

Laws and Regulations for Everyone to Live By by Carol Woodbury

One might think that if your business is not part of a particular industry such as health care or finance that you don't have to worry about any laws or regulations regarding the security implementation of your OS/400 or the protection of your private data. If that's the assumption you're making, you may be in for a surprise.

By now most of you have probably heard of the Gramm-Leach-Bliley Act (GLBA) which sets forth a set of data security requirements and privacy standards for the financial sector. You've probably also heard of the Health Insurance Portability and Accountability Act (HIPAA) which was written to attempt to ensure the privacy of electronic health care information. But state laws pertaining to the use and disclosure of private data are cropping up that have far-reaching affects beyond these two sectors. Most notably are two California laws. The first law took effect in July 2002. [This law](#) dictates the appropriate use of a social security number, basically limiting its use and disclosure. The next law takes effect in July 2003. [This law](#) requires companies to notify any California resident when their private data has either been breached or believed to have been breached. "Breach" in this case is defined as "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information." The idea is that the California resident will be notified in sufficient time to be able to take measures to protect themselves from identity theft. Before you think you're off the hook because your company isn't based in California you need to understand that both laws are written for any individuals or businesses doing business in California. That means that if you are a retailer and have one store located in California, you are affected. In addition, versions of both of these laws as well as others designed to help reduce identity theft have been introduced into both Houses of Congress. It is anyone's guess as to when or if they will pass and whether they will be as restrictive as the California laws. However, it wouldn't surprise me to see them pass in some form because identity theft is a huge problem and its occurrence is on the rise.

Lest you think that this issue securing private data is confined to the U.S., think again. Europe has regulated the handling of confidential and private data before any U.S. regulation came into effect and Canada, Hong Kong and New Zealand all have published privacy regulations. If you're not familiar with everything that "privacy" entails and the various laws associated with it try <http://profs.lp.findlaw.com/privacy/index.html> for an overview.

Even if you're not currently affected by a state, country or industry-specific regulation, sooner or later I believe all businesses that electronically collect or retain private data are going to come under some regulation or law that governs how this data is protected. Whether you're in a position where compliance is imminent or your company is not affected by current or impending laws, now is the time to address how your security

implementation could be affected by the requirements of these privacy laws and regulations.

Your first step is to determine what private data you have. The definition of private data in most of the regulations is “nonpublic personal information.” Nonpublic personal information is probably best explained by contrasting it to public personal information. Public personal information is information that is available about an individual through readily available information sources. It includes personal information that is mandated by federal, state and municipalities to be publically available. Examples of public personal information include, birth date, date of death, marriages and divorces. Some mandated public information may surprise you. For example, some areas mandate that mortgage information be made publically available! In addition, information that you would commonly share with a casual social contact is also considered public personal data. This includes information such as address, employment and family structure, i.e., how many brothers and sisters you have.

The information that identifies an individual but is not publically available is the information that is regulated and the information that must be protected. Custodians of this information can be held liable under several regulations and laws for unauthorized disclosure of this information. Unauthorized disclosure of private data is defined in the HIPAA regulations as a “security event”. A security event is the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system. Note that the attempt does not have to be successful to be defined as a security event.

Another way to think about private information is that it is information that can be used to identify you. In the regulations, this is called “personally identifiable information.” Not all personally identifiable information is private, however. Personally identifiable information is considered to be private only if the information is not publically available. For example, your home phone number is a personal identifier, but it is not considered to be private data unless it is an unlisted telephone number. However, a telephone number should be considered to be private data unless the business has taken the time to verify that it is publically available (that is, not unlisted.)

Here are examples of data that is considered to be “private”:

- Social security number
- Credit card numbers
- Bank account numbers
- PIN numbers
- Driver’s license numbers
- Health care information including test results, diagnoses, medical history etc.
- Mental health conditions
- Substance abuse
- Any information that endangers an individual’s rights or welfare

Unfortunately, determining what constitutes private data is not always as obvious as the list above. Sometimes it takes an accumulation of data to have that data considered to be private. Data that determines a pattern or habit of an individual is considered to be private. For example, the data that shows the books that an individual purchases from amazon.com or the travel plans made through expedia.com would be considered to be private because it identifies an individual's habits.

Another example of the accumulation of data is when public personal information is taken together with an account number or access number. Take for instance a home security business. The list of home security systems' access numbers is in and of itself not private data. However, that list aggregated with the clients' addresses would constitute private data. Depending on the nature of business, taking business-specific data (such as access numbers) and combining it with publically available personal information can constitute private data.

Finally, using a healthy dose of common sense along with exercising respect for an individual goes a long way to determine what should be classified as private data. When in doubt, here are some questions to ask about the data:

- If the data was disclosed to the public, could it be embarrassing to the individual?
- If the individual had the choice of disclosing the information to the public, would they typically choose to disclose it or choose to keep it out of the public's eye?
- If revealed, could the information somehow be used to harm the individual?

Now that you've determined that you have private data – what do you do?

First, analyze whether you actually need to gather that information and whether each use is appropriate. For example, you may need to gather a social security number for federal reporting purposes, but that number may not need to be displayed on all application screens. Or, some companies gather their client's social security number simply to identify the user. However, they also have an account number that can identify the user. In this case, you might consider dropping the use of the social security number altogether.

Next, get to know your company's legal counsel. Obviously they are the final word on whether particular laws and regulations apply to the business you're in. Work with them to understand the requirements and the ramifications of not being in compliance. Then you can make an informed business decisions as to what (if any) security implementation changes are required.

If you determine that changes are required, the next step is to secure the private data. Many of the regulations – in particular HIPAA and GLBA – stipulate the use of the "least privilege" concept. Basically that means that someone is restricted from running an application or accessing data unless it's in their job description to do so. Even if you aren't covered by GLBA or HIPAA, this is a great scheme to abide by. It means that you



restrict general access to the libraries or directories of the applications that use the private data and only grant access to those users whose job it is to run the application.

Take an HR (Human Resources) application. What users should actually be running the HR application or accessing the HR data? Typically only the users in the HR department. To implement the least privilege concept in this case, you would set *PUBLIC authority to *EXCLUDE on the application library(s) and directory(s) and grant the HR_GROUP *USE or possibly *CHANGE (if objects are created into the library) authority to these objects. You may need to go further and secure specific objects such as files containing very sensitive data, but often, securing the library or directory is sufficient.

I recommend object level security to implement the least privilege concept because it's in effect no matter how the application or its data is being accessed. Whether it's accessed through FTP, ODBC, a mapped drive using a share defined to root ('/') in the IFS, a web application whose protection directives are not defined appropriately or a programmer typing a command from a "green screen" command line, if a user is excluded from a library or directory, they are not able to access the confidential or private data contained therein.

When determining what data needs to be secured, remember that data often resides in several places. Don't forget about securing the media containing system back-ups, the data that has been mirrored to your high availability machine and the data on your development machines that provide programmers' with "real" test data. All instances of the private data need to be secured.

Once secured, can data still be compromised? Yes. That's because humans are involved and sometimes their behavior is inappropriate. Disgruntled employees who have legitimate access to data can mis-use private data. Fortunately the laws regarding use of private data for identity theft are being developed and existing laws are being made tougher. For example, the State of Washington has declared it to be a felony when private data is used for identity theft. Hopefully stricter laws will act as a deterrent.

No company wants to be caught in the position of having to tell its clients or customers that a breach has occurred and their private data has been compromised. Yet that's exactly what several laws are requiring. Though nothing is fool-proof, I believe there are steps you can take to significantly reduce your business risk - take a look at these laws, analyze your data and take corrective actions when necessary.

This information first appeared in the May 2003 iSeries Extra Administrator Newsletter
www.eservercomputing.com/iseries/e-newsletters

SkyView Partners, LLC
25563 SE 41st Court, Issaquah, WA 98029
+1-425-657-0133 +1-425-657-0135 (fax)
www.skyviewpartners.com



SkyView Partners, LLC
25563 SE 41st Court, Issaquah, WA 98029
+1-425-657-0133 +1-425-657-0135 (fax)
www.skyviewpartners.com