

# SHA Online Compliance and Regulatory Training

With Code and HIPAA Attestations



*Trusted to deliver exceptional compassionate care close to home*

Per Federal regulations, all employees, contractors and agents working with Summit Healthcare must be trained in compliance and regulatory information. We also include risk management and HIPAA privacy and security elements. Individuals and entities must agree to review and comply with Summit policies, specifically the *Code of Conduct and Ethics* and the *Workforce Member HIPAA and Confidentiality Agreement*.

(Source: CMS, Deficit Reduction Act, HIPAA)

Welcome to our organization. Staff are here to assist you if needed.

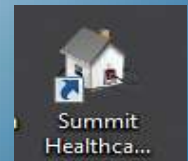
To reach us call:

- Professional Development at 928-537-6368
- Human Resources at 928-537-6520
- Compliance at 928-537-6510
- Risk Management at 928-537-6817
- HIPAA Privacy at 928-537-6939
- HIPAA Security at 928-537-6389

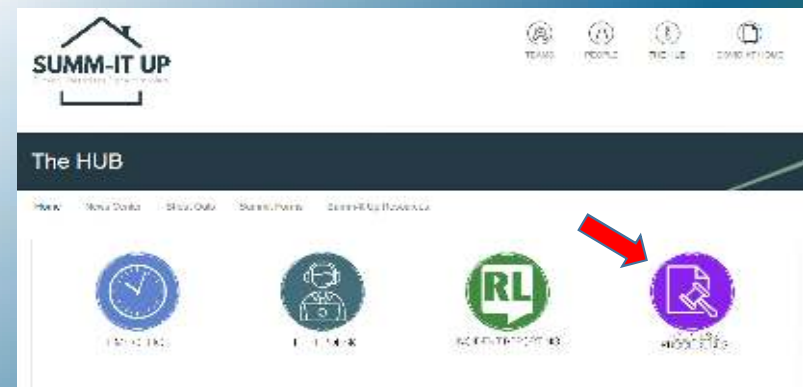
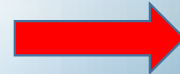


# Policies and Procedures

Summit Healthcare policies and procedures can be accessed from any desktop computer using the hospital intranet icon. If you do not have direct access, reach out to a Summit employee or contact the Compliance staff for assistance.



If you have access to the Summ-it Up intranet, select The Hub and click the purple Policy and Procedure box.





## Compliance

- Prevent, detect and correct conduct or behavior which is not compliant with laws and regulations, and promote an ethical culture.
- Implement Summit Healthcare Code of Conduct and Ethics, and the 7 Elements of a Compliance Program.



## Risk Management

- Assess risk to the entire organization
- Identify, evaluate and mitigate injury to patients, staff and the organization (e.g. strategic, fiscal, legal, etc.)
- Domains: operational, Financial, Human Capital, Strategic, Legal & Regulatory, Technology



## Privacy/Security

- Safeguard patient privacy, protected health information and confidentiality in compliance with federal and state law.
- Ensure the integrity, accuracy and availability of medical records and maintain them in accordance with federal and state privacy and security laws.

# Submitting Incident Reports

Summit Healthcare utilizes a web based incident reporting and feedback system. If you encounter an incident, it is your duty to report it to a Summit Manager or Director. If you have access to Summ-It Up, you can enter reports directly into the RL system.

You may also report to:

David Murray, CCPRO (928) 537-6830

Laura Nicks, Compliance Manager, (928) 537-6510

Natalie Roehlk, Privacy Officer, (928) 537-6939

Mary De Los Reyes, Risk Management, (928) 537-6817

Jay Larson, Security Officer, (928) 537-6389



Reporting allows for early investigation of events that have or may have caused harm to patients, staff, students, or visitors. Compliance, risk and privacy or security concerns are reported via the RL system. Events are trended and utilized to improve quality of care and services.



# Summit Healthcare Association's Compliance Program

## What is the goal?

To be compliant with (follow) federal and state legislation and regulations.

## What does it do?

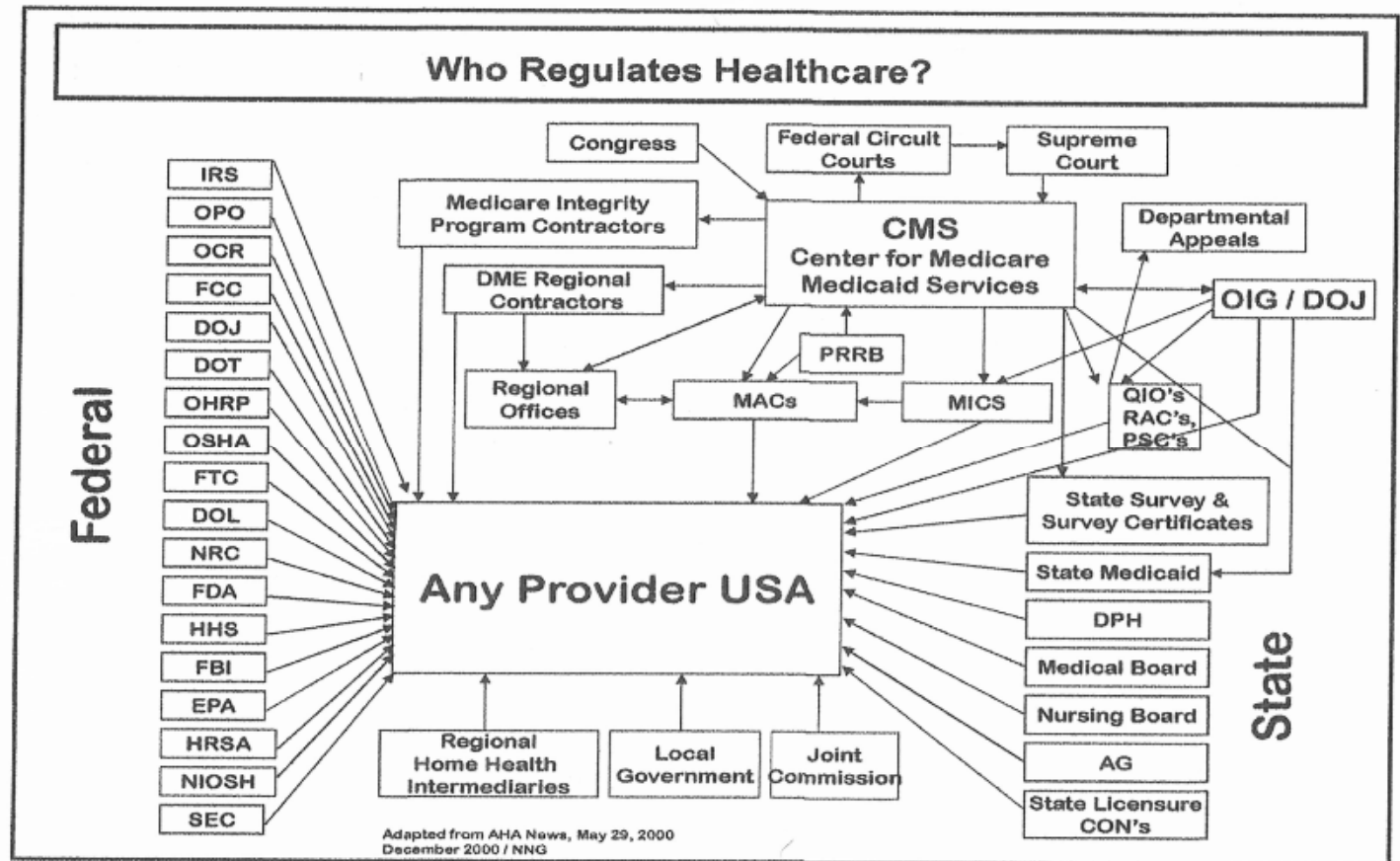
Checks (validates) to see the 'right thing' is done.

- Why is it Important? The Compliance Program supports our Mission, Vision and Values and safeguards against misconduct.
- What is our Mantra? "The Right Way Every Day" is what we strive for.
- Is there a Committee? Yes. The Enterprise Compliance and Risk Management Committee focuses on all types of risk.
- Who is Responsible? Everyone contributes to a culture of compliance.



# Regulation and Legislation

Healthcare is one of the most regulated industries in the country and subject to a host of different agencies. The majority of Summit's reimbursement comes from federal and state funded insurance companies, namely CMS and our State Medicaid program AHCCCS. To participate in these programs, we must be compliant with their laws and regulations.



# Deficit Reduction Act of 2005

Summit Healthcare Association's policy AW1084, "Code of Conduct and Ethics," provides guidance on the standards of ethical business and care practices which direct our organization. **All** workforce members must abide by our Code of Conduct and our Policies and Procedures. The primary elements include:

- Element 1: Quality of Care
- Element 2: Compliance with Laws and Regulations
- Element 3: Work Place Integrity
- Element 4: Billing, Coding, and Records Integrity
- Element 5: Protection and Use of Information, Property, and Assets
- Element 6: Conflicts of Interest
- Element 7: Non-Retaliation and Duty to Report
- Element 8: Compliance Responsibilities

The policy is attached at the end of the slide deck for your review.





# The False Claims Act (“FCA”)

The FCA was enacted in 1863 during the Civil War to combat fraud by companies that sold supplies to the Union Army, such as selling crates filled with sawdust instead of weapons. This law adopted a *qui tam* provision, which allowed private citizens, called “relators” to file suit on the government’s behalf against those defrauding the government. Relators were entitled to 50% of the amount recovered from their cases. Relators are more commonly known as “whistleblowers.”

- In 1943 Congress amended the FCA, drastically reducing the Relators’ recovery and prohibiting *qui tam* lawsuits if the government already had the evidence or information in hand. President Reagan revised the FCA again in 1986, increasing the whistleblower reward to 15-30% of the recovery plus attorneys fees. Additional amendments to the FCA were made in 2009 and 2010.
- The FCA contains strong whistleblower protections and prohibits retaliation against whistleblowers, including being “discharged, demoted, suspended, threatened, harassed, or in any other manner discriminated against in the terms and conditions of employment.” 31 U.S.C. § 3730(h)(1).
- In addition to the federal FCA, the State of Arizona has its own anti-fraud laws.
- These laws include civil and criminal penalties for knowingly submitting false claims, and have a large role in preventing fraud, waste and abuse in federal health care programs.



# Examples of False Claims and Duty to Report

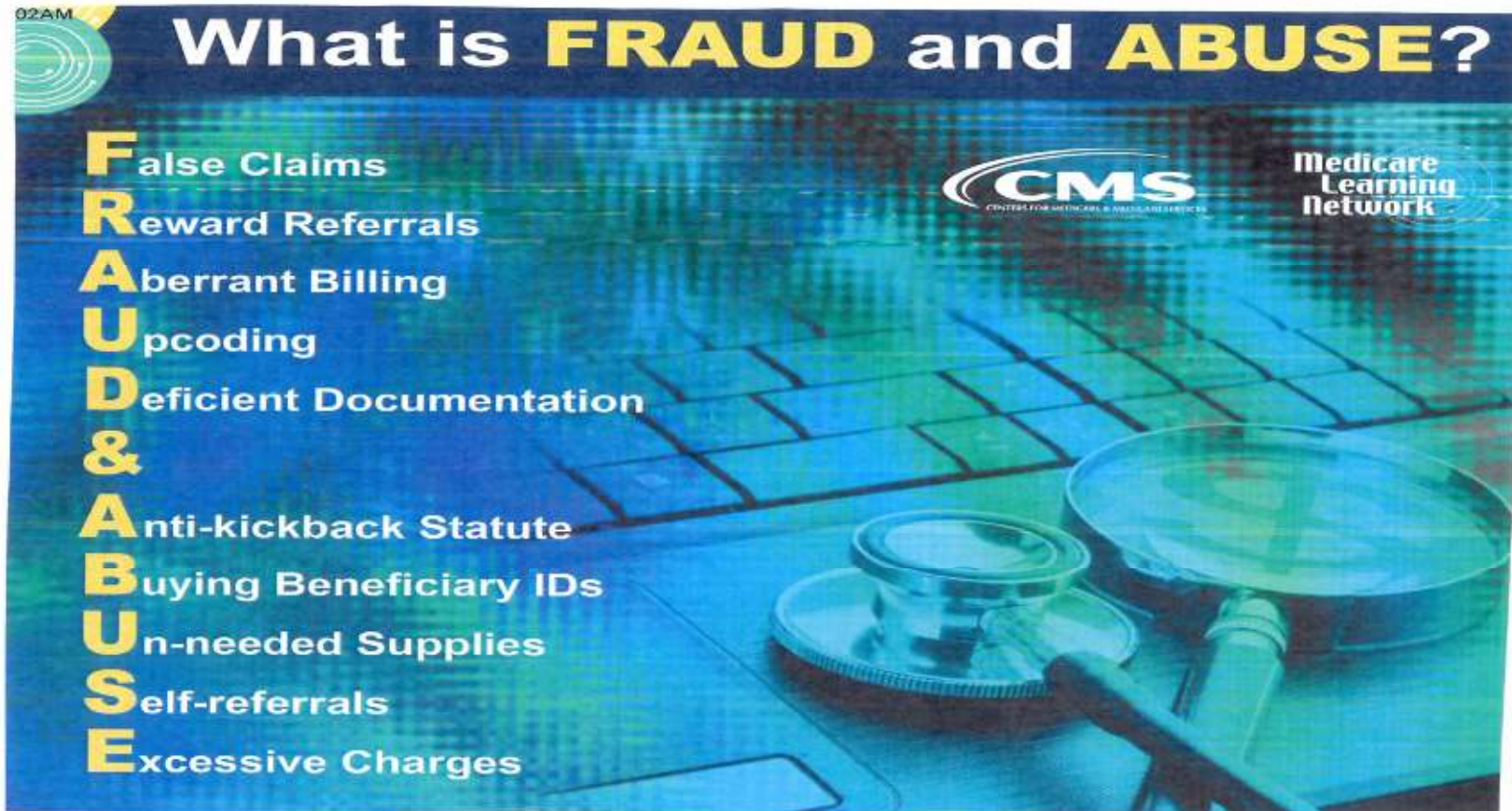
One of the primary purposes of false claims laws is to combat fraud and abuse in government health care programs, such as Medicare, Medicaid, TriCare and VA programs. Examples of false claims include:

- Billing for a procedure not performed or services not provided
- Falsifying information in the medical record or submitting false records of any kind
- Billing for services not medically necessary (or documentation does not support services provided)
- Billing for the incorrect level of services (miscoded)
- Billing for services covered under another claim (duplicate billing, etc.)
- Retaining payment when it is not rightfully yours to keep; this is a “reverse” false claim
- Violation of another law which causes a claim to be invalid or “tainted”, such as illegal relationships between providers involving kick-backs

If you observe behavior or actions which could lead to a false claim, you have a duty to report your concern to a Summit Manager, Director or Administrator. Retaliation for reporting in good faith is strictly prohibited. Reference policies: AW1175 “Non-Retaliation Policy” and AW1433 “False Claims Laws: Federal and State of Arizona”



# CMS Examples of Fraud and Abuse



02AM

## What is **FRAUD** and **ABUSE**?

**F**alse Claims  
**R**eward Referrals  
**A**berrant Billing  
**U**pcoding  
**D**eficient Documentation  
**&**  
**A**nti-kickback Statute  
**B**uying Beneficiary IDs  
**U**n-needed Supplies  
**S**elf-referrals  
**E**xcessive Charges

**CMS**  
CENTERS FOR MEDICARE & MEDICAID SERVICES

Medicare Learning Network

# Federal Government Enforcement

**“If you think  
compliance is  
expensive –  
try non-compliance.”**

*Former U.S. Deputy Attorney General Paul McNulty*

- The consequences of non-compliance can be devastating to organizations & individuals.
- Fines: treble (three times) the amount of the false claim
- Penalties / Loss of License
- Sanctions: Not allowed to participate in federal programs (exclusion)
- Criminal: prosecution / jail time
- Integrity Agreements (5 year improvement & audit plan)



# The State of Arizona Enforcement

Arizona has an active enforcement group called the Medicaid Fraud Control Unit which focuses on the AHCCCS (Medicaid) Program.



For more information on the MFCU, visit their website at:  
<https://www.azag.gov/seniors/senior-abuse/mfcu>

To submit a report:  
2005 N Central Ave  
Phoenix, Arizona 85004  
602.542.3881  
602.364.0411 (fax)



# 7 Elements of Compliance Programs



The health care industry shall operationalize the 7 Elements of a Compliance Program to protect from fraud and abuse, and facilitate an ethical and law-abiding culture.

*\*Source: DHHS Office of Inspector General*

The purpose of a Compliance Program:

**Prevent, Detect and Correct**

conduct or behavior which is not compliant with laws and regulations, and promote an ethical culture.

*\*Source: U.S. Federal Sentencing Guidelines*

Applicable to all industries that accept federal money.

## 7 Elements: #1

### **Written Policies and Procedures (P & Ps); Standards of Conduct**

P & Ps address regulatory requirements and provide guidance and direction. Indidge is our web-based repository for P & P.

The *Summit Healthcare Association Code of Conduct and Ethics* is a cornerstone document to guide day to day operations and conduct (behaviors and habits). It is a summary of principles to which we are committed.



## 7 Elements: #2

### **Compliance Structure: Officer, Committee, Governing Board**

- David Murray – Chief Compliance, Privacy and Risk Management Officer; Ext. 6556
- Laura Nicks – Compliance Manager; Ext. 6510
- Natalie Roehlk – HIPAA Privacy Officer; Ext. 6939
- Jay Larson – HIPAA Security Officer; Ext: 6389
- Mary De Los Reyes – Director of Risk Management; Ext. 6817
- Enterprise Compliance & Risk Management Committee
- Summit Healthcare Association Governing Board





## 7 Elements: #3

### **Education and Training**

- Goal: Understand and practice compliance principles as you go about your day to day work. Get to know the laws, regulations and Summit policies.
- Compliance and regulatory training is required upon hire or on-boarding, and in most cases annually thereafter.
- Web-based learning modules are assigned.
- Job-specific training is provided by your department leaders.



## 7 Elements: #4

### **Lines of Communication & Reporting**

- It's your duty to report compliance concerns, as described in Summit's Code of Conduct & Ethics. There are multiple ways and methods. The reporter may choose any of the following:
  - Report to a Supervisor/Manager/Director
  - Contact the Compliance Staff or an Administrator
  - Call the 24/7 Compliance Hotline 1-844-965-3490. You may report anonymously or provide your name
  - You may also report directly to a regulatory agency
- Non-Retaliation Policy AW1175 – Summit supports and protects individuals (relators or whistleblowers) who report compliance concerns in good faith. If you feel you are being treated unfairly as a result, inform any of the contacts above.



## 7 Elements: #5

### Enforcement Standards

- Summit's Goal: Be fair and consistent in the methods used to educate, counsel and/or discipline staff when there is wrong-doing.
- We have adopted 'Just Culture' behavior-based algorithms to guide our investigations and actions. There are three behavior pathways.
  1. Human Error – example: a one time mistake resulting in re-training and coaching
  2. At-Risk Behavior – example: same mistake done repeatedly resulting in a performance improvement plan
  3. Reckless Behavior – example: a serious breach of duty has occurred resulting in disciplinary action

Refer to HR policies for more information.



## 7 Elements: #6

### **Auditing and Monitoring; Identification of Risks**

- Need to validate the right thing *is* done and not assume we are in compliance with rules and regulations.
- Key workflows and processes (internal controls) are to be monitored, audited and reported to prevent errors and mistakes.
- Trust *and* Verify is the guiding principle.
- Compliance risks are continually identified and prioritized throughout the year and via an annual Work Plan.
- Know what is audited or monitored within in your department.
- Contractors and Vendors: Know what may be audited or monitored within your scope of work such as contractual services, deliverables, etc.



## 7 Elements: #7

### **Summit responds to reports; develops Corrective Action Plan (CAP)**

- Don't ignore mistakes; act on them; investigate
- Apply Root Cause Analysis (RCA) methodology until the source of the problem is identified.
- Develop a robust CAP to ensure the problem doesn't happen again. This may include a monitoring plan to validate compliance with the CAP.
- With some offenses, a self-report to a regulatory or enforcement agency may be necessary.



# Compliance, Your Role, Summit Goals

- Support a 'Culture of Compliance' whereby Summit conducts business with integrity and honesty while providing quality care.
- Report potential problems and concerns right away to minimize risk.
- Ask questions, seek clarification. We are your resource and here to help with understanding the 'why' behind the 'what'.
- Research and know the laws and regulations that govern what you do.
- Share your best practices. We are stronger, together.
- Compliance does not happen by accident. It is purposeful and intertwined in our day to day operations.



# Patient Rights

Patients have a right to care, treatment and services that:

- Protect their dignity and respect their values
- Support their ability to make choices
- Involve them in their care and treatment decisions
- Protect their civil rights

Every caregiver is responsible to act on behalf of the patient/family by advocating for safe, quality healthcare and treatment.

The right to: Have information about the facility and its policies

The right to: Confidentiality

The right to: Have access to translators

The right to: Safety

The right to: Non-discrimination

The right to: Have access to emergency services

The right to: Informed consent

The right to: Complaint resolution

The right to: Know names and qualifications of the people responsible for their care

# Risk Management

Summit Healthcare's Risk Management Program is a component of the Compliance Department. Its purpose is to identify, analyze, prioritize and manage risks to the organization and to patient safety. These risk domains include:

- Operational
- Financial
- Human Capital
- Strategic
- Legal and Regulatory
- Domain and Technology

Risks may be internal (often preventable risks which are usually addressed via policies and procedures), external (which arise from outside and are often beyond organizational control) and strategic (voluntary risk acceptance tolerance, which must be managed).

Summit's approach to risk depends on the type of risk identified, which domain it falls in, and is dependent upon the facts of the individual situation.





# Risk Management – Domain 1: Operational

Operational risks may result from failed internal processes or lack of compliance with processes affecting business or clinical operations.

- Documentation standards – follow them
  - Policies and procedures, document integrity, accurate medical records, etc.
- Adverse event management
  - Medication/medical/surgical errors, adverse events, etc., are reported promptly
- Patient and staff safety
  - Infection prevention, injury, care coordination, etc., “do no harm” – to our patients and/or to ourselves
- Professional liability and accountability for our work
  - Auditing & monitoring, transparency, disclosure & apology, etc.
- Effective chain of command
  - Chain of command reviews, non-retaliation policy



## Risk Management Domain 2: Financial

Financial risks are risks associated with potential financial losses across the organization.

- Charge capture, billing and collection – ensure accuracy
- Salary and wage issues – time cards, contractual requirements
- Legal actions against the association or its employee – notify Risk promptly
- Insurance contracts – know policies
- Capital structure – meet requirements for capital funding
- Capital equipment – plan for replacement, ensure maintenance

# Risk Management Domain 3: Human Capital

Human capital refers to those individuals who work at Summit Healthcare. Risks occur within all aspects of the workforce — recruitment, retention, staffing, termination and on-the-job injuries.

- Culture
- Morale
- Hiring practices
- Benefits
- Policies
  - Sexual harassment, discrimination, diversity, competency, disruptive behavior, substance use, etc.



## Risk Management Domain 4: Strategic

Strategic risks are those risks associated with the focus, mission and vision of Summit Healthcare. The overall direction of change Summit undergoes is determined by the Summit Healthcare Association Governing Board.

- Business ventures
- Contract administration
- Media relations
- Professional alignment (telemedicine, affiliations, etc.)
- Conflicts of interest

All must comply with regulations to ensure protection of Summits' Not-for-Profit status as well as protection from running afoul of those regulations.



# Risk Management Domain 5: Legal & Regulatory

Legal and regulatory risks largely revolve around management and professional liability and adherence to statutory mandates.

- Fraud and abuse
- Malpractice
- Claims (many claims relate to delays in care/treatment)
- Medicare Conditions of Participation
- Federal, state and local requirements
  - Federal – CMS, HIPAA, HHS Office of the Inspector General, DOJ, etc.
  - State – Arizona Department of Health Services, Medical Board, Nursing Board, etc.
  - Local – Navajo County Department of Environmental Health, Public Health, Indian Health Services at Whiteriver, Navajo Nation and Ft. Apache reservations, etc.



# Risk Management Domain 6: Technology

Technology domain risks include hardware, software, tools, techniques and methods used in clinical diagnosis and treatment.

Remember that in order for treatment to be provided, the physical location where care is rendered must be safe and hazard-free.

- Electronic health records and systems
- Information storage and retrieval
- Electronic equipment –
  - Transmission between systems
  - Reliance on systems v. manual processes
- Facility management and plant upkeep
- Emergency management equipment and processes



# Risk Management

The feedback section of the Safety Management System is used for documenting patient complaints and concerns.

These entries are received and followed up by the Patient Advocate in the Quality Department.

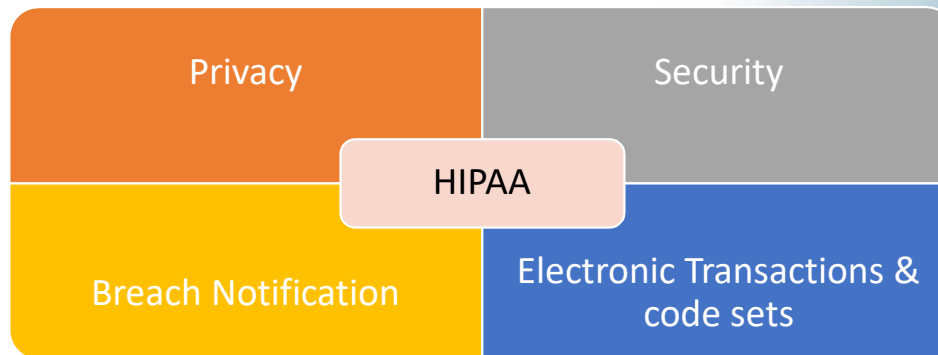
The Patient Advocate can also be contacted by calling X6746.

*If you have a concern or incident with/about a patient, contact the Director of Risk Management directly at x: 6817.*



# HIPAA (Health Information Portability and Accountability Act)

- **HIPAA** is an acronym for the **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct of 1996.
- HIPAA has four key sections:





# The Goal of the HIPAA Privacy and Security Programs

- To protect confidential information from improper acquisition, access, use, or disclosure and ensure its security, integrity and availability.
- To safeguard patient privacy, protected health information and confidentiality in accordance with the law.
- To provide a resource to staff to assist in navigating federal and state privacy, confidentiality and information security laws.
- To ensure complete and accurate medical records are maintained in accordance with federal and state privacy and security laws, regulations and policies.



# What is HIPAA?

A set of regulations intended to protect the privacy and security of a patient's health information.

- The *HIPAA Privacy Rule* became effective April 14, 2003. This Rule sets national standards for the protection of individually identifiable health information by three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically.
- The *HIPAA Security Rule* became effective April 20, 2005. This Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information.
- The *HIPAA Enforcement Rule* went into effect March 16, 2006, to provide enforcement mechanisms for HIPAA standards.
- The *HITECH Act of 2009* expanded the responsibilities of business associates under the HIPAA Security Rule, and
- The *Omnibus Rule*, (effective September 23, 2013) meant to strengthen the privacy and security protections for health information established under HIPAA.
- Additional updates to HIPAA are anticipated in 2023.



# HIPAA - Key Terms

- *Individually Identifiable Health Information* is a subset of health information created or received by Summit Healthcare Association, and:
  - Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
  - That identifies the individual; or
  - With respect to which there is a reasonable basis to believe the information can be used to identify the individual.



# HIPAA - Key Terms

- *Protected Health Information* (“PHI”) means Individually Identifiable Health Information:
  - Transmitted by electronic media;
  - Maintained in electronic media; or
  - Transmitted or maintained in any other form or medium.
- *Electronic Protected Health Information* (“ePHI”) means PHI transmitted by, or maintained in, electronic media.
- Where does PHI live?
  - Within the facility (paper and computers)
  - Verbal or written information
  - Information shared with other health care providers
  - Payers or third parties



# HIPAA - Key Terms

*Examples of PHI Identifiers* are:

- Names, street addresses, city, county, precinct, zip code and their equivalent geocodes,
- All elements of dates (except year) for dates directly related to an individual (e.g., birth date, admission and discharge dates, etc.),
- Phone numbers, fax numbers, email addresses,
- Social Security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate/license numbers,
- Vehicle identifiers and serial numbers, including license plate numbers,
- Device identifiers and serial numbers, Web Universal Resource Locators (URLs), Internet Protocol (IP) address numbers,
- Biometric identifiers, including finger and voice prints,
- Full face photographic images and any comparable images, and
- Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data)



# Your Role in HIPAA

- Only access charts of patients for whom you are directly involved with their care, and use only the minimum amount of protected health information necessary to do your job.
- Never access your own chart or those of immediate family members, friends or loved ones. All requests for access must follow Health Information Management (HIM) procedures, including submitting a Release of Information form.
- Ask your co-worker to treat family members, register patients, claims, etc.
- Never gossip about patients (many HIPAA violations stem from overhearing verbal discussions). Do not discuss patient information within anyone other than those directly involved with the patient's care.
- Respect confidential information - All information that identifies any individual is considered confidential.
- Be sure that patient information is ONLY given or disclosed to others who have a legal right to it.
- Follow all Summit Healthcare policies and procedures.
- ALWAYS report any suspected HIPAA incidents or privacy violations. Retaliation for filing a good faith complaint is strictly prohibited. If you see something, say something -
  - RL system via The Hub on SUMM-IT Up ([https://summitcommunity.net/summit\\_hub](https://summitcommunity.net/summit_hub))
  - Compliance Hotline, at 1-844-965-3490
  - To the HIPAA Privacy Officer (Natalie Roehlk, x: 6939) or Security Officer (Jay Larson, x: 6389) directly



# HIPAA Violations

- Legal Consequences:

- Civil or Criminal penalties

Civil Penalties 2022

Penalty Tier	Culpability Definition	Minimum Penalty per Violation	Maximum Penalty per Violation	Annual Penalty Limit
Tier 1	Lack of knowledge	\$127	\$63,973	\$1,919,173
Tier 2	Reasonable Cause, Not Willful Neglect	\$1280	\$63,973	\$1,919,173
Tier 3	Willful neglect, corrected within 30 days	\$12,794	\$63,973	\$1,919,173
Tier 4	Willful neglect, not corrected within 30 days	\$63,973	\$1,919,173	\$1,919,173

- **Criminal:** Up to \$50,000 and One (1) year in prison
- **Knowingly releasing information:** Up to \$100,000 and 5 years in prison
- **Malicious Intent/Gaining access to Health Information under false pretenses:** Up to \$250,000 and 10 years in prison

- Fines **PLUS** imprisonment

- Professional Consequences:

- Disciplinary action by the State Boards (e.g., Board of Nursing, Board of Medicine, Board of Osteopathy, etc.) Certifications, Licenses, etc.
- See SHA Policies and Procedures (<http://Indidge.nrmc.org/GRC/HPM>)
- May result in termination of employment or contract at Summit Healthcare

- Failure to comply may also hurt the reputation of the facility, erode patient trust, put accreditation at risk and result in costly lawsuits.



# Patient Rights Under HIPAA

HIPAA guarantees Patient Rights. These rights are detailed in our Notice of Privacy Practices (NoPP). Generally:

- Right to privacy and confidentiality of their health information,
- Right of access to inspect and receive a copy of their medical record,
- The right to request amendments to their PHI, and request restrictions on their PHI,
- The right to receive an accounting of disclosures of their PHI,
- The right to request confidential communications,
- The right to designate a personal representative,
- The duties of Summit Healthcare,






# Patient Rights Under HIPAA

- A description of how Summit Healthcare may use, disclose and share their PHI,
- Types of uses and disclosures that require an authorization and the right of the individual to revoke the authorization,
- The right to a paper copy of the NoPP upon request,
- Right to request that information is not given out concerning their care to specific individuals, including the right to opt out of our patient directory (called NIP) so individuals their name not listed as being present in our facility other than for treatment, billing, etc.
- Right to request that individuals are not told of their presence in our facility,
- The right to lodge a complaint with Summit Healthcare or the Secretary of the U.S. Department of Health and Human Services (“HHS”) if they believe their rights have been violated,
- The name, or title, and telephone number of a person or office to contact for further information, and
- Effective date.





## HIPAA Security – Things to Remember

- Do not share passwords with others.
- Use multi-factor authentication when possible (2-3 pieces of information that identify the user).
- Avoid using the same password for multiple logins.
- Lock screen when leaving a device. (Try the Windows button  +L)
- Secure the emails being sent to other organizations; “[encrypt]” in subject line.
- Summit Healthcare IT staff will not ask for your username/password or require you to log into a link to preserve access to services.
- Any major account changes will be communicated via I.T. Help Desk announcements which can be verified on the Help Desk portal.



## HIPAA Security – What to do...

If...

You suspect you have received a phishing email,

You...

Do not open any links or attachments. Forward the email to I.T. Help Desk and report it.

If...

You have inadvertently clicked on something suspicious or provided information,

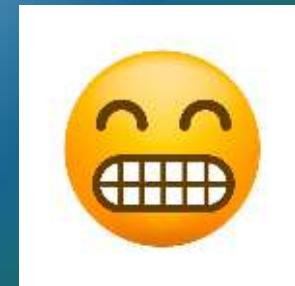
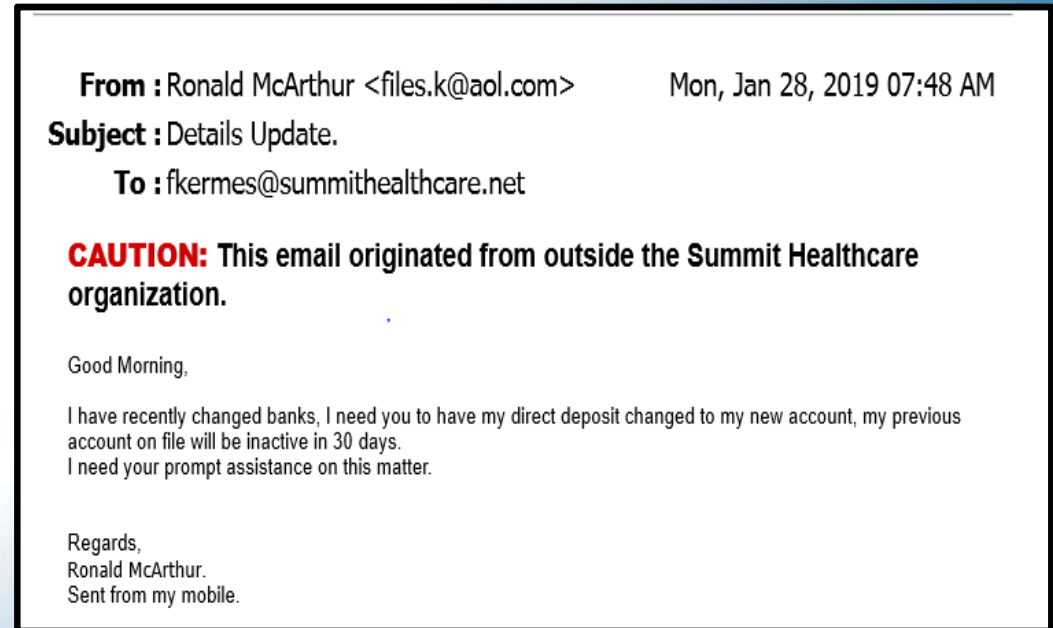
You...

Stop what you are doing right away, change your password immediately. Call the I.T. Help Desk and report the email address, what was clicked on, etc.



# HIPAA IT Security – Phishing Emails

- Check URL addresses. Many are altered or even hidden. Examples:  
[accounts@amazon.com](mailto:accounts@amazon.com) vs.  
[accounts@arnazon.com](mailto:accounts@arnazon.com)  
[name@summithealthcare.net](mailto:name@summithealthcare.net) vs.  
[name@summit-healthcare.net](mailto:name@summit-healthcare.net)
- Look for the “CAUTION” line, which indicates the email came from outside the organization and be alert.
- Ensure that information you are receiving or sending out have an [@summithealthcare.net](mailto:@summithealthcare.net) address, unless other precautions have been taken.
- If it sounds too good to be true or seems unfamiliar to you, it probably is phishing.
- Phishing attacks will often express that you must do these actions urgently.
- Phishing attacks are usually authoritative or threatening in nature.



# Advance Directives

Federal regulations require that all patients over the age of 18 be given the opportunity to formulate Advanced Directives.

Advance Directives include Living Wills and/or Durable Medical Power of Attorney. Advance Directives become relevant only when a patient becomes unable to make decisions for themselves.

If the patient has provided a copy of their Advance Directive it automatically pulls forward with each visit number and can be viewed in the most current medical record.

Patients can formulate or change their Advanced Directives at any time. If the patient/family wants assistance or additional information contact the Social Services department.

While Physician Orders for Life-Sustaining Treatment (POLST) forms do not replace Advance Directives they may complement the patients stated wishes. POLST forms are legally recognized in the state of Arizona.

If you have any questions, please contact the Social Services Department (Ext: 6364) or the Administrative Shift Coordinator (ASC) at (928) 537-6868.



Welcome to Summit Healthcare! We hope you have a positive experience with our organization. Thank you for sharing your professional expertise, care and compassion with the patients and families at Summit Healthcare.

To complete your training requirements, read the attached Summit Healthcare Association documents:

- Code of Conduct and Ethics
- Workforce Member HIPAA and Confidentiality Agreement

*You may proceed to the online documents and complete the attestation. Once submitted it will be directed to the appropriate recipient at Summit.*

