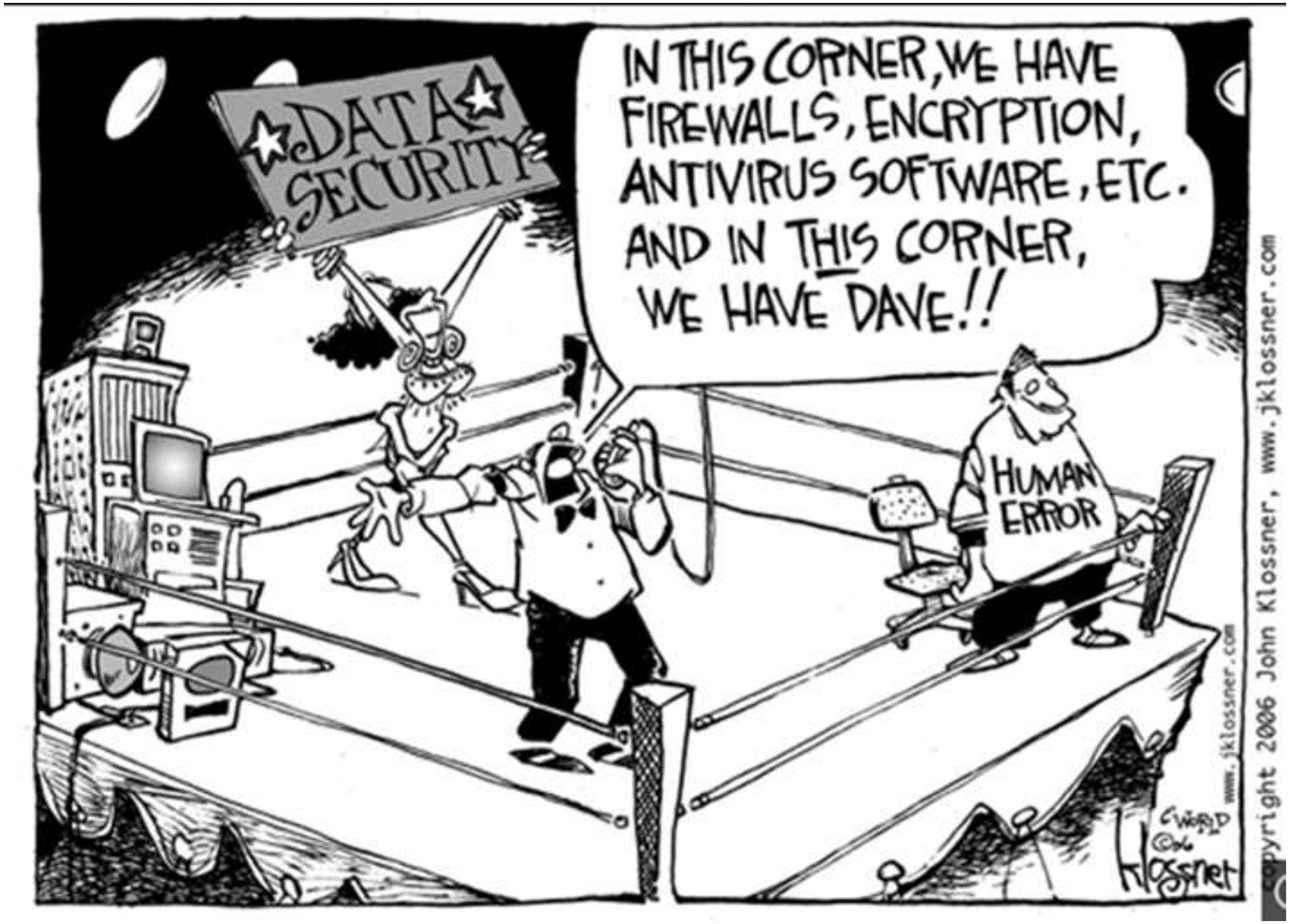
Confidentiality:

Ensuring HR Employees Respect Customer Information

Confidentiality


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
Copyright 2006 John Klossner, www.jklossner.com
www.jklossner.com
CWORLD ©06
Klossner

Confidentiality

Course Overview

This course teaches you about confidential information (CI) in the Human Resources (HR) department. You will learn what CI is and why you must adhere to confidentiality policies issued by Metra and by federal and state governmental agencies. You will also learn what can happen if it falls into the wrong hands.

Confidentiality

Course Overview

You will also learn about best practices for:

- Handling paper documents.
- Handling electronic information.
- Keeping your computer safe.
- Storing CI.
- Conducting telephone conversations.

DRAFT 01/05/15

Confidentiality

Defining Confidential Information (CI)

There is no single "official" definition for CI. Some governmental sources define CI as "information that is not easily-obtainable public knowledge."

Metra defines CI as "any information Metra treats as confidential or private information that has not been issued to the public or to other employees." This includes information about fellow employees in other departments, and fellow employees within the HR department itself.

Confidentiality

Follow Confidentiality Policies

Government agencies and Metra have rules for handling CI. They also have penalties for mishandling CI.

You must handle CI according to Metra's confidentiality policies. These policies include the governmental requirements.

Confidentiality

Examples of CI

Metra’s HR department must protect CI in many categories, such as:

- Names, addresses, phone numbers, email addresses, family members.
- Social Security numbers.
- Health information, including drug test results; and, for law enforcement personnel, psychological exams.
- Background checks.

Confidentiality

Examples of CI

- Financial details, such as bank account numbers, investment/IRA accounts, and tax information.
- Disciplinary information.
- Verification of employment.
- Information about applying for a job within Metra – if you leak information about an employee's interest in a different position within Metra, that information might reach the employee's supervisor.

Confidentiality

Consequences of Leaking CI

If CI is leaked to non-HR employees, it can harm:

- Employees – Identity theft and theft of financial assets are serious crimes.
- Metra – Leaks at Metra could erode public trust and trigger additional federal oversight measures.
- Employees who leak the CI – These employees are subject to disciplinary actions, termination of employment, and civil and criminal penalties.

Confidentiality

Confidentiality Policies and Procedures

You must follow Metra policies pertaining to:

- Identity Protection (Policy and Certification).
- Employee Privacy (Human Resources Department).
- Confidentiality of Information.
- Logon Identification and Password Codes.

Confidentiality

Identity Protection Policy

Under this policy, you must protect Social Security numbers (SSNs) by:

- Limiting access to SSNs to those who must view them.
- Limiting collection, use, and disclosure of SSNs.
- Limiting visibility and distribution of SSNs.
- Properly processing all materials that contain SSNs.

HR employees must take the online Identity Protection Certification course, where they learn the requirements in detail.

Confidentiality

Metra’s Employee Privacy Policy for HR employees:

Under this policy:

- You must not release (in writing or verbally) CI to anyone without the approval of an HR Director or Manager.
- New HR hires (including interns and temps) sign the Employee Privacy agreement at onboarding to demonstrate that they agree to be bound by the policy.

Violators are subject to disciplinary action, up to and including termination of employment.

Confidentiality

Privacy within the HR department:

HR employees must also restrict CI within the walls of the HR department itself. HR employees have access to different levels of CI. Do not share CI with an HR coworker unless they require that CI.

HR employees who handle information about in-house job transfer requests must take special care with sharing this sensitive information.

Violators are subject to disciplinary action, up to and including termination of employment.

Confidentiality

Confidentiality of Information Policy

Under this policy, unless you have permission from a supervisor, you must not:

- Acquire, sell, disclose, or transmit CI about Metra's business or about fellow employees.
- Knowingly convert a Metra business opportunity or information for personal use.
- Use, divulge, or transmit CI during outside employment or succeeding employment.
- Remove Metra documents or copies from the business premises.

Confidentiality

Violations of Metra's Confidentiality Policies

If you violate any of Metra's confidentiality policies, you could suffer disciplinary action, including termination. You can also be subject to civil and criminal penalties.

Confidentiality

Logon Identification and Password Policy

Under this policy, you must:

- Use your logon and password only to conduct Metra business. NEVER let anyone else use your logon information.
- Protect logon IDs and passwords from unauthorized use.
- Change your password often. The system prompts you to change it approximately every 60-90 days.

Warning! You are subject to disciplinary action if you misuse your logon information.

Confidentiality

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA is a federal Act that governs the electronic exchange of Protected Health Information (PHI).

PHI means individually-identifiable information that Metra:

- Transmits by electronic media.
- Maintains in electronic media.
- Transmits or maintains in any other form or medium.

HIPAA governs both privacy and security of health information.

DRAFT 01/05/15

Confidentiality

Handling HIPAA information at Metra

Some CI is subject to HIPAA privacy regulations, but other CI is not. For example:

- HIPAA does not govern first-aid treatment and drug test information.
- HIPAA does govern health insurance claims and Workman's Compensation medical information.

HIPAA information is generally used by the Medical, Risk Management, and Safety departments.

Confidentiality

You must share some types of CI

If you learn of a situation that may cause harm to someone, tell your supervisor right away regardless of whether you learned it as CI. These situations include threats or thoughts of:

- Suicide
- Murder
- Bringing weapons to work

DRAFT 01/05/15

Confidentiality

Handling HIPAA information at Metra

When you work with HIPAA information:

- Do not release HIPAA CI unless the file contains a waiver signed by the employee. Waivers can include time limits on how long they remain in effect.
- Do not share HIPAA-protected information verbally or in writing (emails / documents) with unauthorized recipients.
- Do not disclose HIPAA-protected CI to unauthorized personnel, including employees' supervisors.
- Treat HIPAA CI with the same care as if it concerned a member of your family.

Confidentiality

Handling HIPAA information at Metra

When you access HIPAA information, route HIPAA CI to specific fax machines and printers only. These devices have additional privacy and security safeguards, such as locked offices or segregated areas.

Confidentiality

Handling Confidential Medical Information

When you collect and store CI pertaining to medical conditions or histories of applicants or employees, you must:

- Collect and maintain the CI on separate forms.
- Store the CI in separate files in a secure environment.

Confidentiality

You may disclose confidential medical information to:

- Supervisors and managers to inform them about work restrictions and necessary accommodations.
- First-aid and safety staff to inform them about emergency treatment.
- Government officials who investigate compliance issues.

Never share confidential medical information without the approval of your supervisor.

DRAFT 01/05/15

Confidentiality

Store CI in secure locations. For example:

- Store personnel files containing employees' contact information, hire dates and attendance records, and departmental assignments in one secure location.
- Store employee files containing information about consumer reports, I-9 forms, wage garnishment documents, credit card information, mortgage application inquiries, reference checks, and pre-employment and drug testing results in a separate secure location.
- Store HIPAA-type health information in secure locations that hold only this type of CI.

DRAFT 01/05/15

Confidentiality

Storing and Disposing of CI

- Documents relating to the transaction of Metra business are “public records.” These records can be on paper or digital.
- Metra cannot destroy public records without the permission of the State of Illinois.

DRAFT 01/05/15

Confidentiality

Storing and Disposing of CI

- Metra is currently creating a policy with guidelines for the storage and disposal of CI.
- For now, you must store business documents in a safe place, either at Metra offices or off-site at an approved document storage facility.

DRAFT 01/05/15

Confidentiality

Keeping Your Computer Safe

Emails, attachments, websites, and software programs may carry malware and viruses, damaging your computer and Metra data.

DRAFT 01/05/15

Confidentiality

Keeping Your Computer Safe

Follow these guidelines to help keep Metra data safe:

- Do not preview or open email (or email attachments) from sources you do not know or trust. If you are not familiar with the sender or if the content does not seem appropriate, delete the email.
- Do not use or share freeware or software on Metra equipment.

Confidentiality

Keeping Your Computer Safe

- Do not share inappropriate emails, such as jokes or chain letters, with your co-workers.
- Do not visit “risky” web sites. These web sites install malicious code even on well-protected computers.
- Do not save login and password information on web sites.
- Never share your passwords.
- Change your logon password and web site passwords periodically. Changing passwords monthly is a good idea.

Confidentiality

Keeping Your Computer Safe

- Do not bypass security features on your computer. This includes changing security settings in Internet Explorer or Mozilla Firefox.
- Be careful with portable or “thumb” drives. External drives are potential sources for virus entry into the system.
- Store business-critical files on network drives (e.g., H:/ drive, I:/ drive). Information stored there is automatically backed up daily and stored off-site.

Confidentiality

Keeping Your Computer Safe

Follow these steps to set your computer screen to lock automatically:

1. Click on the *Start* button, then select *Control Panel* in the column on the right.
2. Click on *Personalization* (your screen might say *Appearance and Personalization,* depending on your settings).
3. Click on *Screen Saver* in the lower right corner.

DRAFT 01/05/15

Confidentiality

Keeping Your Computer Safe

4. Click on the Screen Saver drop-down menu and select a screen saver.
5. In the *Wait* box, adjust the number of minutes (15 minutes or less) and check the box for *On Resume Display Login Screen*.
6. Click OK.

Contact the IT department at Ext. 6508 if you need help.

Confidentiality

Guard Your Conversations

Sometimes, an “innocent” remark that you intend to be helpful, can actually betray CI.

Here is an example:

DRAFT 01/05/15

Confidentiality

Guard Your Conversations

Skylar is complaining to a coworker about “X.” (“X” can be a mortgage company, a brand of blood glucose meter, etc.).

Casey, who works in HR, overhears the remark. Casey tells Skylar about the benefits of using “Z” instead, because Mr. Jones in Accounting likes using Z for a similar situation.

Confidentiality

Guard Your Conversations

Casey means well. But both coworkers now have private information about Mr. Jones. Other people in the vicinity also know about it.

They might tell others, such as a cousin who sells mortgages or diabetes supplies. The cousin might call Mr. Jones to try and make a sale.

Confidentiality

Guard Your Conversations

Be careful when discussing CI in person or on the telephone.

- Only discuss CI with authorized individuals.
- Do not discuss CI in a place where you can be overheard by an unauthorized person.
- Keep your voice at a moderate level – don’t shout across the room.
- Use the speakerphone only when you are certain your conversation will not be overheard.

Confidentiality

Alert recipients of emails and faxes

Add an alert notice on emails and faxes when sending CI. Include the following notice on the cover email and fax cover sheet that accompany CI:

Confidentiality

Alert recipients of emails and faxes

This message may contain information that is privileged, confidential, and exempt from disclosure. If the reader of this transmission is not the intended recipient, you are hereby notified that any dissemination, disclosure, copying, distribution, or use of the information contained herein (including any reliance thereon) is strictly prohibited. If you received this transmission in error, please contact the sender and delete the material from any computer immediately.

Confidentiality

Best Practices

When handling confidential paper information:

- Always lock filing cabinets.
- Store documents on your desk in manila folders when you step away.
- Plan to retrieve sensitive information from the printer immediately. Some printers allow you to create and save a password that you must enter at the printer itself before your document will print.

Confidentiality

Best Practices

When handling confidential paper information:

- As you finish working with CI documents, store them in a folder until you put them away before the end of the day.
- At the end of the day, don't leave CI in locations accessible to the janitorial staff.

DRAFT 01/05/15

Confidentiality

Best Practices

When handling confidential electronic information:

- Double-check that you attach the correct sensitive documents to emails. It is easy to forget to include the attachment, or include the wrong one.
- Always lock your computer screen when you step away – even for a moment.

DRAFT 01/05/15

Confidentiality

Best Practices

- Set your computer screen to automatically lock after a specific period of time (15 minutes, for example), and to require a password to regain access.
- At the end of the day, log all the way out of your PC and shut it down.

Confidentiality

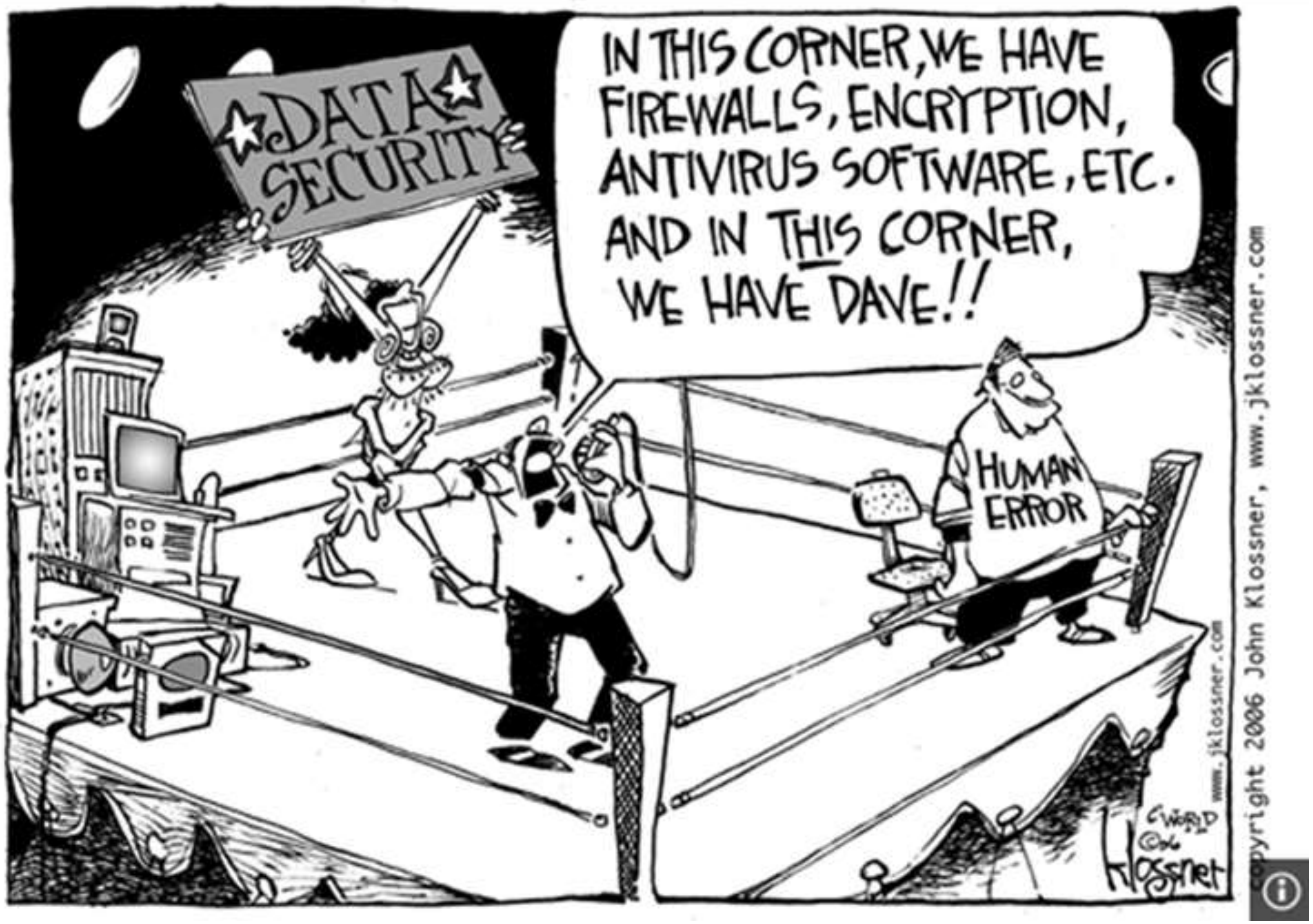
Review

You now have the knowledge to:

- Define confidential information.
- Assess different levels of CI.
- Understand the consequences of leaking CI.
- Use best practices to keep information confidential.
- Use appropriate methods to store or dispose of CI.

DRAFT 01/05/15

Confidentiality


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
Copyright 2006 John Klossner, www.jklossner.com
www.jklossner.com
©WORLD ©06
Klossner