

Data Privacy



MS-ISAC
Multi-State Information
Sharing & Analysis Center

**Enterprise
Information
Security Program**



From the Desk of Ron Jimerson, Chief Information Security Officer

Businesses and individuals need to be aware about the importance of protecting data privacy—the protection of the privacy of personal information. With more and more personal information being collected by companies, websites, and social media, data privacy is something everyone should consider.

To understand the importance of Data Privacy day, it is vital to understand Personally Identifiable Information (PII) and exactly what privacy is. PII is any combination of data points that can lead to the identification of a specific individual (you). This can mean things such as your name or email address, but most times PII refers to “sensitive PII” such as Social Security, driver’s license, state identification, or financial account numbers. Sensitive PII can also exist if PII is combined with another piece of information about you such as a birthdate, medical information, or even passwords. The more pieces of data combined about an individual, the more valuable and sensitive the body of information becomes.

Privacy is often considered to be the concept of confidentiality, which is keeping information secret from those that should not see it. While that is an aspect of privacy, often called “need to know,” privacy is much more. Privacy is a larger concept centering on you as the individual to whom the information refers. It is about your rights to access, correct, and control the information that another entity has about you.

Privacy Rights:

Organizations that honor your privacy will not only protect confidentiality, but should follow a set of principles related to how they manage your information, including:

- Not collecting more information than they need to conduct their business with you;
- Informing you of what they will do with the information that they collect and not doing more with it than they have promised;
- Retaining the information for only as long as it is needed and then properly destroying the information;

- Not sharing your information with others without your permission, except as required by law;
- Allowing you to review and correct information if necessary.

To understand your privacy rights it is essential that you read the privacy policies of any organization to whom you provide information, especially PII. This includes websites, health care providers, insurance companies, and financial institutions. If you do not agree with how they intend to protect your privacy, consider not using their service.

Privacy is a Shared Responsibility:

While organizations and websites have a responsibility to protect your privacy, which most will outline in their privacy policy, this is also your responsibility. Social media users are especially susceptible to privacy concerns. Individuals voluntarily place enormous amounts of information about themselves, their friends, and associates, on social media. It is critical that everyone is aware of the information they post on social media services, such as Facebook, LinkedIn, Snapchat, and Twitter. This awareness is not limited to what you post about yourself, but what you post about others as well!

Identity Theft Protection:

Despite many organizations best efforts in handling and using your private information properly, the countless breaches of PII by cyber criminals in the past few years have resulted in the exposure of information about millions of people. One reaction to such breaches can be to provide credit monitoring for one year. This is a very short amount of time to have such a protection. Those that have stolen the information, or those to whom they have passed it on, may hold it for much longer than a year before using it to steal your identity, commit credit card fraud, or worse in your name. If you have been a victim of a breach, check out some of the [FTC's resources](#) on starting a credit freeze to protect yourself.

If you are considering Identity Theft protection services, research the firms that you are considering engaging and ensure you understand the services they will and will not provide. Also, read their privacy policies, because for them to deliver these services you must provide them with varying amounts of PII.

Protecting privacy is both your responsibility and that of those individuals and organizations that have information about you. Do everything in your power to be aware of how you personally can compromise your privacy and hold those organizations that you engage with accountable for their management, or mismanagement, of your personal information.

For More Information:

[US-CERT Data Privacy Day Events](#)

[Online Trust Alliance Data Privacy & Protection website.](#)

[Stay Safe Online website.](#) National Cyber Security Alliance

[Forbes, Data Privacy Day: Easy Tips to Protect Your Privacy](#)



The information provided in the MS-ISAC Monthly Security Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.