RobbLAW

IT Security &
Compliance Consulting

Protection Frameworks

National Institute of Technology Standards (NIST) Cybersecurity Framework (CSF)

- Provides a high-level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes
- Very risk based and flexible
- Suggestive, not prescriptive
- Focus on Five Areas: (**IPDRR**)
    - **Identify**
    - **Protect**
    - **Detect**
    - **Respond**
    - **Recover**

Health Information Trust Alliance (HITRUST)

- Compliance based and inflexible
- Prescriptive, not suggestive
- Can be certified in compliance

Health Information and Management Systems Society (HIMSS)

Each level represents progressive adoption of an Electronic Medical Record (EMR) system that is in use by a healthcare organization:

- **Level 0 = No ancillaries installed or used**
    - The organization has not installed the three key ancillary department systems:
        - Laboratory
        - Pharmacy
        - Radiology
- **Level 1 = Ancillaries used; PACS; Digital Non-DICOM Image Management**
    - All three major ancillary clinical systems are installed.
    - A full complement of radiology and cardiology PACS systems provides medical images to physicians via an intranet and displaces all film-based images. Patient-centric storage of non-DICOM images is also available.
- **Level 2 = CDR; Internal Interoperability; Basic Security**

- Major ancillary clinical systems are enabled with internal interoperability feeding data to a single Clinical Data Repository ("CDR") or fully integrated data stores that provide seamless clinician access from a single user interface for reviewing all orders, results, and radiology and cardiology images.
- The CDR or data stores contain a controlled medical vocabulary. Order verification is supported by a Clinical Decision Support ("CDS") rules engine for rudimentary conflict checking.
- Information from document imaging systems may be linked to the CDR.
- Basic security policies and capabilities addressing physical access, acceptable use, mobile security, encryption, antivirus and anti-malware, and data destruction are in place.

- **Level 3 = Nursing and Allied Health Documentation; eMAR; RBAC Security**
  - 50% of nursing and allied health documentation (e.g., vital signs, flowsheets, nursing notes, nursing tasks, care plans) is implemented and integrated with the CDR. Capability must be in use in the Emergency Department ("ED"), but ED is excluded from the 50% rule.
  - The Electronic Medication Administration Record application ("eMAR") is implemented.
  - Role-Based Access Control ("RBAC") is implemented.
- **Level 4 = CPOE with CDS; Nursing and Allied Health Documentation; Basic Business Continuity**
  - 50% of all medical orders are placed using Computerized Practitioner Order Entry ("CPOE") by any clinician licensed to create orders. CPOE is supported by a CDS rules engine for rudimentary conflict checking, and orders are added to the nursing and CDR environment. CPOE is in use in the ED, but not counted in the 50% rule.
  - Nursing and allied health documentation has reached at least 90%, excluding the ED.
  - Where publicly available, clinicians have access to a national or regional patient database to support decision making (e.g., medications, images, immunizations, lab results, etc.).
  - During Electronic Medical Records ("EMR") downtimes, clinicians have access to patient allergies, problem/diagnosis list, medications, and lab results.
  - Network Intrusion Detection System ("IDS") is in place to detect possible network intrusions.

    - Nurses are supported by a second level of CDS capabilities related to evidence-based medicine protocols (e.g., risk assessment scores trigger recommended nursing tasks).
- **Level 5 = Physician Documentation using structured templates; Intrusion/Device Protection**
    - Full physician documentation (e.g., progress notes, consult notes, discharge summaries, problem/diagnosis list, etc.) with structured templates and discrete data is implemented for at least 50% of the hospital. Capability must be in use in the ED, but ED is excluded from the 50% rule.
    - Hospital can track and report on the timeliness of nurse order and task completion.
    - Intrusion Prevention System ("IPS") is in use to not only detect possible intrusions, but also prevent intrusions.
    - Hospital-owned portable devices are recognized and properly authorized to operate on the network, and can be wiped remotely if lost or stolen.
- **Level 6 = Technology enabled medication, blood products, and human milk administration; Risk reporting**
    - Technology is used to achieve a closed-loop process for administering medications, blood products, and human milk, and for blood specimen collection and tracking. These closed-loop processes are fully implemented in 50% of the hospital. Capability must be in use in the ED, but ED is excluded from the 50% rule.
    - The eMAR and technology in use are implemented and integrated with CPOE, pharmacy, and laboratory systems to maximize safe point-of-care processes and results.
    - A more advanced level of CDS provides for the "five rights" of medication administration and other "rights" for blood product, and human milk administrations and blood specimen processing.
    - At least one example of a more advanced level of CDS provides guidance triggered by physician documentation related to protocols and outcomes in the form of variance and compliance alerts (e.g., VTE risk assessment triggers the appropriate VTE protocol recommendation).
    - Mobile and portable device security policy and practices are applied to user-owned devices. Hospital conducts annual security risk assessments and report is provided to a governing authority for action.
- **Level 7 = Complete EMR; External HIE; Data Analytics, Governance, Disaster Recovery, and Security; Data Warehousing**

- The hospital no longer uses paper charts to deliver and manage patient care and has a mixture of discrete data, document images, and medical images within its EMR environment.
- Data warehousing is being used to analyze patterns of clinical data to improve quality of care, patient safety, and care delivery efficiency.
- Clinical information can be readily shared via standardized electronic transactions (i.e., CCD) with all entities that are authorized to treat the patient, or a health information exchange (i.e., other non-associated hospitals, outpatient clinics, sub-acute environments, employers, payers, and patients in a data sharing environment).
- The hospital demonstrates summary data continuity for all hospital services (e.g., inpatient, outpatient, ED, and with any owned or managed outpatient clinics).
- Physician documentation and CPOE has reached 90% (excluding the ED), and the closed-loop processes have reached 95% (excluding the ED).

American Association of CPAs

- Service Organization Controls (**SOC**) Reports
  - **Report 1** = Financial Controls
  - **Report 2** = Security Controls
  - **Type I** = Description of controls in place and opinion on effectiveness
  - **Type II** = Type I report and includes actual testing to ensure established controls accomplish what they were designed for