Policy.

This policy covers Internet data transmission only. *It does not cover local data-at-rest or local host or network protections. Sensitive data-at-rest must still be protected by all necessary measures, in conformity with the guidelines/rules which govern the entity's possession of the data. Entities must use due diligence in exercising this responsibility.*

Local site networks must also be protected against attack and penetration from the

Internet with the use of firewalls and other protections. Such protective measures are outside the scope of this document, but are essential to providing adequate local security for data and the local networks and ADP systems which support it.[1]

7. Acceptable Methods

HCFA Privacy Act-protected and/or other sensitive HCFA information sent over the Internet must be accessed only by authorized parties. Technologies that allow users to prove they are who they say they are (authentication or identification) and the organized scrambling of data (encryption) to avoid inappropriate disclosure or modification must be used to insure that data travels safely over the Internet and is only disclosed to authorized parties. Encryption must be at a sufficient level of security to protect against the cipher being readily broken and the data compromised. The length of the key and the quality of the encryption framework and algorithm must be increased over time as new weaknesses are discovered and processing power increases.

User authentication or identification must be coupled with the encryption and data transmission processes to be certain that confidential data is delivered only to authorized parties. There are a number of effective means for authentication or identification which are sufficiently trustworthy to be used, including both in-band authentication and out-of-band identification methods. Passwords may be sent over the Internet only when encrypted.

[1] We note that the Health Insurance Portability and Accountability Act of 1996 (HIPAA) calls for stringent security protection for electronic health information both while *maintained and while in transmission*. The proposed Security Standard called for by HIPAA was published in the Federal Register on August 12, 1998. The public had until October 13, 1998, to comment on the proposed regulation. Based on public comments, a final regulation is planned for late 1999. Policy guidance contained in this bulletin is consistent with the proposed HIPAA security requirements.

ENCRYPTION MODELS AND APPROACHES

Figure 1 depicts three generalized configurations of connectivity to the Internet. The generic model is not intended to be a literal mirror of the actual Internet interface configuration, but is intended to show that the encryption process takes place prior to information being presented to the Internet for transmission, and the decryption process after reception from the Internet. A large organization would be very likely to have the Internet Server/Gateway on their premises while a small organization would likely have only the Internet Client, e.g., a browser, on premises with the Internet Server at an Internet Service Provider (ISP). The Small User and Large User examples offer a more detailed depiction of the functional relationships involved.

The Encryption/Decryption process depicted graphically represents a number of different approaches. This process could involve encryption of files prior to transmittal, or it could be implemented through hardware or software functionality. The diagram does not intend to dictate how the process is to be accomplished, only that it must take place prior to introduction to the Internet. The “Boundary” on the diagrams represents the point at which security control passes from the local user. It lies on the user side of the Internet Server and may be at a local site or at an Internet Service Provider depending upon the configuration.

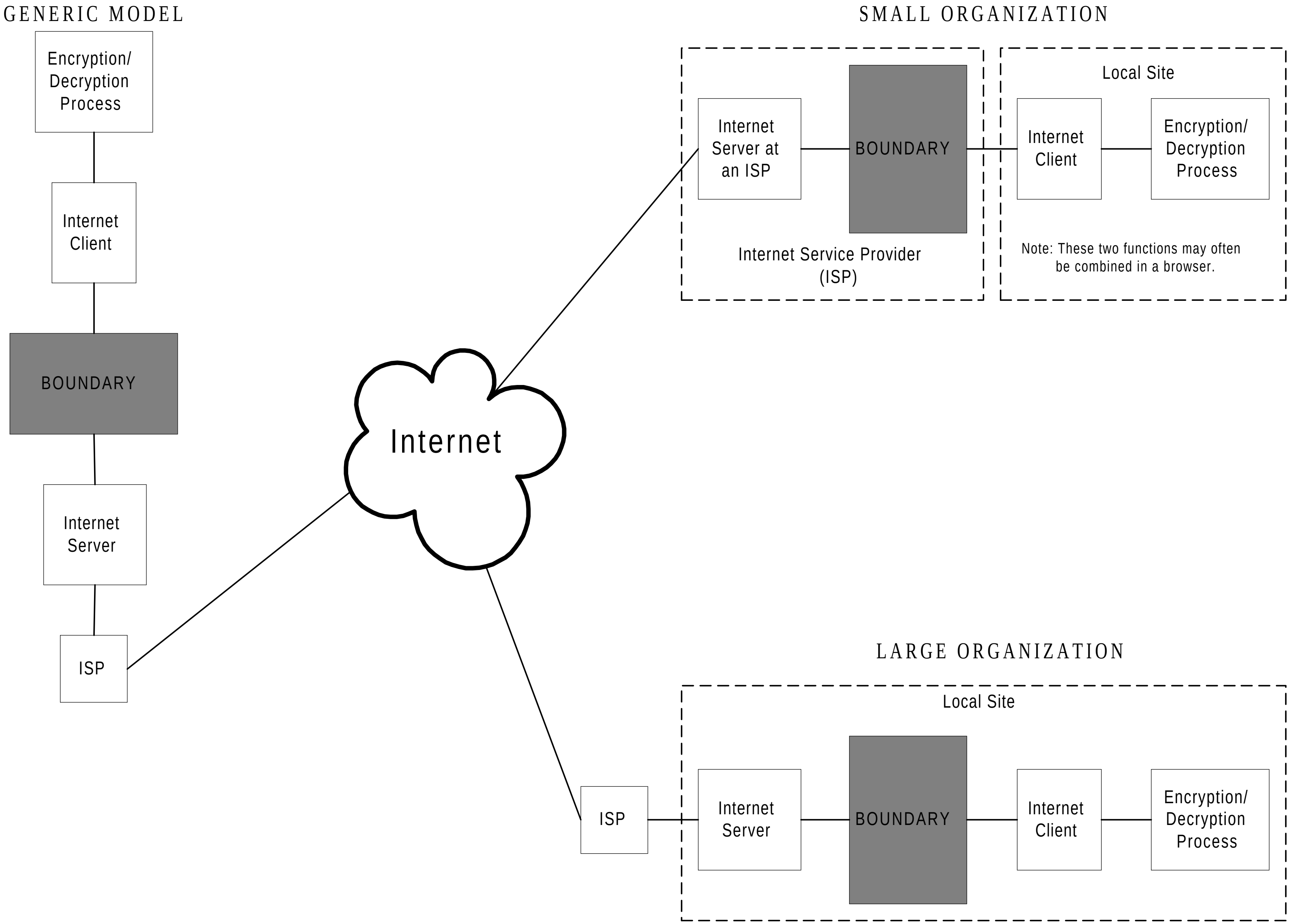
GENERIC MODEL
Encryption/ Decryption Process
Internet Client
BOUNDARY
Internet Server
ISP
Internet
SMALL ORGANIZATION
Internet Server at an ISP
BOUNDARY
Internet Service Provider (ISP)
Local Site
Internet Client
Encryption/ Decryption Process
Note: These two functions may often be combined in a browser.
LARGE ORGANIZATION
Local Site
ISP
Internet Server
BOUNDARY
Internet Client
Encryption/ Decryption Process

FIGURE 1: INTERNET COMMUNICATIONS EXAMPLES

Acceptable Approaches to Internet Usage

The method(s) employed by all users of HCFA Privacy Act-protected and/or other sensitive HCFA information must come under one of the approaches to encryption and at least one of the authentication or identification approaches. The use of multiple authentication or identification approaches is also permissible. These approaches are as generic as possible and as open to specific implementations as possible, to provide maximum user flexibility within the allowable limits of security and manageability.

Note the distinction that is made between the processes of “authentication” and “identification”.   In this Internet Policy, the terms "Authentication" and "Identification" are used in the following sense. They should not be interpreted as terms of art from any other source. Authentication refers to generally automated and formalized methods of establishing the authorized nature of a communications partner over the Internet communications data channel itself, generally called an "in-band process." Identification refers to less formal methods of establishing the authorized nature of a communications partner, which are usually manual, involve human interaction, and do not use the Internet data channel itself, but another "out-of-band" path such as the telephone or US mail.

The listed approaches provide encryption and authentication/identification techniques which are acceptable for use in safeguarding HCFA Privacy Act-protected and/or other sensitive HCFA information when it is transmitted over the Internet.

In summary, a complete Internet communications implementation must include *adequate encryption,* employment of *authentication or identification* of communications partners, and a management scheme to incorporate *effective password/key management* systems.

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 HCFA as minimally acceptable. HCFA 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.

2. Exchange of passwords and identities by U.S. Certified Mail is acceptable.

3. Exchange of passwords and identities by bonded messenger is acceptable.

4. Direct personal contact exchange of passwords and identities between users is acceptable.

5. 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.

8. REQUIREMENTS AND AUDITS

Each organization that uses the Internet to transmit HCFA Privacy Act-protected and/or other sensitive HCFA information will be expected to meet the stated requirements set forth in this document.

All organizations subject to OMB Circular A-130 are required to have a Security Plan. All such organizations must modify their Security Plan to detail the methodologies and protective measures if they decide to use the Internet for transmittal of HCFA Privacy Act-protected and/or other sensitive HCFA information, and to adequately test implemented measures.

HCFA reserves the right to audit any organization's implementation of, and/or adherence to the requirements, as stated in this policy. This includes the right to require that any organization utilizing the Internet for transmission of HCFA Privacy Act-protected and/or other sensitive information submit documentation to demonstrate that they meet these requirements.

9. ACKNOWLEDGMENT OF INTENT

Organizations desiring to use the Internet for transmittal of HCFA Privacy Act-protected and/or other sensitive HCFA information must notify HCFA of this intent. An e-mail address is provided below to be used for this acknowledgment. An acknowledgment must include the following information:

Name of Organization
Address of Organization
Type/Nature of Information being transmitted
Name of Contact (e.g., CIO or accountable official)
Contact's telephone number and e-mail address

For submission of acknowledgment of intent, send an e-mail to: internetsecurity@hcfa.gov. Internal HCFA elements must proceed trhough the usual HCFA system and project development process.

10. POINT OF CONTACT

For questions or comment, write to:

Office of Information Services, HCFA
Security and Standards Group
Division of HCFA Enterprise Standards -Internet
7500 Security Boulevard
Baltimore, MD 21244