Minimizing the Use of **Social Security Numbers** in Government Programs

As government agencies and businesses increasingly rely on electronic communications, benefits and commerce, there is an ever-greater opportunity for data breaches and identity theft. Recently, we have witnessed cyberattacks on well-known retailers and service providers that have resulted in data breaches affecting millions of consumers. It is likely that each of us knows someone affected by these breaches — perhaps it has even happened to you.

As criminals become ever more sophisticated in obtaining personal information, it is incumbent on government and private industry to take all appropriate measures to safeguard the information of the citizens we serve.

Widespread Use of Social Security Numbers

Social Security numbers are one of the most common means of identifying individuals in the United States. The nearly universal ownership of Social Security numbers by legal residents has led to their use by the government and the private sector as a primary method of identifying and collecting information regarding an individual.

There are many purposes that legally require a Social Security number, including collection and use by employers for tax reporting purposes. Many government programs also use Social Security numbers to identify participants, both electronically and on mailed print materials.

Although a Social Security number may be a valuable piece of information to identify and authenticate individuals, some uses may be more for convenience or out of habit.

As a result of greater awareness and concern about protecting personal information, most private health insurance companies have abandoned the use of Social Security numbers to identify individuals. In April 2015, President Obama signed a bill that will end the use of Social Security numbers on Medicare cards and replace them with a randomly generated identifier. We applaud these efforts to protect the identities of consumers and minimize their risk for financial loss.

Social Security Numbers as Program Identifiers

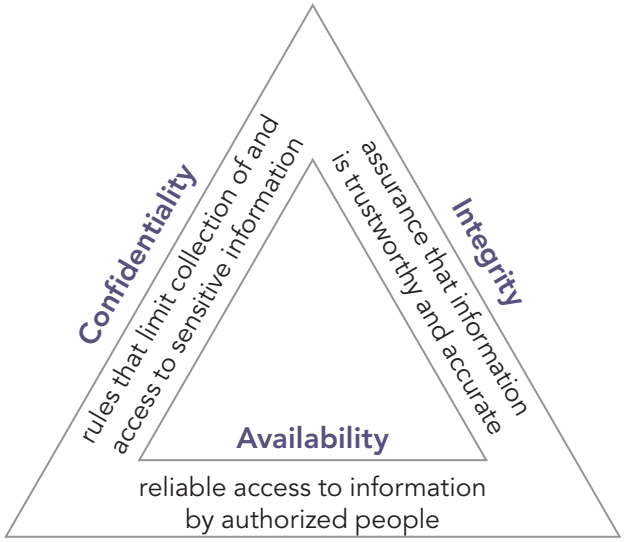
At MAXIMUS, our corporate policies limit the use of Social Security numbers, unless required by law, contract, or explicit client directive. We encourage all of our government clients, vendors and business partners to eliminate the collection of unnecessary personal information, particularly Social Security numbers, and to tightly control and limit their use when absolutely necessary.

Under the theory of "don't collect what you don't need," we recommend our clients, vendors and business partners consider the following:

- Where do Social Security numbers appear in the processes and data flow of the program?
- Are Social Security numbers absolutely necessary for the program or are they being used as a convenient identifier?
- Is the use of a full Social Security number necessary or are truncated versions (e.g., last four digits) sufficient?
- Can case numbers or randomly generated identifiers be used in place of a Social Security number?

Best Practices: Confidentiality, Integrity and Availability

When use of full Social Security numbers is required by law, contract, or explicit client request, MAXIMUS abides by the CIA triad (Confidentiality, Integrity and Availability) to guide decisions for protecting this sensitive information.



Confidentiality

We recommend taking measures that ensure only authorized people can access the correct information and minimize the risk that Social Security numbers get in the hands of unauthorized people.

- **Training** that informs authorized people about correct data-handling rules, as well as risk factors and how to guard against them
- Use of **two-factor authentication** (e.g., security tokens, key fobs or biometric verification) whenever possible and practical
- **Minimize where the information appears** (particularly in printed and mailed outreach materials) and the number of times it is actually transmitted to complete a required transaction

Integrity

We recommend taking measures to maintain the consistency, accuracy and trustworthiness of Social Security numbers. This means making sure that data is not altered in transit or by unauthorized people.

- **File permissions** and **user access controls** to minimize the risk of errors or accidental deletion by authorized users
- Evaluation of the **security of data transmissions**
- **Backups** to restore data to its correct state following any alternations

Availability

We recommend maintaining and upgrading (when practical) hardware and systems to minimize the risk of data loss or interruptions in connections.

- Evaluation of the **security of data storage**
- Backups stored in a geographically **isolated location**
- **Use of firewalls and proxy servers** to minimize the risk of malicious actions (e.g., cyberattacks)

MAXIMUS®
HELPING GOVERNMENT SERVE THE PEOPLE®

1891 Metro Center Drive
Reston, Virginia 20190
1.800.MAXIMUS
maximus.com