About this article: *Agents are being increasingly asked by their E&O underwriters whether they encrypt their clients' personal data when it is being transmitted. This article provides recommendations with regard to two major areas agencies need to address – secure email and securing their websites when personal data is requested. The article also discusses "encryption" and major types of "personal data" that are the subject of the various laws. Finally, the article outlines the type of resources that are available on the ACT website to help agencies address the email and website issues, as well as to develop and implement a comprehensive agency information security policy and program for their agency.*

Agency Strategies to Send & Receive Personal Data Securely

by Jeff Yates

The Internet and mobility revolutions have enabled agents and their clients to live in an electronic world where the parties can work and communicate with each other from anywhere, opening up wonderful new opportunities for agencies to reach out to new consumers and provide their clients with enhanced services and responsiveness. These developments, however, have multiplied the security risks that agencies must manage in order to protect their clients' personal data.

It is no wonder then that E&O underwriters extending coverage for data breach to agencies increasingly are asking their applicants whether they encrypt or use other protective measures to safeguard this client personal data when it is being transmitted. This article explores approaches agencies can take to protect personal data in transit and then references a number of resources to assist agencies.

Encryption

A common question agents ask is: "what is encryption?" When you think of encryption consider those codes the military employs to keep conversations unintelligible to the enemy. You can find many definitions of encryption on the Internet, but I like this simple one from Microsoft:

> Encryption is a way to enhance the security of a message or file by scrambling the contents so that it can be read only by someone who has the right encryption key to unscramble it. For example, if you purchase something from a website, the information for the transaction (such as your address, phone number, and credit card number) is usually encrypted to help keep it safe. Use encryption when you want a strong level of protection for your information.

Requiring a strong password to gain access to your system is an important security procedure, but it is not the same as encrypting the data within the system.

Personal Data

What are the types of "personal data" that are most sensitive and need to be encrypted when transmitted? The definition of "personal data" can vary by state and is contained in the state data breach notification and privacy laws, as well as in various federal laws, such as HIPAA (PHI – Protected Health Information). Insurers, too, might employ various definitions of "personal data" in their policies, so it is incumbent upon the agency to be familiar with not only the specific laws but also the coverage definitions that apply to the agency. Note also that the applicable state law is based upon the residency of the individual whose personal data is being protected, not the location of the agency. This is an important consideration for both agencies writing business in multiple states and agencies writing policies that cover individuals who reside in multiple states.

With all of the above caveats, the most commonly mentioned types of non-public, individually identifiable "personal data" covered in the laws are those such as: social security numbers, driver's license numbers and other government issued ids, debit and credit card numbers and pins, bank and financial account numbers, and protected health information (PHI under HIPAA). While often not mentioned in state laws, other particularly sensitive personal data that should be protected includes information commonly used for security verification (mother's maiden name, date & place of birth, etc.) or sensitive insurance information (such as jewelry schedules).

It is important for agencies to know what types of personal information they collect, where it is retained and who has access to it. They then need to decide whether they really need to keep this sensitive information. For example, many agencies no longer retain copies of bank checks and are careful only to pass along credit card numbers to carriers, but not to retain them, so that they do not become subject to the comprehensive PCI (Payment Card Industry) compliance requirements. These agencies are also extremely careful to shred this personal data as soon as it is no longer needed.

Further, if the agency decides it must keep particular sensitive personal data, it should limit access to it to only those employees who need to see it, to maximum extent possible. This is particularly true for Protected Health Information. Finally, the agency should be careful to make sure that this personal data is kept off of PCs, mobile devices, thumb drives, where there is a significant risk of loss or theft.

PCs & Mobile Devices

Users of PCs and mobile devices should be trained to remove any emails with personal data that may be received on these devices, as soon as they are read. In addition, the agency should audit to make sure any PCs and mobile devices that can access agency applications are password protected. Further, the agency should implement software that can wipe all of the data off of these devices should they be lost or stolen, restoring them to their original manufacturer's state.

Secure Email

Email is the first major area where agencies need to begin to encrypt their communications to carriers and clients when personal data is included. Some prominent examples of emails likely to include personal data include: sending insurance applications to carriers for a quote or to clients to complete or to sign, and sending insurance policies to clients.

With respect to emails between agencies and carriers (and general agents), ACT recommends that TLS secure email be implemented wherever possible. TLS (Transport Layer Security) is an open standard that once implemented between an agency and a carrier (both parties must have TLS implemented), all of the emails between the partners go securely in a manner that is transparent to the end users. In other words, the agent or carrier underwriter does not have to go to a proprietary website to pick up each email (which many underwriters will not do and is inefficient for agency employees to do). TLS is a great solution for business partners where there are frequent email communications going back and forth.

Many agencies can implement TLS if they have email servers or hosted solutions that offer TLS. We recommend that the initial TLS set up be handled by the agency's technology person, who should also verify that the TLS is working properly with each carrier and general agent. You will find a number of resources that explain TLS secure email more thoroughly on the ACT website (see "ACT Resources" below), including a list of carriers which have advised us that they have TLS available.

Unfortunately, most agency clients will not have TLS capability and therefore, TLS is not a solution for communications with them. This will require the agency to implement a proprietary email solution as well for these clients. When the agent sends a secure email to the client using one of these proprietary solutions, the client accesses it on the email vendor's secure website. The secure email tool also enables the client to send a secure email back to the agent, which is very helpful when the client is being asked to complete a D&O application, for example. Fortunately, there are a number of vendors which can help agencies with both TLS hosted emails and proprietary emails, as well as to provide many other useful tools. (Two examples of such vendors are AppRiver and RPost.)

Real Time

Today email is used heavily to convey applications and other information between agencies and carriers and general agents, particularly in commercial lines. It is important to note, however, that Real Time offers a more efficient and secure method to handle these communications, where the communications are automatically encrypted and kept within the agency's and carrier's management systems.

Agencies are heavily using Real Time for personal lines and we need to increase the usage in commercial lines. Many agencies and carriers are already using Real Time to submit commercial

lines applications and make quote requests for small commercial business, and some have started to use their real-time functionality to make mid-commercial submissions.

In addition, there is great potential for the industry to use Activity Notifications to communicate other types of messages directly between the parties' systems (such as the need for more underwriting information), without having to manage a morass of emails in employees' mailboxes.

We urge agencies and carriers to continue to push the use of Real Time within their organizations and with their business partners, particularly for commercial lines transactions and communications. Real Time is the workflow of the future for commercial lines, as well as personal lines. Email is not.

Agency Websites

It is also critical that agencies provide secure website connections for consumers when they ask the consumer to provide personal data on the website – to receive a quote, for example. The website should create a secure "https" tunnel before the consumer can fill out any form that asks for personal data, just as you would experience when purchasing something online or banking online.

In addition, if the agency provides a "non-https" protected free-form text field which the consumer can use to contact the agency and make requests, there is some risk the consumer will enter private, personal data. Therefore, it is a best practice to take one of the following steps with regard to this free-form text field: (1) to secure it, (2) change it to specified fields that ask only for basic contact information, such as name, phone number, email, address, or (3) include a note with the free-form text field that it is not secure and should not be used to provide any private personal data.

If the agency provides clients with the capability to access their insurance information or documents online, the website should create an "https" connection before any information can be accessed. Once again, agents should work with their website provider to help them with the technical aspects of creating this secure website capability.

Some agency E&O providers also require the agency to post a privacy statement on its website(s), if there is an option for the consumer to submit personal data through the website. It is important that the agency customize its privacy statement to track the agency's particular data collection, usage, sharing, and protection practices with regard to data collected through its website(s). Honda's financial services website privacy statement provides a good example of the types of information that are typically included in such statements.

ACT Resources

This article has covered a few of the areas agencies must manage when protecting the security of their clients' and employees' personal data. ACT has developed several resources for agencies to

review as they establish and implement their agency's comprehensive information security program. All of these resources are included on the Security & Privacy page of the ACT website. These resources include a prototype agency information security policy which agencies can use as a template to build their own customized policy or as a checklist of security issues they should address.

For more on TLS secure email, the ACT Security & Privacy page includes articles, FAQs, a recorded webinar and a list of carriers which have implemented TLS. For more on securing your website and managing potential E&O exposures arising from the website, see the article "Don't Get Caught in the Web."

ACT's Security & Privacy page also includes sample website disclaimers, a recorded briefing on HIPAA-HITECH requirements for "Business Associates," and additional articles focusing on: the E&O and security risks arising from the use of social media, precautions to take when using free, public Wi-Fi sites, and how to manage the "Bring Your Own Device" trend where employees are using their personal devices to access business applications.

Jeff Yates is Executive Director of the Agents Council for Technology (ACT) which is part of the Independent Insurance Agents & Brokers of America. Jeff can be reached at jeff.yates@iiaba.net. ACT's website is www.iiaba.net/act. This article reflects the views of the author and should not be construed as an official statement by ACT.