King’s Daughters

Annual General Compliance Training

November 2022

KING'S DAUGHTERS

King’s Daughters Commitment

- King’s Daughters is committed to compliance with applicable laws, rules and regulations, including the Anti-Kickback Statute, Stark Law, and other federal healthcare laws and regulations.

- At the direction of the Board of Directors, King’s Daughters established a comprehensive compliance program through the establishment of the Compliance & Integrity Department.

- The Compliance & Integrity Program (“Program”) aligns with the Office of Inspector General (OIG) Guidelines and the Federal Sentencing Guidelines. The Program contains the following seven elements: (i) written policies, procedures and Code of Conduct; (ii) compliance officer and compliance committee; (iii) training and education; (iv) effective lines of communication for reporting concerns; (v) enforcement and discipline of policies and procedures; (vi) internal monitoring and auditing program; and (vii) response and prevention program to detect, deter and prevent offenses and violations of fraud, waste and abuse.

KING'S DAUGHTERS

Seven Elements of the OIG Model Compliance Program

Policies and Procedures

Compliance Officer and Compliance Oversight

Screening Employees, Contractors, Physicians, Board Members

Education

Auditing and Monitoring

Corrective Actions to Identified Problems

Enforcement of Violations

KING'S DAUGHTERS

Heather Marcum
Compliance & Privacy Officer
x80161

Tonia Hall
Compliance & Privacy Manager
x84451

KING'S DAUGHTERS

How do I report suspected compliance violations?

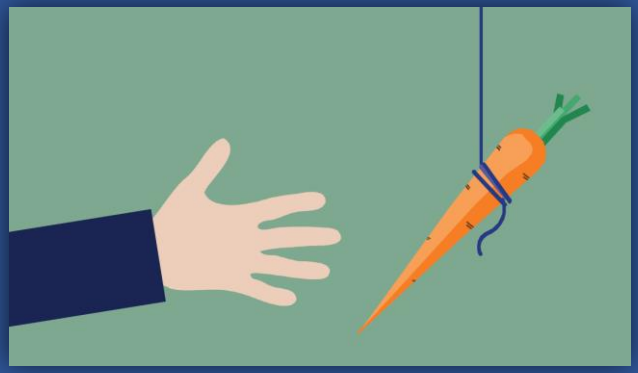
All King's Daughters team members, providers, and contractors/vendors are required to report concerns about actual, potential or perceived misconduct to the Compliance & Integrity Department. One may use any of the following reporting tools:

- Call the Compliance Hotline at (606) 408-4145 or (877) 327-4145;
- Call the Lighthouse Services Hotline at (844) 940-0003 which is an independent third-party hotline provider contracted by King's Daughters as an additional anonymous reporting tool;
- Complete the Compliance Concern Form found on the intranet;
- Contact Compliance team, Tonia Hall @ (606) 408-4451 or Heather Marcum @ (606) 408-0161;
- Contact your supervisor, director or Vice President;
- Email corporatecompliance@kdmc.kdhs.us (not anonymous);
- Send written correspondence intercompany to 2201 Lexington Avenue, Ashland, KY 41101 Attn: Compliance & Integrity Department.

KING'S DAUGHTERS

Inducements to Patients

- Social Security Act – enacted as part of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), prohibits providers of Medicare or Medicaid payable services from offering remuneration to beneficiaries.
- Examples of remuneration are:
  - Waivers of copayments and deductible amounts
  - Providing items or services for free or for other than fair market value
  - Providing gifts of more than nominal value



So how does this apply to team member's everyday work?

- Neither KD nor team members are permitted to give or receive cash, either individually or collectively, to patients or families
- Social work team can access resources to assist patients in some circumstances
- As part of service recovery, and occasionally through grant funding, KD provides small amenities and/or gas cards to patients/families
- Gifts to patients/families are limited to a retail value of no more than $15 individually, and no more than $75 annually per patient
- Patient representative team tracks items provided to patients and families
- If you perform service recovery to a patient, please make your manager or supervisor aware for tracking purposes

KING'S DAUGHTERS

Federal False Claims Act

The False Claims Act provides for civil liability for individuals and organizations that knowingly submit, or cause the submission of, false claims to the Federal Government.

Examples include, but are not limited to, claims for services that:

- Have not been provided;
- Are not supported by documentation in the patient's medical record;
- Are paid or being paid by another claim; or
- Are incorrectly coded

KING'S DAUGHTERS

Fraud, Waste, and Abuse

King's Daughters is committed to preventing, detecting, reporting, and correcting fraud, waste, and abuse. Examples of fraud, waste, and abuse include:

- Misrepresentation of the type or level of service provided;
- Misrepresentation of the individual rendering service;
- Billing for items and services that have not been rendered;
- Billing for services that have not been properly and timely documented;
- Billing for items and services that are not medically necessary;
- Seeking payment or reimbursement for services rendered for procedures that are integral to other procedures performed on the same date of service (unbundling);
- Seeking increased payment or reimbursement for services that are correctly billed at a lower rate (up-coding);
- Misusing codes on a claim; and
- Charging excessively for services or supplies.

KING'S DAUGHTERS

Stark Law & Anti-Kickback Statute

Stark Law (also know as Physician Self-Referral Law)

Prohibits physicians from referring Medicare or Medicaid patients to receive “designated health services” from an entity with which the physician or an immediate family member has a financial relationship.

Some examples of designated health services include: clinical laboratory services; therapy services; durable medical equipment; home health services; inpatient and outpatient hospital services

Anti-Kickback Statue

Prohibits receiving or offering to exchange anything of value in an effort to induce or reward the referral of healthcare program business

Kickback examples can include: gifts, bribes, overbilling

KING'S DAUGHTERS

How does King's Daughters prevent violations of the False Claims Act?

- King's Daughters established a comprehensive compliance program through the establishment of the Compliance & Integrity Department.
- Here are some examples of compliance program activities:
  - Internal Audit's auditing efforts;
  - Compliance & Integrity Department's monitoring and auditing compliance plan;
  - Contracting with external resources to provide reviews;
  - Revenue Cycle's data mining and monitoring;
  - Leaders' self-monitoring their department risks;
  - Annual Compliance Risk Assessment;
  - Review of the Office of Inspector (OIG) Work Plan which identifies risks;
  - Follow up on concerns reported to the Compliance & Integrity Department

KING'S DAUGHTERS

Overpayments

The Affordable Care Act requires that a person (e.g., provider, hospital, medical office) who received a Medicare or Medicaid Overpayment to report and return the Overpayment.

What is an Overpayment?
A Medicare or Medicaid overpayment is "any funds that a person receives or retains to which the person, after applicable reconciliation, is not entitled."

Examples of Overpayments include, but are not limited to, the following:

- Billing the wrong level of care for an office visit;
- Separately billing services which should have been bundled into one bill;
- Billing for an MRI when a CT was performed;
- Billing for a service which was not properly documented; or
- Billing for a service which was not medically necessary.

It doesn't matter if an Overpayment is a mistake or not intentional. If Medicare or Medicaid paid an excess amount, an Overpayment occurred.

KING'S DAUGHTERS

Overpayments

- An Overpayment must be reported and returned no later than sixty (60) days after the date on which the Overpayment was identified.
- Failure to report an Overpayment may result in liability under the False Claims Act.
- If you suspect an Overpayment has occurred, immediately contact your supervisor or the Compliance & Integrity Department.

KING'S DAUGHTERS

Medical Necessity

- Medical Necessity is a term which can be complex for all participators in healthcare.
- A provider's understanding of medical necessity may be different from that of a patient, patient's family or third-party payer. Different participators sometimes apply the term in different ways.
- CMS gives a definition of Medical Necessity in the Social Security Act:
  - *"…no Medicare payment shall be made for items or services that are not reasonable and necessary for the diagnosis or treatment of illness or injury or to improve the functioning of a malformed body member"*
- Because the diagnosis drives the determination of medical necessity, it is important that patient's history and assessment is thoroughly documented in the medical record.
- Medicare issues National Coverage Determinations (NCDs) and Local Coverage Determinations (LCDs) to provide guidance on coverage requirements/limitations for specific treatments or procedures. NCDs and LCDs are available on the internet.
- Medical necessity becomes more complex with third-party payers who often have specific coverage rules for specific treatments or procedures. If you have questions regarding medical necessity, please contact leaders in your work area or the Compliance and Integrity team.

KING'S DAUGHTERS

Preventing Overpayments

To reduce the chance that an overpayment could be made, King's Daughters takes these actions:

Monitoring	National and Local Coverage Determinations	Audits	Reporting
• Billing functions for professional, hospital, and home care services are regularly monitored by applicable departments;	• National and Local Coverage Determinations identify Medicare's payment and coverage criteria for certain tests and procedures. Many of these National and Local Coverage Determinations are 'built' in EPIC and generate prompts when entering a test or procedure;	• Audits are performed by Internal Audit, Compliance & Integrity, and external contractors.	• Team members are required to report any suspected concern with billing activities which may result in overpayment. Reports can be made using any of the available reporting methods.

KING'S DAUGHTERS

National and Local Coverage Determinations

- One way Medicare provides guidance regarding medical necessity is through the issuance of National (federal) Coverage Determinations and Local (regional) Coverage Determinations (NCD/LCD) (see Administrative Policy A(7)).
- NCD/LCD document identifies the conditions under which payment will be made for certain tests, services and procedures.
- Department directors are responsible to be knowledgeable of those NCD/LCDs which pertain to the services provided by the Department and ensure the NCD/LCD elements, as applicable, are met.
- Elective ordered tests, services and procedures which do not meet NCD/LCD requirements should be processed in accordance with Administrative Policy A(5), Issuance of Advance Beneficiary Notice.

Potential Consequences of Noncompliance

Failure to comply with applicable laws, regulations, and CMS requirements may lead to serious consequences, such as:

- Contract Termination
- Criminal Penalties
- Civil Monetary Penalties
- Exclusion from Federal Health Care Programs

KING'S DAUGHTERS

EMTALA – Emergency Medical Treatment and Active Labor Act

EMTALA defines 3 responsibilities of participating hospitals (defined as hospitals that accept Medicare reimbursement):

1. Provide all patients with a medical screening examination
2. Stabilize any patients with an emergency medical condition
3. Transfer or accept appropriate patients as needed

Most common violations include:

- Failure to screen for emergency medical condition
- Failure to stabilize a patient with emergency medical condition
- Hospital failed to accept transfer of a patient with emergency medical condition
- Inappropriate transfer of a patient with emergency medical condition
- Failure to provide medical screening exam and stabilize an obstetric patient in active labor

KING'S DAUGHTERS

HIPAA and IT Security

KING'S DAUGHTERS

Notice of Privacy Practice

- HIPAA requires King's Daughters to provide each patient a "Notice of Privacy Practice" which:
  - Describes how the facility may use and disclose PHI
  - Advises the patient of his/her privacy rights
- King's Daughters must attempt to obtain a patient's signature acknowledging receipt of the Notice, EXCEPT in emergency situations. If a signature is not obtained, the reason must be documented.
- The registration process is critical in distributing the Notice of Privacy Practices and getting patient signatures.

KING'S DAUGHTERS

Business Associates

- HIPAA also applies to business associates. A business associate is a person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a covered entity.
  - Examples: Billing vendors, Tri-Data, Knight Horst Maintenance service providers, etc.
- To comply with HIPAA, all business associates must have business associate agreements with King's Daughters.
  - King's Daughters can be held responsible if our business associates are not compliant with HIPAA.
- If you utilize a vendor who may qualify as a business associate, please contact Legal Services to assure an appropriate agreement is in place.
- You can contact Sydney Keeton, Director of Legal Services, at x 80179.

www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html

KING'S DAUGHTERS

Protecting Patient Information

- As a King's Daughters Team Member, maintaining a patient's privacy is part of your job. You should access or view a person's PHI only when it is required for your job. Simply because you are able to see a person's PHI does not mean it is permissible.

- King's Daughters routinely conducts audits of access to patient records and our systems to ensure proper access by Team Members.

- All patients are entitled to privacy and confidentiality. Do your part and only look at the Minimum Necessary information you need to do your job.

Privacy policies can be located in the Privacy Manual on the intranet.

KING'S DAUGHTERS

Protected Health Information

Protected Health Information (PHI) is information you create or receive in the course of providing treatment or obtaining payment for services. It includes:

- Information related to the past, present or future physical and/or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present or future payment for the provision of healthcare; **AND**
- Includes at least one of the **18 personal identifiers OR** there is a **reasonable basis to believe** the information can be used to identify the individual.
- Information in all formats – oral, written, electronic – including videos, photographs, x-rays, etc. - must be protected.
- It **DOES NOT** include health information about individuals who have been deceased more than 50 years.

KING'S DAUGHTERS

PHI Identifiers

PHI identifiers are

1. Name
2. Postal Address
3. All elements of dates except year
4. Telephone number
5. Fax number
6. Email address
7. URL address
8. IP address
9. Social Security Number
10. Account numbers
11. License numbers
12. Medical record number
13. Health plan beneficiary number
14. Device identifiers & their serial numbers
15. Vehicle identifiers and serial number
16. Biometric identifiers
17. Full face photos & other similar images
18. Any other unique identifying number, code or, characteristic

KING'S DAUGHTERS

How can PHI be used?

- Providers are permitted to use or disclose PHI for:
  - Treatment
  - Payment
  - Healthcare operations (e.g., legal, medical staff/peer review, audit, business management)
  - The individual patient who is the subject of the PHI, and
  - Other uses and disclosures required by law
  - In **all other instances**, a **written authorization** from the patient is needed.
  - Whenever in doubt about release of information, contact Medical Records Department (81821), Privacy department, (x80161 or x84451) or Legal Services (x80179) for guidance.

KING'S DAUGHTERS

Patient Rights Under HIPAA

- Right to access and receive a copy of one's own PHI (paper or electronic format)
- Right to request amendments to information
- Right to request restriction of PHI uses and disclosures
- Right to restrict disclosure to health plans for services self-paid in full
- Right to request alternative forms of communications
- Right to request an accounting of disclosures of PHI

Any questions regarding these rights, please call the Privacy Department at x80161 or x80455

KING'S DAUGHTERS

Privacy Tips

- Never take unsecured PHI home with you
- Speak quietly in work areas
- Avoid using patient names, discussing cases, or other patient identifying characteristics in public areas
  - We live in a small community, and even the smallest details might be identifiable to someone who overhears
- Use the shred bins located throughout King's Daughters to shred documents (that do not need to be preserved) with PHI
- Always obtain at least two patient identifiers before handoff of documents or discussing patient information
- Double check the mailing address to ensure the PHI is being sent to correct person

KING'S DAUGHTERS

Privacy Monitoring

- The Privacy Department has monitoring capabilities through implemented artificial intelligence and machine learning tools
- Team Members who access medical records unrelated to their job may face corrective action including discipline, suspension, or termination of employee

KD policies:

- Confidentiality of PHI (E8)
- Minimum Necessary Requirements (Privacy Manual)

KING'S DAUGHTERS

Examples of Inappropriate Access

- Accessing records to “check on a patient” because you saw a news story about the patient and wanted to see their status
- Accessing the records of a family member when you are not involved in their care
- Accessing medical records of a neighbor out of curiosity
- Accessing medical records of a co-worker in the hospital to “see how they are doing”
- Accessing your child’s or spouse’s medical records to check their health status
- Obtaining telephone numbers or demographic information without proper authorization or necessary means

KING'S DAUGHTERS

Social Media and Patient Privacy

- NEVER share identifiable information about patients on social media, for example:
  - Posting of patient name/date of birth
  - Posting of images and videos of patients without written consent
  - Posting of gossip about patients
  - Posting of any information that could allow an individual to be identified
  - Sharing of photographs or images taken inside a healthcare facility in which patients or PHI are visible
  - Sharing of photos, videos, or text on social media platforms within a private group
- Identifiable information can also include tattoos, birthmarks, moles, patient's face or initials
- Considered by Privacy Department to be a high risk activity
- Corrective action can include termination

"HIPAA Social Media Rules". HIPAA Journal. April 2022. www.hipaajournal.com/hipaa-social-media

KING'S DAUGHTERS

THINK

BEFORE YOU SPEAK, POST ONLINE OR HIT SEND

Take into consideration:

- *Who might be able to read this?*
- *Am I posting in anger?*
- *Could someone feel disrespected?*
- *Does my post include information to identify the individual?*
- *Am I revealing too much about myself?*
- *Am I showing a bad side of myself?*
- *Could someone misinterpret what I'm saying?*

KING'S DAUGHTERS

House Bill 5 – KY Data Privacy Bill

Due to public entity status, members of the health system are subject to Kentucky's Data Privacy Bill, imposing data security, investigation and breach notification requirements.

Key Concepts

House Bill 5 Kentucky Data Privacy Bill: Imposes data security, investigation, and breach notification requirements on governmental agencies and "nonaffiliated third parties" (NTPs) doing business with governmental agencies. There is a 72-hour reporting requirement to complete the initial breech report to governmental agencies.

KD Impact

- Due to public entity status, KD will be required to complete breach notifications in accordance with the KY Data Privacy Bill.
- If you have questions, please reach out to Heather Marcum, KD Compliance Officer.

KING'S DAUGHTERS

Why Report Privacy Concerns?

- King's Daughters is required by law to report breaches to the Department of Health and Human Services, Office of Civil Rights.
- When King's Daughters reports a breach, we are essentially reporting a violation of the Privacy Rule (HIPAA).
- If HHS suspects that the breach or violation resulted from "willful neglect," they will conduct a compliance review.
- A fine of up to $50,000 per violation can be assigned for each HIPAA violation.

KING'S DAUGHTERS

KD Password Recommendations

- Passwords should be difficult to guess
- Passwords should be as complex as possible
- Do not use the “Remember Me” feature in Windows
- 12 Character Minimum
- Password Change Interval = every 2 years

KING'S DAUGHTERS

User Credentials

- **Only log on to computer systems with your own user ID and password. Never use someone else's.**
- You will be held responsible for all activity under your user ID.
- Log off from work stations when you walk away from it.
- Do not share passwords, ID badges, or other access credentials with anyone.
- Password complexity is an important deterrent to unauthorized access.

KING'S DAUGHTERS

Guide to Great Security Hygiene

The following are a few common, non-technical processes that help improve your daily security hygiene. Keep in mind that the following tips aren't isolated to work, we encourage you to apply them to your personal life and promote security awareness within your household!

1. **Create strong, unique passwords or passphrases for every account.** Great security hygiene begins with strong passwords that are at least 12 to 16 characters long and are never used for more than one account. Even better, replace your traditional passwords with passphrases, which are strings of words that make sense to you such as obscure quotes from your favorite book or song. This tactic makes them easy to remember but hard to guess.

2. **Keep your work area clean and organized.** When working in a traditional office, keep your area clean and organized. Believe it or not, messy desks qualify as security risks. It's a lot easier to misplace sensitive materials, ID cards, and other important items if your workstation is disorganized.

3. **Report all security incidents immediately.** Where sensitive materials are concerned, always store them in a secure manner, and shred them when no longer needed. Proper disposal prevents unauthorized access to sensitive data.

4. **Always follow KD policies.** Keep in mind that despite our best efforts, security incidents may happen. So if you see something, say something immediately! The longer an incident goes unreported, the more damage it could cause. From phishing emails, to unsecured doors, every incident, even those that seem minor, should be reported immediately.

5. **Secure your work-from-home environment (if applicable).** If you work from home, remember that King's Daughters policies still apply. Be sure to secure your work-from-home environment by keeping your devices locked when not in use and preventing other members of your household from accessing anything work related.

KING'S DAUGHTERS

What is Social Engineering?

Social engineering is the art of manipulating or deceiving you into taking an action or divulging sensitive information.

Watch out for three types of attacks:

• **Digital Attacks** – Phishing - Email-based social engineering targeting an organization. – Spear Phishing - Email-based social engineering targeting a specific person or role	**YOUR ROLE:** STOP, LOOK, and THINK before clicking on a link or opening an attachment.
• **In-Person Attacks** – USB Attacks - An attack that uses a thumb drive to install malware on your computer. – Tailgating - When a hacker bypasses physical access controls by following an authorized person inside.	**YOUR ROLE:** STOP, LOOK, and THINK before complying with requests from strangers who prey on your social nature. It is better to be firm than insecure.
• **Mobile/Phone Attacks** – Smishing - Text-based social engineering. – Vishing - Over-the-phone-based social engineering.	**YOUR ROLE:** STOP, LOOK, and THINK before clicking on a link in a text message or divulging sensitive information over the phone.

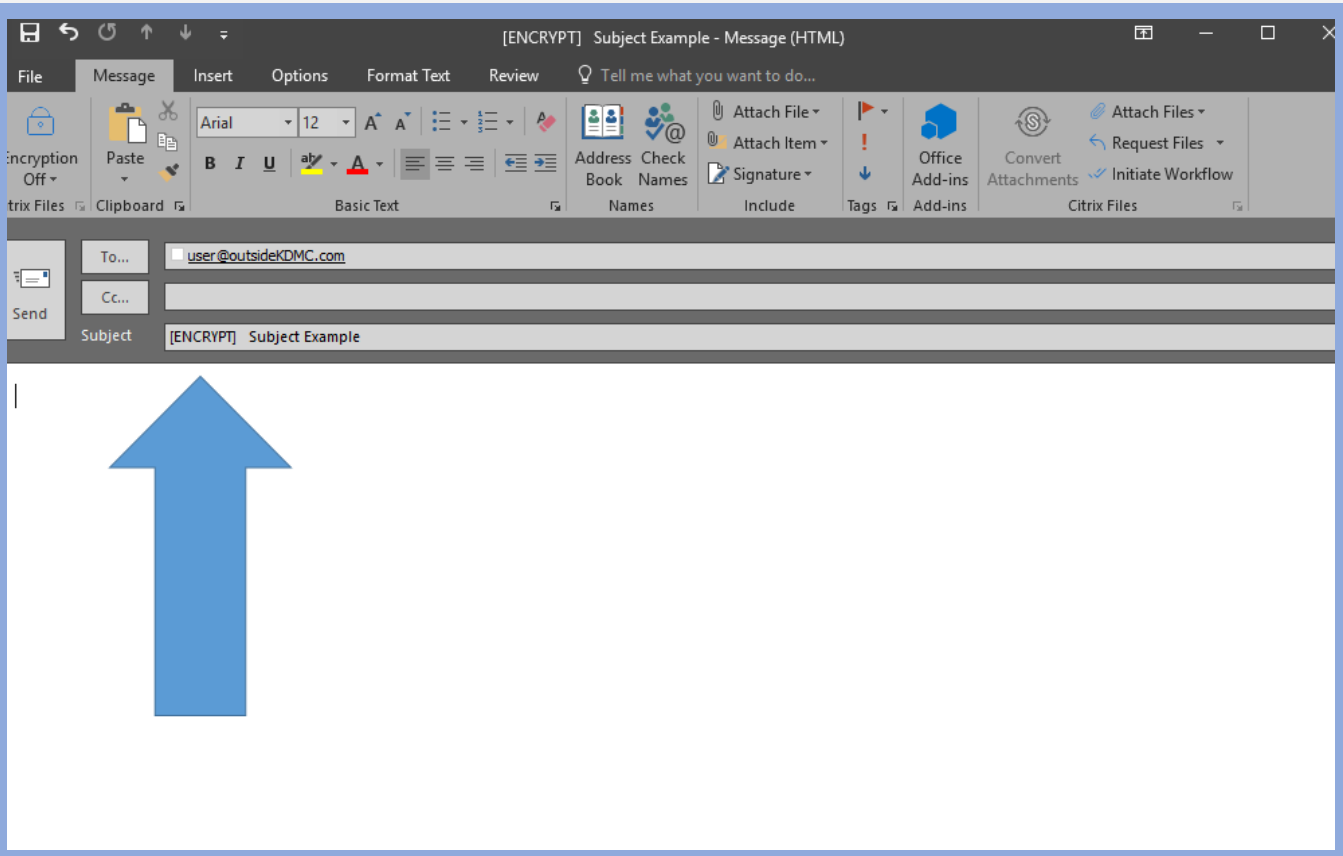
KING'S DAUGHTERS

Email Security & Protection

- Do not send confidential information in an email, in either the message or in an attachment, unless the communication line is secure and encrypted.
- If you do not know the sender of an email do not open the email, if you inadvertently open the email do not open attachments or select any hyperlinks.

KING'S DAUGHTERS

Secure Encrypted E-Mail



Do not send confidential information in an external email, in either the message or in an attachment, unless the communication line is secure and encrypted.

KING'S DAUGHTERS

Business Email Compromise

Business email compromise, or BEC, is an advanced phishing scam that impersonates people, organizations, or entities that the victim knows. It works by manipulating email addresses so the sender appears to be legitimate.

Common Examples of BEC:

- Fraudulent Invoices - By impersonating vendors or other account representatives, scammers can trick people into wiring funds to fraudulent accounts. This is often accomplished by sending fake invoices that look almost exactly like an invoice the victim typically receives.
- CEO Fraud - How likely are you to respond to an email that appears to come from your boss? CEO fraud involves a cybercriminal attempting to impersonate upper management and sending out requests for wire transfers of money or confidential information.
- Account Takeover - When someone falls victim to a phishing attack, they may lose control of their email account. This then allows the attacker to distribute phishing emails to the victim's contact list. Since the recipient recognizes the account, they are likely to engage with the attacker.
- Employee Data Theft - Those who work in accounting or human resources have access to an abundance of employee information. Cybercriminals often target those people in hopes of stealing data such as full names, national ID numbers, home addresses, and phone numbers.

You can thwart these attacks by slowing down and:

- Carefully inspecting the sender's email address. Scammers often create addresses that appear to be legitimate but actually contain slight variations in the way they're spelled.
- Paying attention to the tone. When you email regularly with someone, you are likely familiar with how they communicate via text. Unusual tone = untrustworthy email.
- Avoiding attachments. Email attachments represent one of the most common ways malware gets distributed. Never open an attachment unless you have confirmed it's safe.
- Verbally confirming. If you receive a request for money or confidential information, it's always a good idea to confirm with them via an alternative method before complying.

KING'S DAUGHTERS

Phishing Fundamentals

Securing Your Inbox
Email continues to represent the main way cybercriminals launch phishing attacks. Even though modern spam filters can eliminate the majority of spam and suspicious messages, it's up to you to filter out the rest. Here are five ways to secure your inbox:

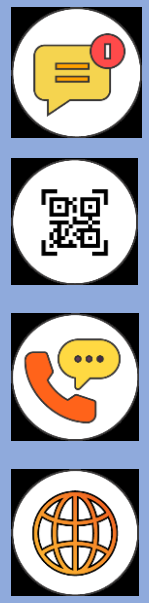
- **Know the warning signs.** Phishing scams often feature recognizable warning signs. Poor grammar, threatening language, unrealistic promises, and unexpected attachments all qualify. If a message includes any of these signs, take extreme caution and assume you're being targeted.
- **Hover over links.** Hovering your mouse over a link will reveal the full URL. This helps you spot malicious links, which usually lead to websites that have nothing to do with the context of the message. Note, however, that even if a link appears safe, it could still be dangerous. Only click if you're absolutely sure.
- **Don't make assumptions.** Just because an email appears to come from someone you know doesn't mean it's safe. For example, if a major data breach leaks thousands of usernames and passwords, cybercriminals could use that data to take over people's accounts and distribute phishing emails. Always take note of the tone and context of a message to avoid getting scammed.
- **Remain skeptical.** There's a fine line between being paranoid and being proactive. We want you to live on the proactive side by treating all requests for confidential information or money with a high degree of skepticism. Follow your instincts, and use situational awareness!
- **Report suspicious emails immediately.** Any time you suspect an email is a phishing attack, don't click, don't respond, and don't ignore it. Instead, follow policy and report it immediately. Timely reporting allows King's Daughters to analyze the email and take measures to ensure the sender can't distribute additional phishing attacks to your co-workers.

KING'S DAUGHTERS

Phishing in every format

Email isn't the only way scammers attempt to phish people. They'll happily use every format available to them. Let's explore a few other avenues.

- Text Messages
  - Malicious text messages feature many of the same techniques found in typical phishing attacks. They often claim a bank account has been compromised and ask you to immediately click on a link. Doing so could give a cybercriminal access to personal information or allow them to take over banking and social media accounts.
- QR Codes
  - Many organizations use QR codes as a quick and convenient way to direct users to websites or other services. Scammers also use QR codes to send users to malicious sites that steal login credentials or infect devices with malware. It's generally best to never scan codes unless you're sure they're safe. When in doubt, go directly to a website through a browser app rather than a QR code.
- Phone Calls
  - Since phone numbers are so easy to acquire, cybercriminals have been using them for decades to scam people out of money and personal information. It's a practice known as vishing, or voice phishing. In many cases, vishing attacks use an automated system that asks you to enter banking details. Some attacks will even connect you to a live scammer who will attempt to impersonate legitimate organizations.
- Web Browsers
  - Browser push notifications are small messages that deliver information to users. While push notifications can serve useful purposes, they're also abused by malicious hackers to deliver malicious advertisements or trigger installation of unwanted software. Ideally, block all browser notifications to help avoid this threat.



KING'S DAUGHTERS

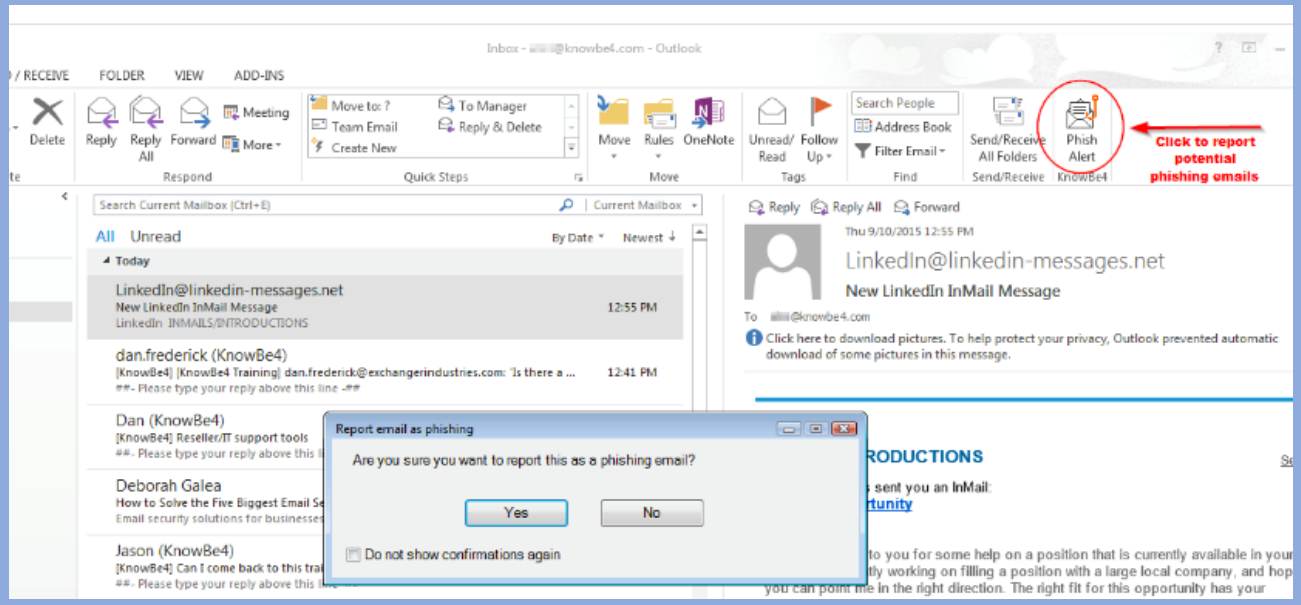
Phish Alert button

- KD has installed the Phish Alert Button (PAB) in your mail client. Learn how this tool works and how you can use it to help keep King's Daughters safe from malicious phishing emails.
- When do I use it?
  - Click the PAB if you believe you have received a phishing email or any potentially dangerous email. Any emails you report using the PAB will be automatically deleted from your inbox. The emails you report will be forwarded to IST Security for analysis.
  - **The PAB should only be used to report emails you believe to have malicious intent.**
  - If you are receiving *spam or marketing emails*, you should not use the PAB to report these. You can delete these types of emails.
- Why should I use it?
  - Reporting emails will help KD stay safer. Because the potential phishing emails you report are sent for analysis to IST Security, King's Daughters will now be aware of which phishing attacks are able to reach their employee inboxes. Once we are aware of possible vulnerabilities, we can better defend against them. You are an important part of the process of keeping KD safe from cybercriminals.

KING'S DAUGHTERS

Phish Alert button

- How do I use it?
  - Once the PAB add-in is installed the PAB add-in will appear at the top of your Outlook client.



In this view, to report an email as a phishing email:

1. Click the **Phish Alert** button while the email is open.
2. A prompt will ask you if you want to report the email as a phishing email. Click **Yes** to report the email, or click **No** to not report the email.

How To Report a Phishing Email if You DO NOT HAVE the button:

Please forward the email to: phishalert@kdmc.kdhs.us

KING'S DAUGHTERS

Cybercrime happens more than you think!

Large-scale cyberattacks make the news, but that's just the tip of the iceberg. Cybercrime is on the rise, and the majority of attacks go unreported.

- A cyberattack every 36 seconds
  - The University of Maryland found that there is an average of 2,244 cyberattacks per day, which is one every 36 seconds.
- 43% of Small–and–medium sized businesses lack a cybersecurity defense plan
  - The International Criminal Police Organization (Interpol) reported that small- and medium-sized businesses (SMB) are being targeted at an increased rate.
- $108 Million lost in only 6-months
  - The US Federal Trade Commission, in a recent 6-month period, had seen over 128,000 phone-based fraud scams that cost victims a whopping $108 Million – that's only half a year!

In the time it took you to read this document, there were multiple cyberattacks across the globe. Make sure you stop, look, and think before you take any sort of action.

KING'S DAUGHTERS

Things YOU can do to avoid data breaches

- If you see something strange, in the physical, cyber, or human domains, report it immediately!
- Know how to recognize social engineering attacks via email, SMS, on the phone, and social media.
- Mind your devices. Our lives are more mobile than ever thanks to smartphones and tablets. Where we go, our information goes.
- Always keep your technology with you when you are not in the office. We live a mobile life and security is absolutely essential!
- Use common sense while on the internet, using email and social networks.

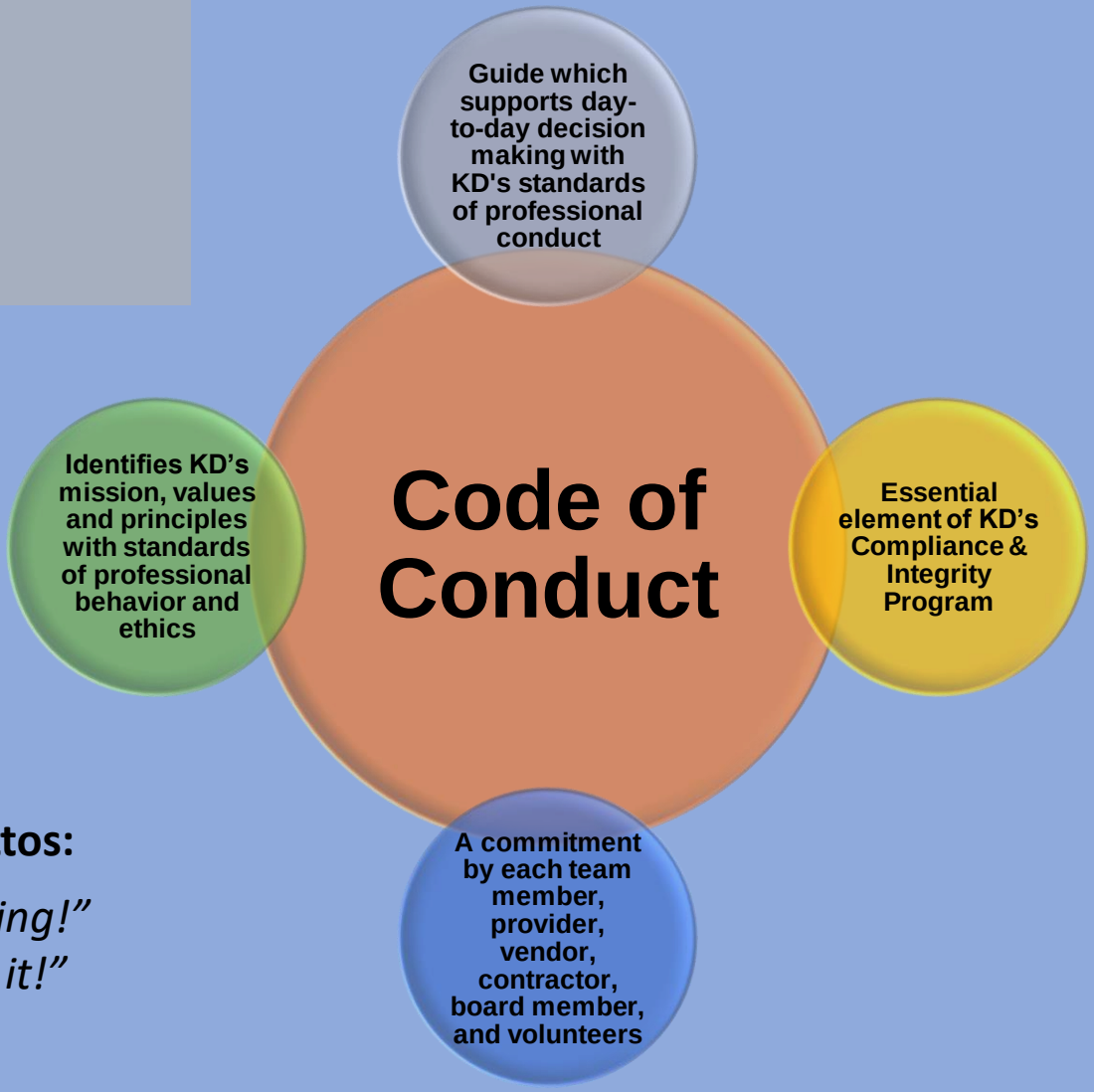
KING'S DAUGHTERS

IST Security Team

- David McDonald, Chief Information Security Officer, x89139
- Jason Fox, Cybersecurity Analyst, x 89134
- Alan Clark, Cybersecurity Analyst, x89137

KING'S DAUGHTERS

Code of Conduct



Compliance Mottos:

"Do the Right Thing!"
"See it, say it, fix it!"

KING'S DAUGHTERS

Code of Conduct

- King's Daughters is committed to honest and ethical behavior and to conducting our business with integrity. The practice of behaving honestly, ethically and with integrity is an individual responsibility. We make decisions about how to conduct ourselves every day as we go about our work. Each of us is accountable for the actions that we choose to take.
- The Code of Conduct is the keystone of its corporate integrity philosophy and communicates its ethical business standards. The Code of Conduct serves as a cultural compass for team members, management, vendors/contractors, volunteers and others who interact with King's Daughters and all subsidiaries. It is an essential element of our Compliance & Integrity Program.
- The Compliance & Integrity Department oversees the King's Daughters Compliance & Integrity Program and ensures the subsidiaries maintains its commitment to conducting our business with integrity. The Compliance & Integrity Program is a partnership among all of us to make the right business choices.

KING'S DAUGHTERS

Conflicts of Interest

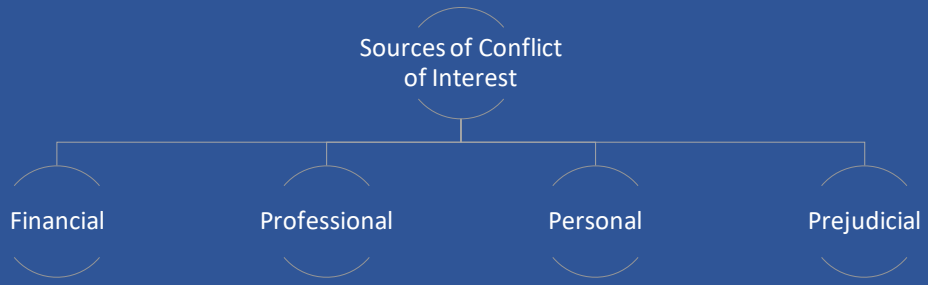
TM may not use their positions to profit personally at the expense of King's Daughters and subsidiaries.

Examples of Potential Conflicts:

- Provide consulting services to competitor
- Responsible for purchasing medical devices and you own a medical device company
- Directly supervising a close family member or in a position to make decisions to benefit the family member

Team members are obligated to report potential conflicts of interest:

- Upon hiring / on boarding process (conducted by HR)
- Any time a conflict develops
- During annual compliance training



KING'S DAUGHTERS

Gifts and Gratuities

King's Daughters Code of Conduct identifies:

- **Team members may accept unsolicited business courtesies from vendors, excluding cash, up to $50.00.**
  - For this reason, we are most often unable to accept vendor offers for complimentary conference attendance.
- **Team members and contracted providers may accept an unsolicited gift, excluding cash, from a patient or a patient's family member of less than $100.00**.

NOTE: Mastercard and/or Visa gift cards are considered cash.

Examples of acceptable gifts are:

- $25.00 gift cards for Starbucks, Texas Roadhouse, Cheddars
- $50.00 Cinemark movie pass
- Flower arrangement, candle
- Edible Arrangements bouquet, a cake from Tipton's or cookies from Sweet Caroline's

KING'S DAUGHTERS

Gifts to Medical Staff and/or Immediate Family

- Non-monetary compensation to physicians and their immediate family is regulated by CMS
- Examples of non-monetary compensation are: non-working meals, gift baskets, physician appreciation events, holiday parties, sporting events
- Physicians services tracks non-monetary compensation to physicians
- $452 annual limit for 2022; 2023 annual limit will be released in January
- Please report any gift to a provider or provider family member to your supervisor/manager/director, Physician Services, or Compliance and Integrity

KING'S DAUGHTERS

Workplace Sexual Harassment policy J(4)

King's Daughters strives to maintain a workplace that fosters mutual team member's respect and promotes harmonious, productive working relationships. In providing a productive working environment, King's Daughters believes that its team members should be able to enjoy a workplace free from all forms of discrimination, including harassment on the basis of race, color, religion, gender, national origin, age, disability, veteran status, uniformed service, marital status, pregnancy, sexual orientation, gender identity, or any other status or characteristic protected by law.

It is King's Daughters policy to provide an environment free from such harassment.

It is a violation of policy for any team member, whether a manager, supervisor or co-worker, to harass another team member. Harassment of third parties by King's Daughters team members, or harassment by third parties of King's Daughters team members, is also prohibited.

Please report suspected or violations to the Human Resource Department, supervisor, manager, director, or to the Compliance and Integrity Department.

KING'S DAUGHTERS

Conflict vs Bullying

Conflict

- Disagreement or argument in which both sides express their views
- Equal power – mutual engagement
- Equal emotional reaction
- Happens occasionally
- Can be accidental
- Not seeking power or attention
- Feelings of remorse and responsibility
- Effort to solve problem

Bullying

- Goal is to hurt, harm, or humiliate the victim
- Imbalance of power – one sided
- Strong emotional reaction from victim
- Happens repeatedly
- Intentional, threatening
- Seeking power and control
- No remorse – blames victim
- No attempt to stop

KING'S DAUGHTERS

What to do:

If you feel that you are being bullied, discriminated against, victimized or subjected to any form of harassment:

- **DO**
  - Firmly tell the person that his or her behavior is not acceptable and ask them to stop. You can ask a person you trust, such as a supervisor or team member to be with you when you approach the person.
  - Document the events in RL6 reporting system. Record:
    - The date, time, and what happened in as much detail as possible
    - The names of witnesses
    - The outcome of the event
  - Remember, it is not just the character of the incidents, but intent of the behavior and the number, frequency, and especially the pattern that can reveal bullying or harassment
  - Keep copies of any letters, memos, e-mails, etc., received from the person
  - Please report suspected or violations to the Human Resource Department, supervisor, manager, director, Risk Management Department, or to the Compliance and Integrity Department
  - If your concerns are minimized, proceed to the next level of management
- DO NOT RETALIATE. You may end up looking like the perpetrator and will most certainly cause confusion for those responsible for evaluating and responding to the situation.

KING'S DAUGHTERS

Abuse

- Abuse, neglect, exploitation know no boundaries. Any patient, at any age can become a victim, although people who depend on others for their emotional and physical health are at high risk.
- Everyone has a responsibility to immediately report suspected cases of abuse, neglect, domestic violence, sexual assault, or exploitation to Social Services.
- Social worker is on call 24/7 and can be reached through the switch board operator.

KING'S DAUGHTERS

Government or Accrediting Agency Contact

- If an agency requests information or access, in writing or in person, notify Compliance or Risk Management
- If an agency arrives at any location, notify Quality or Accreditation
- Always obtain Legal Services review PRIOR to signing any document on behalf of King's Daughters

KING'S DAUGHTERS

Open Records

Due to public entity status, members of the health system are subject to Open Records and Open Meeting statutes.

Key Concepts

Open Records: As a public entity all records are classified as "public records" and are subject to inspection pursuant to the Open Records Act (KRS 61.870-61.884). All written and recorded communications are subject to this requirement and must be disclosed unless a narrow exception applies.

KD Impact

- Electronic messages stored on KD servers (examples include: Doc Halo and KD email) are subject to open records, patient protected health information is redacted. However, an exemption may prevent disclosure.
- Direct any open records questions to Amy Saunders, King's Daughters General Counsel. UK Open Records Office will handle open records request in support of the health system.

KING'S DAUGHTERS

How do I report suspected compliance violations?

All King's Daughters team members, providers, and contractors/vendors are required to report concerns about actual, potential or perceived misconduct to the Compliance & Integrity Department. One may use any of the following reporting tools:

- Call the Compliance Hotline at (606) 408-4145 or (877) 327-4145;
- Call the Lighthouse Services Hotline at (844) 940-0003 which is an independent third-party hotline provider contracted by King's Daughters as an additional anonymous reporting tool;
- Complete the Compliance Concern Form found on the intranet;
- Contact Compliance team, Tonia Hall @ (606) 408-4451 or Heather Marcum @ (606) 408-0161;
- Contact your supervisor, director or Vice President;
- Email corporatecompliance@kdmc.kdhs.us (not anonymous);
- Send written correspondence intercompany to 2201 Lexington Avenue, Ashland, KY 41101 Attn: Compliance & Integrity Department.

KING'S DAUGHTERS

In Conclusion

Compliance can be summarized in a short phrase…

KING'S DAUGHTERS

Thank you for viewing this presentation.

Please complete the following items to receive credit for this course:

1. General Compliance Training Post-Test (upper right corner of this screen)
2. Conflict of Interest (on your KDHSU To Do List)
3. Americans with Disabilities Act Notice (on your KDHSU To Do List)
4. Training and Code of Conduct Attestation (on your KDHSU To Do List)

KING'S DAUGHTERS