

Wireless Text Messaging

by Brian Gilmore

We take wireless text messaging for granted

Wireless text messaging is a natural outgrowth of paging technologies dating back to the 1950s, the 1980s, and 1990s. After years of hard work, the telemessaging industry has achieved what was once only a dream – wireless text messaging. A telephone message neatly typed into a computer in the call center appears almost instantly on the screen of any wireless device carried by the client, combining automated message delivery and notification. With the exception of message delivery confirmation, no further labor is required after the caller disconnects from the call center agent.

Over the course of the last seventy years, little has impacted the telemessaging industry more significantly than wireless text messaging. In many cases, the ability to deliver the entire text of a telephone message through automation reduces the call center labor cost per message by as much as fifty percent.

The process, procedures, and technology have all become so familiar to the industry that we essentially take them for granted. Yet there are challenges to be faced as changing technologies, competing business interests, and new governmental requirements threaten to disrupt the technology we depend upon so heavily.

Massive upheaval among wireless carriers

Most recently we have seen a tremendous proliferation of new options as wireless telephone service carriers bundled wireless text messaging into digital telephone handsets and rate plans. The six major wireless telephone carriers and a handful of regional carriers decimated the enormous subscriber growth of the traditional paging industry in the 1990s.

While the number of business users of paging services has increased steadily in recent decades, a handful of paging carriers sought to create nationwide paging networks. As a result, their market share grew at an astounding pace with increased consumer sales. When wireless telephone carriers rolled out their inexpensive digital services with bundled text messaging, millions of consumers canceled their paging service and signed up for a wireless telephone. Only MCI's SkyTel Paging remained focused mainly on business sales.

The effect on the national paging carriers was profound. These carriers faced enormous customer losses and many went through bankruptcy reorganization. As of this writing, only four national paging companies survive in the US and their customer base is once again comprised mostly of business users. There are also well over one hundred regional and local paging carriers in the US, many of whom never had the resources or inclination to pursue the consumer market and many of which are today thriving by providing paging service to business subscribers.

Among wireless telephone carriers, the focus is largely on consumer sales, though each of the big six national carriers devotes substantial personnel and resources to business sales. One carrier, Nextel, focuses most of its sales efforts on the business subscriber. It is not by accident that the wireless carriers with the highest revenues per subscriber are SkyTel Paging and Nextel - both companies focus on business subscribers.

The reasons for the success of these two organizations is clear. While mass marketing techniques let carriers grow their consumer subscriber base at incredible speeds, business subscribers are more stable, do not change carriers as often as consumers, pay larger amounts each month, and pay more reliably than consumers. Business accounts are also less expensive to maintain and are thus more profitable according to wireless financial analysts.

Businesses choose various wireless text messaging solutions

The reasons that businesses choose paging or wireless telephones for employee communications vary widely. There are many reasons why certain businesses choose one technology over another including price,

features, reliability, cost control, wireless coverage and penetration, safety ratings of devices, perceptions of service quality, and even the “coolness factor.”

Paging subscription is now heavily concentrated in specific vertical industries including law enforcement, heavy industry, various trades and crafts, and other service organizations. The paging industry has focused heavily on these niches and worked hard to cater to their special needs. These industries provide intrinsically safe subscriber equipment and paging networks optimized to prioritize “code blue” messages for medical workers.

Without reliable ways to send wireless text messages, the telemessaging industry loses key advantages

Just as the telemessaging industry benefited in the 1990s from the widespread availability of alphanumeric paging technology, it has more recently benefited from the shift to wireless telephones with bundled text messaging features. In many cases, more clients’ employees are equipped with devices that can be used to deliver text messages than ever before. Frequently the devices are purchased and services are paid by the employee instead of their employer, our client. Employees are happy to receive text messages at no additional cost on their wireless telephone handset and our industry is the beneficiary.

But the wireless telephone industry will not continue to provide free text messaging. In Europe, Asia, and elsewhere the price of text messaging is increasing dramatically as paging businesses have faded. Consumers and businesses alike have come to rely on wireless telephone networks as their only reliable source for short text messaging. With voice prices fading fast under withering competition, wireless carriers are looking to increase their revenues from messaging services.

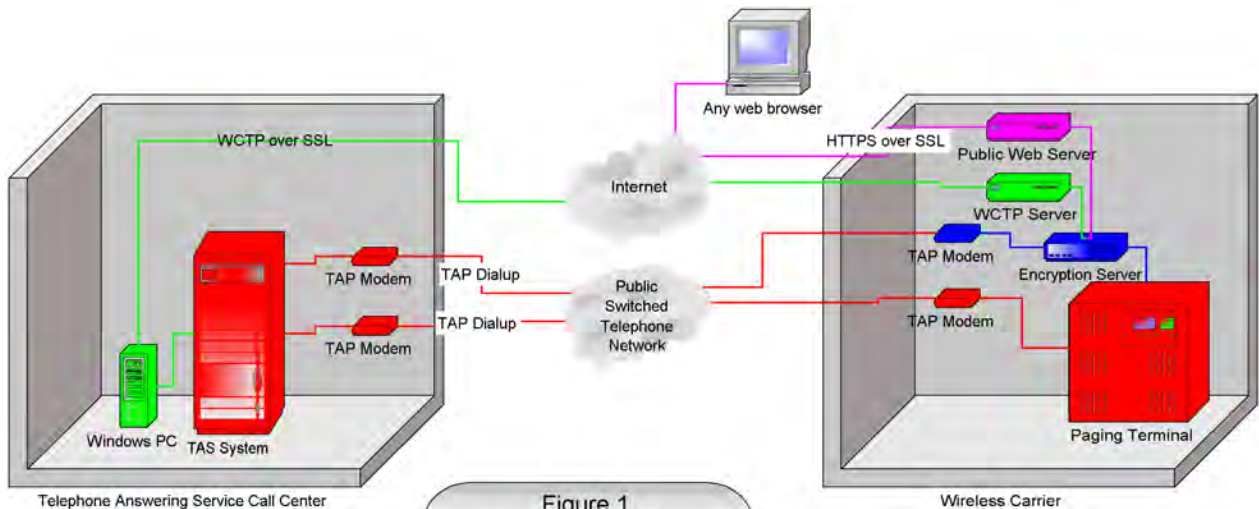
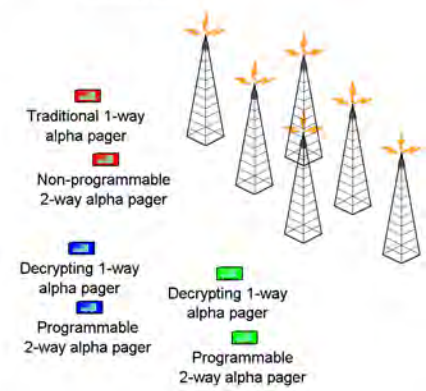


Figure 1

Text messages are currently sent via TAP dialup protocol.
 Using single key encryption scheme, no change is required at the TAS to send encrypted wireless text messages.

Single key encryption scheme also makes secure messaging from any web browser over SSL simple for the general public including TAS clients.

WCTP over SSL protects the messages as they travel at the lowest possible cost over the Internet and makes advanced 2-way text message applications possible.



Already two of the big six wireless carriers have dropped Telocator Alpha Paging (TAP) dialup modem access. TAP was first adopted by paging carriers in the 1980s and was consistently used by every wireless

text messaging provider in the US. TAP dialup modem service is so important to the telemessaging/dispatch industry that every telemessaging system manufactured since the 1980s supports TAP dialup for text messaging.

The alternative is sending an e-mail message to a wireless telephone. However, many telemessaging call centers continue to have mixed results with mitigated success delivering short text messages to digital handsets via e-mail. But even e-mail access is threatened by the increasing scourge of Unsolicited Commercial E-mail (UCE or spam). Indeed, Nextel recently instituted “white list” restrictions on many subscribers, requiring the subscriber to pre-authorize the addresses from which they will receive e-mail on their handset.

E-mail also suffers from other drawbacks as it is a “connectionless protocol” meaning that the e-mail message is sent but no confirmation of its receipt is received until later, if at all. Earlier standards like TAP provided instant acknowledgment of message receipt by the wireless network. The problem is compounded by the tendency of Internet Service Providers to constrain bandwidth on the transfer of e-mail as well as a widespread perception that timely e-mail delivery is not critical to customer satisfaction. Finally, e-mail suffers from another malady that makes its use inappropriate for many medical service messaging applications: clear text e-mail is an inherently insecure messaging medium.

HIPAA raises security issues

The 1996 Health Insurance Portability and Accountability Act (HIPAA) was finally implemented in Spring of 2003 by the US Department of Health and Human Services (HHS). Telemessaging companies and call centers serving medical service providers embraced their responsibility under the Privacy Rule of HIPAA and many entered into Business Associate Agreements (BAAs) contractually obligating themselves to protect certain information known as PHI (Protected Health Information).

Because the task of protecting PHI is so enormous, there are few clear guidelines under the Privacy Rule to guide the Telephone Answering Service (TAS) acting as a contractual Business Associate (BA). One thing is clear; PHI must be transmitted by “secure means” under the law.

Since the earliest reviews of HIPAA issues there has been concern and consternation about how to securely deliver PHI from a call center to a healthcare worker in the field over a wireless text messaging network. None of these networks were built with high security of text message data in mind.

Consequences and motivation

A demonstrated failure to keep PHI secure means HHS sanctions for clients. Both criminal and civil liabilities can apply depending upon the circumstances. Clients are also at risk of unwelcome negative publicity and patient litigation. For telemessaging call centers, a failure to keep PHI secure may result in civil liability to their client under the BAA and the certain possibility that the relationship with the client will be at least damaged or possibly destroyed. For wireless carriers there are also no provisions for HHS sanctions under HIPAA, but natural market forces are widely expected to drive medical services customers who are concerned about demonstrating their own compliance with HIPAA toward carriers who offer security for PHI that must be transmitted to wireless devices.

Telemessaging compliance with the HIPAA Security Rule

It has become clear that telemessaging companies acting as BAs must find secure means to deliver PHI to their medical clients wirelessly or they risk losing the convenience. More importantly, these companies may also lose the tremendous labor cost savings afforded by the use of wireless text messaging networks.

Some companies have adopted makeshift means to comply with their obligations under HIPAA. These include solutions as simple as using pre-agreed codes instead of symptoms, prescriptions, or other medical data when transmitting to wireless devices. In other cases they are not transmitting PHI in any form, opting instead to have the physician or other health care worker call an agent by telephone to receive the PHI. However, these stopgap measures eliminate much of the fundamental value delivered by text paging and drive up labor costs for a telemessaging call center. Better, more comprehensive solutions are needed.

New Technologies for Wireless Text Messaging

When messages are sent via e-mail as clear text from a telemessaging call center, they are extremely vulnerable as they traverse the Internet. As the text messages are transmitted over the air in clear text, they can also be easily intercepted and logged. This vulnerability is all the more important given the privacy issues raised by the Health Insurance Portability and Accountability Act (HIPAA) was discussed in more detail in part one of this article. After close consultation with the wireless text messaging industry, some preliminary solutions are emerging.

First, Telocator Alpha Paging (TAP) modem dialup should serve as a reasonably secure means of delivering unencrypted messages to the carrier's network. This means of transmission is already used for the vast majority of wireless text messaging. All legacy telemessaging systems support it except a couple of wireless telephone carriers. TAP should be preserved until better standards for transferring wireless text messages from telemessaging call centers are implemented.

Second, the most practical solutions perform all encryption functions within the carrier's network. These solutions require no change at the call center. Variations of such technology have been presented at two meetings of the Paging Technical Committee (PTC), the standards body of the paging industry. The proposed solution consists of installing an encryption server at the carrier's location between the paging or Short Message Service (SMS) terminal and TAP dialup modems. Thus, incoming TAP pages are encrypted immediately upon being received by the carrier, before the messages reach the paging or SMS terminal. The message text remains in encrypted form throughout the radio transmission and as the message is received and stored on the wireless device.

This highlights the second part of the solution. Many wireless devices will need to be replaced in order to permit the reception and storage of encrypted data as well as the decryption of messages as they are displayed by the user.

Traditional one-way alpha pagers and non-programmable two-way alpha pagers will not be compatible with encrypted text messaging. Some existing programmable two-way devices are expected to be compatible with the addition of software upgrades. Several low cost and new, compatible programmable two-way devices are presently coming to market. There is at least one known one-way pager currently on the market that is capable of handling encrypted messages. Similar issues will apply to wireless telephone handsets. Some models are already suitable to run the software applications necessary to manage encrypted text messages.

Third, ensuring that all encryption and decryption takes place within the wireless network and the subscriber's device resolves one of the most vexing issues of data security – key management. Encryption schemes require keys to scramble and unscramble message contents. There are several complex technical models describing how the keys are distributed to message senders and receivers.

This type of solution uses a single “secret key” or “symmetric key cryptography” eliminating the need for the call center, the client's office staff, or the personnel carrying the wireless devices to know or manage encryption keys or passphrases. Before the device is delivered to the end user, the carrier will physically connect the subscriber device to its network for a few seconds coordinating the “secret key” between the device and the encryption server. From that point on, all communications between the encryption server and the wireless device are encrypted and no third party is aware of the encryption key shared.

The value of the carrier providing seamless and transparent encryption of message data cannot be overstated. From the perspective of the telemessaging call center, there is no change in procedure required, other than changing the TAP dialup modem number for pager units that will be exchanged for encrypted pagers.

The client can continue to use TAP dialup paging software or they can use a secure web page to send text messages using the same Internet security technology used to place online orders. The sender using a secure web page will probably not notice any difference from using an unsecured web page. This technology is known as Secure Sockets Layer (SSL). SSL is active when you see a small padlock symbol in the lower right hand corner of your web browser and the web address is preceded by “https://” standing for Secure HyperText Transfer Protocol. SSL protects the web page data as it crosses the Internet.

Alternative means of delivering text messages to the wireless carrier

Although it is highly desirable to continue to be able to deliver wireless text messages to carriers via TAP dialup modems for the time being, there are better solutions. One proposal being considered in the PTC, the technical standards body of the paging industry, also relies on SSL over the Internet. It is widely understood that a technically superior means of delivering wireless text messages to carriers is accomplished over the Internet using a standard called Wireless Communication Transfer Protocol (WCTP). This standard defines a sophisticated means of exchanging wireless text messages including two-way text messages and detailed message content such as order information or medical data, via the XML Internet standard. XML stands for eXtensible Markup Language, a data interchange standard.

WCTP can be carried via SSL, which protects the XML data as it crosses the Internet from a call center system to a wireless carrier. Wireless carriers and their vendors are studying WCTP over SSL as a next generation alternative to TAP dialup modems.

No wireless carrier supports WCTP over SSL today, although implementation could be relatively swift and reasonably inexpensive according to some in the wireless text messaging industry. Similarly, no telemessaging system vendor supports WCTP over SSL today either.

A Windows PC as a WCTP Gateway

Supporting WCTP over SSL at a telemessaging call center could be relatively painless through the use of an inexpensive Windows PC with an Internet connection and a serial port connection to a TAP port on the telemessaging system. A Windows software program on the PC, called a WCTP Gateway, would receive TAP pages from the telemessaging system and send them to the paging carrier through the Internet using WCTP over SSL. The WCTP gateway would accept an acknowledgment from the wireless carrier and return a TAP acknowledgment to the TAS system.

From the perspective of the call center, the wireless text messages are being sent via TAP dialup modem, only much faster. All telemessaging system alpha paging features such as message character limits, automatic insertion of a system time, date or serial number, and marking the message as having been delivered to the wireless carrier are maintained without modification to the telemessaging system. On many systems, these are significant benefits over using e-mail to attempt message delivery to a wireless carrier.

Gateway approach delivers more benefits

There are other advantages to using WCTP over SSL instead of TAP dialup modems. The associated telephone lines and telephone usage charges would be reduced or eliminated. There would be no need to track and change TAP dialup modem numbers periodically and experimenting with modem configurations and setup strings would be a thing of the past.

But most importantly, because WCTP over SSL is a two-way connection-based standard, more of the unrealized promises of two-way text messaging can be recognized in the call center. For example, some wireless networks can detect when a text message has been read on the device or when the user confirms receipt of the message on the device. This information can be used to mark a message delivered or continue with automated escalating relay steps (to other wireless devices) until message delivery has been confirmed, much as voice messaging systems handle "cascade paging" today. The data can be logged and extensive automated message delivery reporting can be generated, including the actions of the client employee carrying the text messaging device. These detailed and enhanced functions are not supported effectively today by any standards for connecting a telemessaging system to a wireless carrier's network.

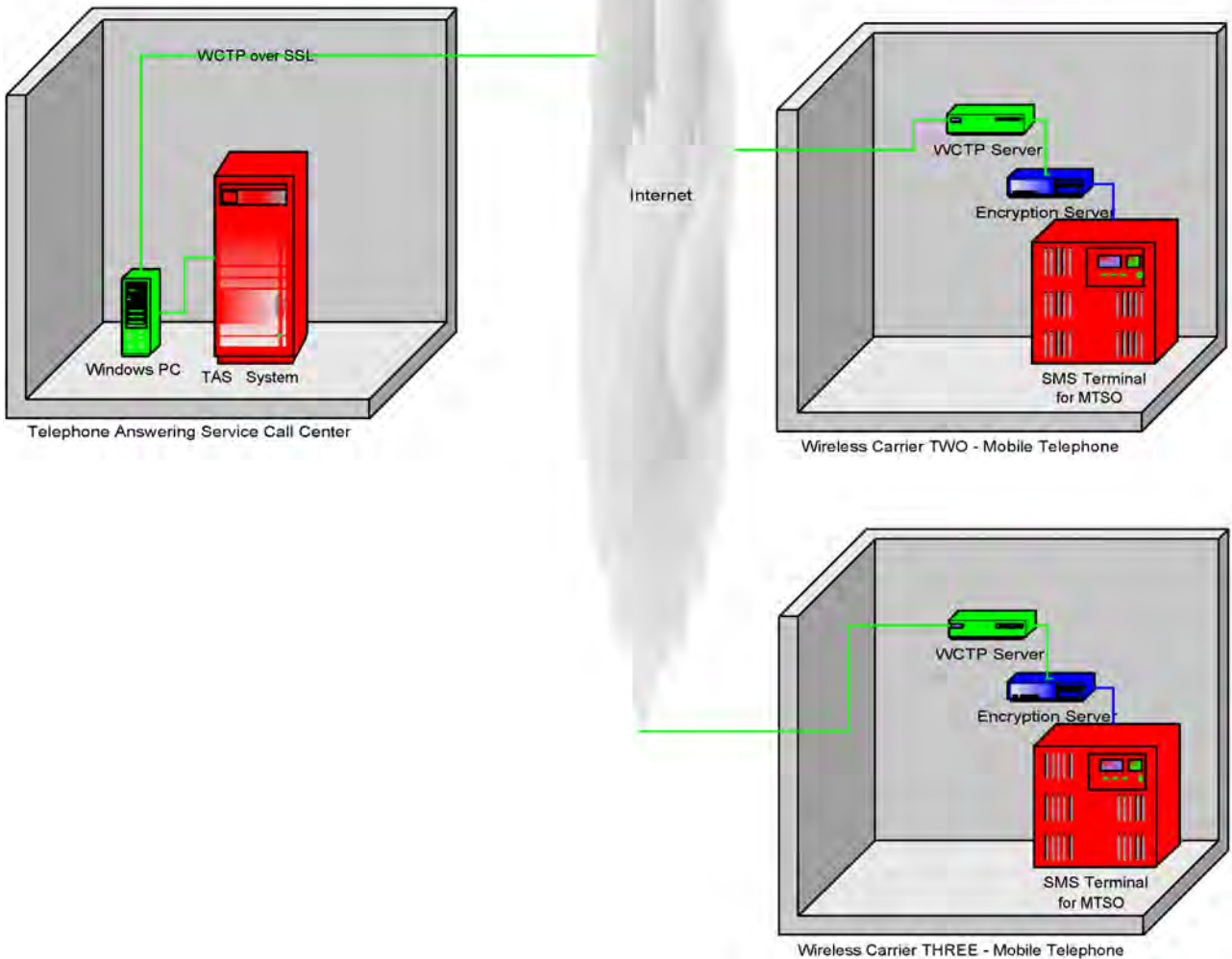
Some telemessaging system vendors may want to incorporate such features directly into their software. Other vendors and users of legacy systems may want to keep such specialized functions separate, handling them through a third party WCTP gateway. A WCTP gateway can communicate with a telemessaging system through other means than a serial TAP connection. For example, an Ethernet network connection between a WCTP gateway and a telemessaging system can be used. Alternatively, another text messaging standard already supported by some vendors, called Simple Network Paging Protocol (SNPP), could be employed.

Figure 2

Two way text message applications between each TAS call center and all compliant wireless carriers could be supported with the widespread adoption of a WCTP over SSL standard and the installation of a WCTP gateway at each TAS location.

TAP dialup numbers, modem settings, phone lines and local telco usage charges would be eliminated.

TAS system vendors can also incorporate WCTP gateway functions into existing and future TAS/Call Center systems.



Other uses for a WCTP Gateway PC

As more carriers begin to use WCTP, a single WCTP Gateway PC could handle multiple, simultaneous WCTP connections to various carriers. More serial TAP connections, or more Ethernet bandwidth or SNPP connections, with a TAS system can accommodate increased traffic.

Other wireless carriers may never support WCTP. As an example, AT&T Wireless has embraced a standard called Short Message Peer to Peer (SMPP) which also provides for secure wireless text message delivery from a call center to their network over a Virtual Private Network (VPN) through the Internet. The same WCTP Gateway PC used for TAP to WCTP software could also route text messages to AT&T Wireless via SMPP.

Even more standards for wireless text messaging may evolve. Wireless text messaging providers may begin to charge more for access to their networks or they may adopt pricing plans that make it difficult for smaller call centers to afford access to those networks. A WCTP Gateway PC may also serve to securely send messages to a service provider who aggregates text messages from many telemessaging call centers to send them to various carriers at better high volume rates.

No consensus exists yet

It is important to note that no consensus on the technical standards for these solutions exists yet. There are currently six national wireless telephone carriers, four national paging carriers, and over 100 regional and local paging carriers. There are several wireless phone and pager manufacturers, many wireless network infrastructure vendors, over 4000 telemessaging call centers, and over a half dozen major telemessaging vendors and user groups as well as many other consultants, independent software publishers, and engineers all working on these issues. Most of them are not aware of or concerned with the needs of the telemessaging industry.

ATSI (Association of Teleservices International) is creating the Telemessaging Wireless Forum (TWF) to bring these parties together in order to make sure the telemessaging industry and vendors are in close contact with the carriers and their vendors. They hope to influence the standards chosen as the technology, regulatory, and competitive business conditions continue to evolve (see sidebar).

The kinds of solutions ultimately used to address the telemessaging industry's wireless text messaging issues may be markedly different than the concepts described above. You can have a seat at the table and an opportunity to influence the outcome by joining the discussion at www.telemessagingwirelessforum.org.

Brian Gilmore of Fallon Communications is a member of the ATSI Legislative Affairs Committee. You can reach him by e-mail at atsiconmag104@falloncommunications.net.

Telemessaging Wireless Forum

ATSI, the Association for TeleServices International, is creating a new online meeting place for professionals in the telemessaging, call center, and wireless industries including paging and wireless telephony. One of the initial focuses in the new Telemessaging Wireless Forum (TWF) will be wireless text messaging as it relates to the telemessaging industry and its clients.

There will be web forums where telemessaging employees can find valuable information from all major wireless carriers regarding the accessibility of their text messaging networks – dial-up numbers, modem and other configuration settings, standards for e-mail addressing, and other protocols supported. ATSI is asking all major wireless carriers to provide special technical support through the TWF to assist telemessaging employees working to get text messaging implemented on client pagers and handsets. Other call center owners, managers, and employees will be on hand as forum participants and moderators to assist as well.

Other TWF forums will focus on other topics including alternative solutions for text messaging, interaction with various telephone handsets, pagers and devices like wireless Palm, Pocket PC, and RIM Blackberry units and the impact of HIPAA on wireless text messaging.

ATSI's initiative to address these issues

ATSI's (Association of Teleservices International) Legislative Affairs Committee is working diligently to forge a consensus between wireless carriers, telemessaging call centers, and their respective vendors on HIPAA issues. The committee is pursuing a three-part initiative:

1. ATSI believes that in many cases the amount and substance of Protected Health Information (PHI) actually transmitted over paging networks is insignificant. To that end, ATSI is actively seeking the cooperation of the paging industry to work directly with the US Department of Health and Human Services (HHS) to educate the agency on this particular issue and solicit specific published guidance from HHS in order to clarify the matter. In a position first articulated by the immediate past chairman of the committee, Gary Pudles of Answernet Network, the committee maintains that HHS should exempt from HIPAA security requirements, wireless text message transmissions by covered entities (CEs) and their business associates (BAs) that contain no substantial PHI. Known in legal terms as a "de minimis exception," there is already some indication that HHS is thinking along these lines in other matters covered by the HIPAA Security Rule.

2. In other cases where substantial PHI must be transmitted wirelessly, there is little doubt expressed by HIPAA experts that PHI should be transmitted securely. The committee accepts this advice and is urging a consensus on methods, procedures, and protocols among interested parties through the Telemessaging Wireless Forum (TWF). The committee is dedicated to finding solutions that require little or no short-term changes in telemessaging software or equipment. Ideally, the committee believes that telemessaging call centers should continue to be able to use their existing TAP dialup modems for the foreseeable future to securely deliver wireless text messages to carrier networks.

3. The committee recognizes that no telemessaging system installed or in production today supports the forthcoming security standards consensus. The committee further recognizes that an extraordinary combination of people from multiple industries, in many cases competing industries or at best competitors within specific industries, must work together to achieve even basic security standards for wireless text messages. To this end, the committee suggests the development of an inter-industry RFC (Request For Comments – later to be adopted as a standard) for inexpensive and modular Windows PC Internet gateway software to securely interface TAS systems to wireless text messaging networks.

ATSI has already sought the advice and assistance of the Paging Technical Committee (PTC) and the board of directors of the American Association of Paging Carriers (AAPC) on this issue. They are inviting the close cooperation of all interested parties in the new Telemessaging Wireless Forum.

FAQs

Q: The three points of the initiative seem almost contradictory, why work on ways to secure PHI at the same time you are working to get approval for an exception from HHS?

A: The approval for an exception is uncertain. While we believe an exemption is a very valuable concession to seek from HHS, we know that we may not succeed. We also need to be able to comply with the Security Rule requirements regardless of the outcome of the HHS initiative since some telemessaging call centers use significant amounts of substantial PHI and need to be able to transmit it securely. Finally, we know that developing standards and software solutions will take time, while BAs are already contractually required to secure PHI for their clients. If we succeed in getting an HHS exception for insignificant PHI in the interim, then a substantial percentage of the industry will already be in compliance with their Business Associate Agreement (BAAs) while the standards and software solutions are being made ready.

Q: Is dialup TAP really secure?

A: The answer depends on how securely PHI must be protected. HHS recognizes that there are practical limits. While it may be technically possible to intercept unencrypted TAP modem dialup calls from a call center, we believe it is unlikely. HHS guidance suggests they already think the same way, permitting unencrypted dialup facsimile transmissions for example.

Q: So why the call for a RFC and a standard for certain software?

A: To make standardized development possible between all the carriers and their vendors, as well as all call centers and their vendors. There are so many stakeholders involved with so many competing interests that mayhem and mischief is inevitable. The last thing anyone wants to see is proprietary standards, closed networks, and expensive access to text messaging for all but a handful of select telemessaging firms. It is believed that costs will be lowest for all involved if certain open standards can be agreed upon and implemented by the stakeholders. Because some wireless carriers are not expected to adopt open standards, it will be necessary to create PC software to act as a wireless text messaging gateway between telemessaging systems and all the various carriers and their interfaces, proprietary or standardized.

This gateway system should be available as soon as possible for all legacy telemessaging systems. Telemessaging system vendors could build these capabilities into their systems or they could integrate an external system from another vendor. It is expected that telemessaging system vendors will eventually build compelling enhanced software applications that take advantage of the gateway concepts and eventually all telemessaging call centers will be incentivized to upgrade to newer systems to get those features.

Q: How can I get more involved in ATSI and learn more about these issues?

A: Visit www.atsi.org.

Acronyms Used in This Article

AAPC: American Association of Paging Carriers
ATSI: Association of Teleservices International
BA: Business Associate
BAA: Business Associate Agreement
CE: Covered Entity
HHS: Health and Human Services
HIPAA: Health Insurance Portability and Accountability Act
PHI: Protected Health Information
PTC: Paging Technical Committee
RFC: Request For Comments
SSL: Secure Sockets Layer
SMPP: Short Message Peer to Peer
SMS: Short Message Service
SNPP: Simple Network Paging Protocol
TAP: Telocator Alpha Paging
TWF: Telemessaging Wireless Forum
VPN: Virtual Private Network
WCTP: Wireless Communication Transfer Protocol
XML: eXtensible Markup Language