The Health Insurance Portability & Accountability Act, the Gramm-Leach-Bliley Act, & CKM®

Table of Contents

BACKGROUND

The purpose of this memorandum is to summarize selected elements of the Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley Act (GLBA) as they relate to TecSec's Constructive Key Management® (CKM®) technology. It is intended to be a brief overview of the salient parts of these complex laws where TecSec can assist its clients with compliance. This memorandum should be reviewed in the context of copies of the actual legislation, implementing regulations, presentation materials, press releases, and meetings/discussions with TecSec regarding its role with the Health Care Financing Administration (HCFA).

CKM & HIPAA

1 Introduction ~ CKM & HIPPA

TecSec® provides methods, software and capabilities that enable organizations to comply with HIPAA. This software is enabled by TecSec's landmark encryption and information access management technology called Constructive Key Management® (CKM). Please visit http://www.tecsec.com for additional information on the company, its technology and its products.

Over the past ten months (and in particular, August, October and December 2000, and April 2001) there have been significant developments with respect to HIPAA's governing regulations. Implementing regulations related to HIPAA mandate sweeping changes in the way healthcare organizations maintain, transmit and store electronic medical information, allowing for severe civil and criminal penalties for noncompliance. For example, in October 2000 final regulations outlining new standards and protocols for electronic transactions (e.g., e-filings of medical claims) became effective. In December 2000, sweeping patient privacy protection rules and medical community compliance timelines were stipulated. In January 2001, there was a question as to whether the Bush Administration might relax certain elements of the recently announced rules. In April 2001, the Bush administration announced that these and other sweeping privacy regulations were going to take effect on schedule, stating "the regulation will go into effect precisely as published in the Federal Register on December 28th, 2000," despite significant lobbying efforts to the contrary.

The healthcare industry accounts for approximately 16% of the U.S. GDP, amounting to trillions of dollars in annual expenditures. A key institution within the U.S. healthcare system is the Department of Health and Human Services (HHS), and within it, HCFA is the agency within the overall U.S. healthcare system that administers and pays for Medicare and Medicaid, among other programs. HCFA, as the trustee for Medicare and Medicaid, administers and disburses nearly $400 billion in annual insurance and benefit entitlements, has approximately one billion medical evidentiary records in its computer databases, receives approximately one billion filings from healthcare providers annually from around the U.S., has approximately 100,000 healthcare vendor partners, and interfaces with the U.S. Social Security Administration who holds electronic records related to all U.S. citizens.

Over the past 18 months TecSec's executive and senior program, operations, and security management has worked extensively with HCFA (and HHS) management to secure a strong relationship on multiple fronts. First, HCFA has announced that it intends to use CKM in

connection with the United States Postal Service NetPost.Certified™ product. NetPost.Certified will be used by HCFA for the electronic transmission and receipting of healthcare claims and other information. HCFA and USPS selected TecSec's CKM encryption technology for this challenge because of its unique fine-grained data protection and Cryptographically Enforced Access Management (CEAM™) capabilities.

HHS and HCFA have also announced that they intend to use CKM for internal and external applications outside of the NetPost.Certified program where security and privacy are required or otherwise deemed important. There are multiple elements of this decision that are currently unfolding. TecSec is in the process of finalizing an initial seat license and 200,000 seat Basic Ordering Agreement (BOA) with HCFA in this regard. HCFA is in the process of finalizing a license for TecSec's Software Development Kit (SDK) to tightly integrate both its commercial off-the-shelf and proprietary applications. HCFA has designated integrators to embed CKM in its electronic forms for healthcare claim purposes. HCFA has assigned another integrator to work with TecSec to develop an extranet platform for the purpose of communicating with its medical care quality assurance partners around the United States.

TecSec has been selected for these programs not only because of the unique capabilities of CKM on a standalone basis, but also its capabilities to broadly support compliance with the HIPAA requirements. TecSec is currently unaware of any companies inside or outside of the HCFA/HHS domain with software features, capabilities, signed contracts, program initiatives or even announcements that involve another technology or product similar to the foregoing discussion.

Summarized below are selected elements of HIPAA and GLBA that CKM technology addresses.

1.1 Electronic Exchange of Private Patient Information

> *"Standards for information transactions and data elements" on page 110 STAT.2024 "Sec. 1173 (a) Standards to enable Electronic Exchange" paragraph (1) states "The secretary shall adopt standards for transactions, and data elements for such transactions, to enable health information to be exchanged electronically that are appropriate for financial and administrative transactions."*

In August 2000 former HHS Secretary Donna Shalala announced standard formats to streamline the processing of health care transactions, reduce the volume of paperwork, save the U.S. health care system "billions" of dollars, and provide better service for providers, insurers and patients.

The Standards for Information Transactions & Data Elements: Sec. 1173 Standards to Enable Electronic Exchange states:

Transactions include:

1. Health claims
2. Health claims attachments
3. Enrollment and disenrollment in a health plan
4. Eligibility for a health plan
5. Health care payment and remittance advice
6. Health plan premium payments

7. First report of injury
8. Health claim status
9. Referral certification and authorization

In late April 2001 the End Stage Renal Disease (ESRD) program networks will begin submitting patient information forms to the quality side of HCFA in electronic format via NetPost.Certified. NetPost.Certified is an end-to-end secure transport service that harnesses the power of CKM's encryption, cryptographic key management technology and utilizes a secure transport built and integrated by TecSec to deliver, time-stamped, dated, return receipt and digitally signed patient information in electronic format. Tampering with private patient information transmitted by NetPost.Certified can be a felony as it is declared to be "mail" that falls under the scope of the USPS' 225 year old legal liability platform. As indicated in the Introduction above, in addition to the USPS NetPost.Certified program, HCFA has tasked one of its integrators with embedding CKM in its electronic forms for healthcare claim purposes. This dovetails with several of the transaction and general standards referred to in this section -- and places TecSec in a strong position to be the leading security infrastructure provider to HCFA, HCFA's vendor partners, and other providers and caregivers who treat 33 million Americans on Medicare and 39 million Americans on Medicaid.

Paragraph D Security standards for Health Information of Sec. 1173 Standards to Enable Electronic Exchange states:

Electronic Signature

1. Adopt standards for electronic transmission and authentication of signatures in regard to transmissions referred to previously.

Digital signatures are a significant component of the NetPost.Certified program. Before a document is encrypted and sent, it is digitally signed by the doctor or caregiver. When the document is received at the receiving server, a hash of the signed and encrypted file is taken and signed by the U.S. Postal Service. The server then sends a signed receipt back to the sending party. The transaction is completed securely, digitally signed, time stamped and dated with a return receipt to both parties. Again, this is particularly importantly as USPS provides a 225 year-old legal liability platform for the enforcement and prevention of unauthorized use of NetPost.Certified or its traffic.

1.2 Information Safeguards

Paragraph 2 of "Standards for information transactions and data elements" on page 110 STAT.2026 states that Each person described in section 1172(a) who maintains or transmits health information shall maintain reasonable and appropriate administrative technical and physical safeguards to (A) ensure the integrity and confidentiality of the information.

Paragraph (2) requires the health care industry to implement safeguards to guard data integrity, confidentiality, privacy and availability. Confidentiality involves the protection of stored information and enforcing privacy. Privacy is the controlled access to view and use information and subsets thereof. With CKM, the confidentiality and privacy of the document is maintained as only the correct credentials allow a user access to view the document. Once the document is opened, CKM requires the user to have the correct credentials to view the specific data within the document. CKM's encryption technology is not restricted by file type or data type. Any

data may be considered an object - a sentence in a paragraph, a word in a sentence or a field in an electronic form.

"How does one protect selective electronic information that has been released without having a chance of knowing who may see it or come into possession of it downstream?"

CKM's ability to protect data at rest as well as in transit results in the security of patient information throughout the life of the document. Certain elements of healthcare records have 7, 25, and 50-year archive requirements. CKM encrypted information is secured when the information is stored on a shared network resource such as a database or in transit across a shared network such as the Internet. In addition, only those individuals with the appropriate CKM credential to see the information may access the confidential information. Firewalls are very effective in protecting networks from external intrusion and provide network separation, however when compromised, unencrypted data inside the firewall is completely exposed. CKM is unique in that it continues to protect the integrity of the information at the object level independent of the firewall. This is particularly important as 60%[1] of corporate security breaches occur not by outsiders penetrating a perimeter defense such as a firewall, but by insiders who have access to systems and information inside the firewall.

1.3 Individual's Access to their Personal Healthcare Information

> *§ 164.524 Access of individuals to protected health information states "The individual has a right to inspect and copy his or her PHI that is used, in whole or in part, to make decisions about the individual, for as long as the covered entity maintains the information. However, individuals do not have an automatic right to access (1) psychotherapy notes, (2) information in a criminal, civil or administrative action or proceeding or (3) PHI that is maintained by a covered entity that is subject to or exempted from the Clinical Laboratory Improvement Amendments (CLIA)."*

CKM uniquely addresses this requirement through its ability to provide cryptographically enforced access management to information. An individual would belong to a domain. The domain may be a provider's practice or a national organization devoted to a clinical condition such as the American Heart Foundation or American Cancer Foundation. The individual's domain administrator would issue credentials allowing the individual access to his or her private health information while restricting access to psychotherapy notes, information in a criminal, civil or administrative action or proceedings and private health information maintained by a covered entity that is subject to or exempted from the Clinical Laboratory Improvement Amendments (CLIA). Another important (and unique) feature of CKM is scalability (see below for further explanation) that allows organizations to build complex relationships within domains and address the scalability issues with current security systems.

1.4 De-Identifying Information

> *Under section 1177. "WRONGFUL DISCLOSURE OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION" (a) Offense. A person who knowingly and in violation of this part "(1) uses or causes to be used a unique health identifier; (2) obtains*

[1] CSI/FBI Computer Issues and Security Trends Survey, Spring 2001.

individually identifiable health information relating to an individual; or….shall be punished as provided in subsection (b).”

HIPAA regulations encourage healthcare entities to use “de-identified”; information that has been stripped of elements that could be used to identify individuals. Once information has been “de-identified” it may be used or disclosed without restriction.

CKM object level encryption allows patient data to be “de-identified”. Integrated object management enables data separation and is the foundation of assuring privacy and confidentiality and de-identification electronically. Protecting information normally entails securing an entire item (e.g., record, file, website), not individual components or objects (field, character, paragraph, chart, image, etc.). Unlike any other encryption technology[2], CKM enables object level encryption. CKM provides this fine-grained ability to divide an item (like a form) into separate objects and embed role-based access attributes to individual objects. Individual objects within an item may be tagged such that they can be hidden, moved, or manipulated. It allows for highly flexible control over any object regardless of size or data type such that the end user of the data will "see" only what the document’s owner wants them to "see." For example, an actuarial at an insurance company may need access to information regarding a patient’s treatments and risk profiles, but does not need access to the patient’s name. CKM’s use of cryptography at the object level permits the actuarial to see what’s allowed, but nothing else – all while accessing a single version of the form.

1.5 Workgroup Administration

There are multiple elements of HIPAA that require the establishment of workgroups or domains or what TecSec refers to as administrative peer groups. The healthcare industry is a dynamic environment. One in which patients flow in and out of various health care plans, do not require further treatment, provider practices merge or split or patients belong to multiple practices requiring specific credentials to each practices domain. The combinations are endless. CKM’s administrative capabilities, architecture, and scalability permit network owners or domains to mirror process and work flow as they grow or change.

CKM-enabled products offer flexible integrated information security and information management. HIPAA provides flexibility to create policies and procedures that are best suited to cover the healthcare entity’s practices. The healthcare entity may assess its own needs in the design and implementation of privacy procedures and policies. CKM scalability and flexibility allows healthcare entities to establish, administer and control their own CKM domains. Administrative control over a CKM domain allows the healthcare entity to control and manage the various roles and policies necessary to protect patient data. This translates into the need for highly configurable architecture and a scalable security system. Without the capability to scale and configure, any security system is rendered inefficient, unusable and inadequate. While CKM is especially suited to large distributed networks, it supports both client and server based models and applications. Servers can also be “clients” in certain CKM distributed deployments and configurations. Traditional key management systems are server-dependent and create the risk of a single point of failure. Moreover, many have a negative effect on overall system speed and performance as the number of user’s increases.

[2] TecSec’s ability to protect information at the object level is covered by four or more US patents, the first of which granted in 1994. Please contact the company for additional information on these patents and techniques.

CKM's client-oriented architecture and deployment moves the bulk of the user credential-checking load to the client, which can eliminate the application software's reliance on a networked certificate authority-based trust infrastructure. It becomes unnecessary for each transaction to obtain authentication from the centralized server for certificate verification. And, because TecSec Smart Tokens have CPUs, they can be configured to provide additional security features such as forced disablement at the end of each user's shift, implementing "sunrise/sunset" access features allowing users access to information back/forward to specific dates or times, or enforcing other security policies such as allowing read only or write only access permissions.

CKM & GLBA

2 Introduction ~ CKM & GLBA

Enacted in 1999, the Gramm-Leach-Bliley Act (GLBA) sets out to "... enhance competition in the financial services industry by providing a prudent framework for the affiliation of banks, securities firms, insurance companies, and other financial service providers …." Specifically, GLBA affects the financial services industry in three distinct ways:

- It outlines the structure of the financial industry for the foreseeable future
- It establishes how this new structure will be regulated and supervised, and
- It establishes new requirements with respect to the rights of customers to protect the privacy of their personal financial information.

Compliance with new laws mandating the protection of "nonpublic personal information" is a key driver to the anticipated rapid implementation of information security software in the financial services industry.

GLBA removes the remaining restrictions governing the separation of banking, securities and insurance activities within a single financial services company. Specifically, it repeals provisions of the 1933 Glass-Steagall Act, which separated commercial and investment banking, and it repeals provisions of the Bank Holding Company Act of 1956 that restricted affiliations of banking and insurance. When the key elements of GLBA take effect in July of this year, banks and other financial companies will be allowed to establish "financial holding companies" that can include commercial banking, securities underwriting, insurance underwriting, and merchant banking. Moreover, the Fed, in consultation with Treasury, may add additional financial activities to this list going forward. Financial holding companies will be certified as such by the Fed once they meet certain threshold requirements with respect to capitalization and Community Reinvestment (CRA) ratings. In addition, banks themselves will be able to operate a full service securities business, including underwriting securities, without creating a financial holding company. Insurance underwriting and merchant banking will be required to be conducted outside the bank in an affiliate. Therefore, to engage in these latter businesses, a company must be certified as a financial holding company.

Regarding privacy, banks and other financial institutions (and traditionally non-financial institutions that handle customer financial information) must make it possible for their customers to prevent them from sharing personal financial information with third parties. This is called the "opt-out" privacy provision of the law.

TecSec's CKM technology has had substantial exposure to the financial services industry in connection with its ANSI review process from 1996 - 1999. In 1996, TecSec (and CKM) was sponsored by the Federal Reserve Bank, Citicorp, Chase, IBM and the Digital Equipment Corp before the American National Standards Institute (ANSI). CKM was sponsored for its core capabilities to support a future generation of electronic banking transactions. After 2 ½ years of peer review, ANSI standard X9.69, A Framework for Key Management Extensions was approved. With X9.69 ratified and another standard well along its way towards final approval (X9.73) TecSec and CKM are already well positioned to serve the financial services industry.

2.1 Key Elements and Requirements of GLBA

It is important to note that privacy, confidentiality, security and other requirements of GLBA and HIPAA are similar. Privacy is the controlled access to view and use information and subsets thereof. Confidentiality involves the protection of stored information and enforcing privacy. Moreover, CKM's core capabilities of object management and data separation, Cryptographically Enforced Access Management, inherent cryptographic key recovery, and scalability apply equally well to GLBA and HIPAA.

The main provisions of the GLBA related to privacy are listed below, under TITLE V Privacy, Subtitle A-Disclosure of Nonpublic Personal Information:

SEC. 501. PROTECTION OF NONPUBLIC PERSONAL INFORMATION

(a) PRIVACY OBLIGATION POLICY - It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.

(b) FINANCIAL INSTITUTIONS SAFEGUARDS - In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards

1. The security and confidentiality of customer records and information.
2. Protect against any anticipated threats or hazards to the security or integrity of such records
3. Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

2.1.1 Customer Confidentiality

The GLBA requires all financial institutions to disclose to customers their policies and practices for protecting the privacy of non-public personal information. The disclosure which customers would receive at the time of establishing the relationship and at least annually thereafter would allow customers to "opt-out" of information sharing arrangements to non-affiliated third-parties. The Act permits financial institutions to share personal customer information with affiliates within the holding company.

Effective immediately, it is a criminal offense for any person (including firm employees) to obtain or attempt to attain customer information relating to another person from any financial institution by making a false or fraudulent statement to an employee of that financial institution.

CKM technology addresses this requirement through fine-grained access control, data separation and access management. CKM technology limits individual access to information, creates proportional access to information, and enables multi-level security through fine-grained access management at the object level – that is, fine grained security and information management. Access management enables control over which organizational resources and services users are permitted to view or access for use. Privileges are defined, managed, reported and enforced based upon business roles and organizational policies.

2.1.2 Safeguards

This regulation requires financial institutions to implement safeguards to ensure data integrity, confidentiality, and availability. The integrity of the document is maintained, as only the correct CKM credentials will allow a user access to view or modify the document. Once the document is opened, CKM requires the user to have the correct credentials to view the specific encrypted data within the document. CKM encryption is not restricted by file type or data type. Any data may be considered an object – a sentence in a paragraph, a word in a sentence or a set of fields in an electronic form.

CKM's ability to protect data at rest as well as in transit ensures that the information is secure when stored on a shared network resource such as a network server or in transit across a shared network such as the Internet or an extranet. In addition, only those individuals with the appropriate CKM credential are permitted access to the confidential information. Firewalls are very effective in protecting networks from external intrusion and provide network separation, however when compromised, unencrypted data inside the firewall is dangerously exposed. CKM protects information independent of the firewall, or its integrity, against external and internal threats.

2.1.3 Protection Against Unauthorized Access to Customer Information

CKM addresses regulation (3) through its inherent role based access control. Traditional key management systems are identity-based. CKM provides a flexible, highly configurable system to manage the flow of and access to information by users with defined roles. Domain Authorities assign access rights to users based on their defined business roles. Today's financial institutions assign both employees and temps to handle customer accounts. Not every individual associated with a client needs access to all of the information. Role based access allows only the people with the correct roles and credentials to see the information they have a right to view or modify. For example, the broker responsible for executing trades for a customer may only need to have access to the client's brokerage account while the customer relations manager would need information about the entire account. Likewise, the insurance agent associated with a client's account should never need access to the client's brokerage information.

Credentials can be stratified and categorized to limit individual access to information, create proportional access to information, and enable multi-level security.

3 Secure Wireless Communications

GLBA does not directly call out or require financial institutions to secure wireless communications that carry financial data, but the implication is clear. In today's highly networked and increasingly mobile financial world, wireless communications are a critical component of many financial institutions' daily operations. Information needs to be available immediately and securely. TecSec is developing methods and the framework for porting CKM to PDAs and other personal wireless devices. Industry observers have commented that too often users and network owners are more concerned with protecting the transmission conduit and not the data on the PDA from being lost, stolen, or otherwise be improperly accessed.

3.1 Scalability

Financial institutions today require a transparent, efficient and agile security system. Without the capability to scale and configure, any security system is rendered inefficient, unusable and inadequate. While CKM is especially suited to large distributed networks, it supports both client and server based models and applications. Again, servers can also be "clients" in certain CKM distributed deployments and configurations. Traditional key management systems are server-dependent and create the risk of a single point of failure. Moreover, many have a negative effect on overall system speed and performance as the number of users increases. A client-oriented architecture and deployment of CKM moves the bulk of the load to the client and can significantly reduce the run-time reliance on a certificate authority-based infrastructure (that is, scalability). It becomes unnecessary for every transaction to obtain authentication from the centralized server for certificate verification. CKM enables integrated information security and information management.

3.2 Conclusion

The manifest impact of GLBA is evolving. Further regulations will be issued by multiple Federal agencies designated under the Act. Compliance will be difficult and noncompliance costly. The Act sets forth requirements that protect personal information. Numerous exceptions must be tracked and enforced by the "owner" of the information. Other key management systems, such as those that identify access by individual identity, will have difficulty scaling to the magnitude required. Realistically, only a role-based access control system will handle the sheer number of records and types of access allowed. CKM not only provides role-based access based on "owner" rules about content, it also enforces such access by encryption. CKM has built in flexibility to modify access as requirements evolve. It is clear that the financial services industry faces a challenge in the coming months in order to ensure compliance with the Act. CKM's unique ability to provide a scalable, secure and elegant solution to meet key elements of GLBA and HIPAA will position TecSec as a leading enabler in the race to compliance.