San Joaquin
GENERAL HOSPITAL

Information Systems (IS)

- Staff of 28 people
- Support provide 24 x 7 x 365
- Supports all technology, applications, communications, and cybersecurity
- Utilizes a ticketing system to record, track, and manage requests for service
- Physically located next to the Cafeteria
- Dept Head is Ken Hoach, CIO (Chief Information Officer)

Health Informatics (HI)

- Staff of 6 clinicians (RN's)
- Staffed Mon-Fri during business hours with after-hours support for critical issues
- Supports the Cerner Electronic Health Record (EHR) and other integrated clinical systems
- Provides clinical training to staff and physicians
- Utilizes a ticketing system to record, track, and manage requests for service
- Dept Head is Dr. Joseph Izzo, CMIO (Chief Medical Information Officer)

How to request IS or HI Support?

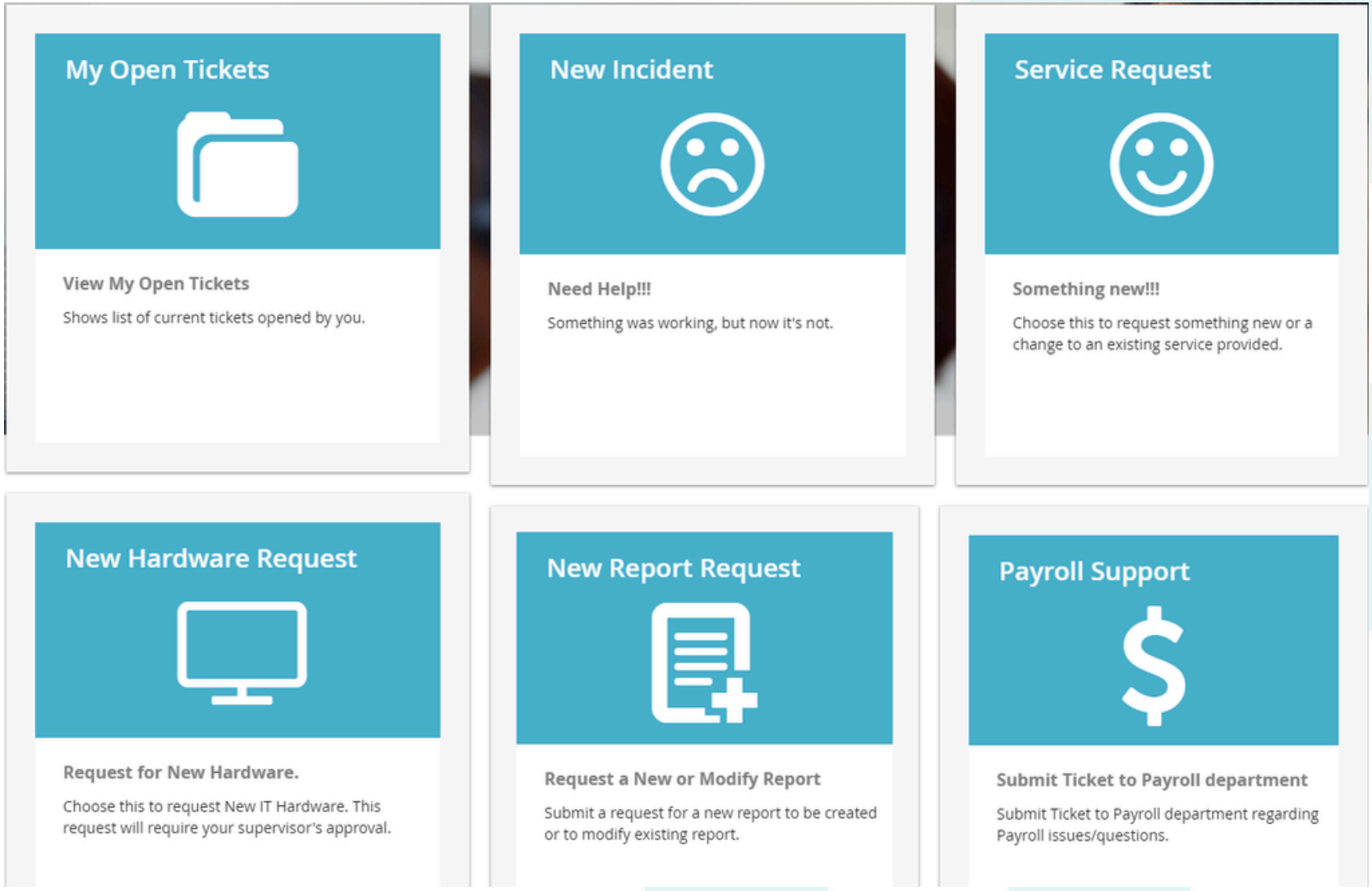
You can request IS or HI support through one of three ways:

1. Call the Service Desk (8-6180 or 468-6180)
2. Email the Service Desk (SJGHHelpDesk@sjgh.org)
3. Submit a request using the Self-Service Portal

How to request IS or HI Support?

- New or modified REPORT? : Send an email or submit a request via the portal
- PROJECT request? Send an email or submit a request via the portal
- New hire access/changes to existing access: Send user access form to SJGHonboarding@sjgh.org
- If you have an IS SECURITY concern (virus, compromised account, lost or stolen laptop, etc.), this is an INCIDENT. Call the IS/HI Service Desk at ext 8-6180
- You can view, track, and message the agent assigned to your ticket through the Self-Service Portal

Self-Service Portal



Cerner

- Comprehensive Electronic Health Record used for electronic medical records, practice management, charting, billing, etc
- Cerner was recently purchased by Oracle and is in the process of rebranding. Goes by Oracle Cerner – eventually Oracle Health
- The hospital uses Oracle Cerner Millennium (Oracle Health EHR) in a shared domain called Community Works

HIPAA Security

- The hospital is required to comply with the HIPAA Security Rule
- Defines the standards and requirements for securing protected health information (PHI)
- We must secure data when it's transported outside SJGH
- The hospital must designate an Information Security Officer. The SJGH Information Security Officer is: Arnel Cara acara@sjgh.org

Cybersecurity Terms

- **Malware**: Malicious Software intentionally developed to cause harm.
- **Virus**: A .specific type of malware that can self -replicate
- **Ransomware**: A type of malware that is designed to encrypt files, rendering any file unusable without a decryption key.
- **Spoofing**: An email that is disguised to look like it's from a legitimate source
- **Phishing**: Designed to trick you into clicking on a link, website, or opening an attachment.
- **Encryption**: Puts a secure "lock" on data that requires a virtual key known only to the recipient.
- **Patching:** Something IT routinely performs to ensure software has the latest security protections.

Cybersecurity Threats

- Change Healthcare (2023): Ransomware attack. Impacted 1/3 of US citizens. Est. $1 billion in damages. Paid $22 million in ransom.
- Dameron Hospital (2023): Ransomware attack. All IT systems and services were down for several months.
- CommonSpirit Health (2022): Ransomware attack. 623k patient records exposed. $160 million in damages.
- WannaCry (2017): Global ransomware attack. Est.$4 billion in damages.
- ILOVEYOU (2000): Global worm virus that infected over 10% of all connected PCs in the world. $5-8 billion in damages and $10-15 billion to remove the worm.

Cybersecurity at SJGH

- Security Awareness Training
- Multifactor Authentication
- Monthly Cybersecurity Newsletter
- SJGH Phishing Tests
- Systems Updating/Patching
- Cybersecurity Oversight on New Projects
- Cybersecurity Culture
- Policies and Procedures
- Harden Security Posture
- Backup / Disaster Recovery
- Endpoint Detection and Response
- Email Protection
- Vulnerability Scanning
- Security Operations Center Monitoring

IS Security Do's and Dont's

- Don't share your password with anyone
- Don't use someone else's account to log on
- Don't leave your laptop in your car or unattended
- Don't use email for personal reasons
- Do logoff or lock your workstation when not in use
- Do submit IS access request via IS Access Request Form
- Do report any IS Security concerns or events immediately

….remember, EVERYTHING you do on the computer is tracked and recorded. No expectation of privacy.

IS Security and Emails

- You are the best defense against malicious software.
- Email is one of the primary ways for malicious software.
- Be alert and on the lookout for malicious email.
- Bad hackers can make email appear legitimate.
- Sending Protected Health Information? ENCRYPT
  - Subject line: SJGHENCRYPT or SJGHSECURE

Things to look for in emails

- Sender's email address. Does the email address match the company's domain name?
  - Example: service@intl.paypal.com accounts@management.Microsoft.com
- Undisclosed or hidden sender's email address.
- A warning, urgency, problem, etc. "Response Required" "Account Locked" "Compromised Account"
- Enticement to open an attachment or click on a link.
- Ask you to verify your information.
- Any email that asks you to enter any information is MALWARE
- Do not call the phone # within the email. Look up the company.

In closing…..

- Please do not save anything on the local computer. Use your “H” drive, dept drives, or OneDrive.
- Please don’t move your computer or any IS equipment.
- Please submit a ticket and avoid calling IS staff directly.
- For the status of your ticket, please check the portal or reply to the automated email.
- Incident = something broken / security event
- Request = something new/different
- Don’t click any links or open any attachments unless you're positive they're legitimate. When in doubt, call or contact IS.
- Pay attention to emails from
  - SJGH-IS ALERTS-SM
  - SJGH-IS-CYBERSECURITY