CTSI
TECHNICAL UPDATE
Volume 29 Number 1 | January 7, 2025

CYBERSECURITY INSIGHTS: PROTECTING INFORMATION

In today's digital age, cybersecurity is a critical concern for counties of all sizes. As cyber threats become increasingly sophisticated, counties must stay vigilant and proactive in protecting their sensitive data. CTSI stays informed of evolving threats and provides quarterly cybersecurity updates on the latest concerns, best practices, and security protocols. This knowledge can significantly reduce the risk of a successful cyber attack and promote a security-first culture.

WHAT IS PERSONALLY IDENTIFIABLE INFORMATION?

Sensitive information is considered privileged when its compromise—through alteration, corruption, loss, misuse, or unauthorized disclosure—could seriously harm an individual or organization. The highest level of protection must be provided to such information to mitigate risks and safeguard trust.

For data protection purposes, Personally Identifiable Information (PII) is any instance of an individual's first name (or first initial), last name, and any of 29 additional confidential items. These items are non-public and can be used to identify a specific individual uniquely.

Examples of Additional Confidential Items

- Social Security numbers
- Credit card or debit card numbers (including expiration dates)
- Date or place of birth
- Wage and salary information
- Vehicle identifiers, including plates and driver's license
- Medical history or health information

The guiding principle is simple: if a combination of data can uniquely identify an individual and includes non-public details, it qualifies as PII. It must be treated with utmost care and security.

Examples of PII in Practice

Consider the following scenario: *John Smith was born on January 1, 1965*. Which of the following examples contains PII?

A. John Smith – DOB 1/1/1965

B. John S. – DOB 1/1/1965

C. John Smith – DOB 1/1/xxxx

The correct answer is A. While "John S." or a partial date of birth may not individually identify someone, the full name and complete birthdate do, making it classified as PII.

THE CONSEQUENCES OF NEGLECTING PII PROTECTION

Failing to safeguard sensitive information can have severe consequences, including:

- **Legal Fines:** Non-compliance with data protection laws can result in hefty penalties.
- **Increased Operating Costs:** Data breaches often lead to expensive mitigation measures, investigations, and system upgrades.
- **Loss of Confidence:** Breaches erode trust and can damage an organization's reputation.
- **Enhanced Regulation:** Frequent data breaches may result in stricter governmental oversight and new compliance requirements.

HOW YOU CAN HELP PROTECT SENSITIVE INFORMATION

Every employee has a role to play in safeguarding PII. Here are some best practices to follow:

- **Store Securely:** Always use encrypted systems or locked storage for physical records.
- **Share Minimally:** Only share PII with authorized personnel, when necessary.
- **Dispose Properly:** Use secure methods, such as shredding or data deletion, to dispose of PII.
- **Stay Vigilant:** Be aware of phishing attempts and other tactics to extract sensitive data.

WHAT THIS MEANS FOR COUNTIES

Regular cybersecurity updates are vital to an effective security strategy. They help keep counties informed, vigilant, and prepared to respond to threats. CTSI recommends counties implement these essential cybersecurity controls to help manage their cyber exposures. This will safeguard and reduce digital vulnerabilities at the county level and assist in obtaining coverage with higher limits and lower premiums for CAPP. For more information, contact CTSI at (303) 861-0507.

County Technical Services, Inc.
Technical Updates are available online at ctsi.org
800 N Grant St, Suite 400, Denver, CO 80203
(303) 861-0507 | Fax: (303) 861-2832