1. Review the Software EULA - Before installing any software, take the time to read its EULA. To protect information systems and networks from security and privacy problems related to EULAs, US-CERT recommends that entities:

- also limit their ability to sue for damages.

Software license agreements are legal binding agreements that can have restrictions on how the software can be used; the agreements can require entities to agree to certain conditions when using the software, and can contain language in a software license agreement, as such behavior can expose a computer and its connected networks and systems to security risks.

A software license agreement (also known as end user license agreement (EULA) highlights the risks that can make ePHI vulnerable. Data can be compromised if Covered Entities and Business Associates ignore the restrictions.

Good morning -

Please see the email below issued by the Office for Civil Rights today on third-party application software. If there are actions recommended that your area does not already take, please give consideration to implementing those actions. Also, please take a minute to be sure that the actions you do take with regard to third party application software are documented in your area’s policies or procedures.

Please share this information with anyone else you think may find it useful.

Thank you.

Jill

Jill Bush Raines
Assistant General Counsel, Office of Legal Counsel
and University Privacy Official
The University of Oklahoma
1105 N. Stonewall Avenue, Suite 221
Oklahoma City, OK 73117-1221
(405) 271-2033
(405) 271-1076 (fax)
jill-raines@ouhsc.edu

The majority of software developers disclose their security flaws to public; however, attackers exploit these known vulnerabilities if Covered Entities and Business Associates do not fix the security flaws in a timely manner.

Though applying patches is essential to ensure the security of information systems, patches should be assessed before deployment to determine the risk they pose to the Covered Entity’s information systems.

Reviewing Software License Agreements

A software license agreement (also known as end user license agreement (EULA) highlights the risks that can make ePHI vulnerable. Data can be compromised if Covered Entities and Business Associates ignore the language in a software license agreement, as such behavior can expose a computer and its connected networks and systems to security risks.

Software license agreements are legal binding agreements that can have restrictions on how the software can be used; the agreements can require entities to agree to certain conditions when using the software, and can also limit their ability to sue for damages.

To protect information systems and networks from security and privacy problems related to EULAs, US-CERT recommends that entities:

1. Review the Software EULA - Before installing any software, take the time to read its EULA.

2. Beware of Firewall Prompts When Installing Software - During installation, if your firewall generates a prompt asking whether you want to allow certain inbound or outbound connections, proceed with caution. Verify that the software requires changes to your firewall settings for normal operation and that you are comfortable with this operation.

3. Consider the Software Publisher – If you are not familiar with the company or organization that published the software, review the software EULA with added scrutiny.

Resources: