ST. CHARLES COUNTY AMBULANCE DISTRICT
REGULAR BOARD MEETING OVERVIEW
July 27th, 2023

I. CALL TO ORDER - The meeting will be held at District Headquarters and is scheduled to begin at 6:00 p.m.

II. PLEDGE OF ALLEGIANCE

III. PUBLIC COMMENTS

IV. AWARDS & ANNOUNCEMENTS

V. CONSENT AGENDA

A. Agenda Approval

Enclosed marked **# 1** in your packet is the proposed Board Agenda for Thursday, July 27th, 2023 for Board approval. *Management is requesting the following: move to approve the agenda as presented for Thursday, July 27th, 2023.*

B. Approval of Minutes

Enclosed marked **# 2** for Board approval is the Board Minutes from Thursday, July 13th, 2023. *Management is requesting the following: move to approve the Board Minutes from July 13th, 2023.*

VI. STAFF REPORTS

A. June Financial Report

Enclosed marked **# 3** for Board review is the June Financial Report, presented by Rick Rognan with Rognan and Associates.

B. 2023 Preliminary Tax Assessments

Enclosed marked **# 4** for Board review is the 2023 Preliminary Tax Assessment, presented by Rick Rognan with Rognan and Associates.

C. Senate Bill 190

Enclosed marked **# 5** for Board review is Proposed Senate Bill 190, presented by Rick Rognan with Rognan and Associates.

VII. OLD BUSINESS

A. Training Department Reorganization

Enclosed marked Item **# 6** for Board consider and review you will find supporting documentation related to proposed changes within the Training Division.

B. Insurance Broker RFP

Enclosed marked Item **#7** for Board consideration is memo with recommendation to stay with MMA Broker Services.

Management is requesting approval of awarding the competitive bid to MMA to provide brokerage services for Medical, Dental, Vision, Short-Term Disability, Long Term Disability, Life and Disability and FSA administration, not to exceed $60,000 per year, for a term of three years (36 months).

C. HIPAA Policies

Enclosed marked **#8** for Board consideration is several policies related to our HIPAA guidelines and practices.

1) 102-25a Privacy Officer
2) 102-25b Chief Information Security officer
3) 209-11 Security Incident Management
4) 209-14 Preserving Data and Electronically Stored Information
5) 209-16 Contingency Planning
6) 209-19 HIPAA Incident Management
7) 701-4 Photography Policy
8) 701-08 IAM and Password Policy

VIII. NEW BUSINESS

IX. ADJOURN PUBLIC PORTION

NOTICE OF MEETING

Public notice is hereby given that a public meeting of the Board of Directors of the St. Charles County Ambulance District will be held at the District's Offices, 2000 Salt River Road, in St. Peters, Missouri, on Thursday July 27th, 2023 at 6:00 p.m., to consider and act upon the matters on the following tentative agenda and such other matters as may be presented at the meeting and determined to be appropriate for discussion at that time.

6:00 P.M. –BOARD MEETING

I CALL TO ORDER

II PLEDGE OF ALLEGIANCE

III PUBLIC COMMENTS

IV AWARDS & ANNOUNCEMENTS
- A.

V CONSENT AGENDA
- A. July 27th, 2023 Agenda Approval
- B. July 13th, 2023 Minutes Approval

VI STAFF REPORTS
- A. June Financial Report
- B. 2023 Preliminary Tax Assessments
- C. Senate Bill 190

VII OLD BUSINESS
- A.

VIII NEW BUSINESS
- A. Training Department Reorganization
- B. Insurance Broker RFP
- C. HIPAA Policies
    1) 102-25a Privacy Officer
    2) 102-25b Chief Information Security officer
    3) 209-11 Security Incident Management
    4) 209-14 Preserving Data and Electronically Stored Information
    5) 209-16 Contingency Planning
    6) 209-19 HIPAA Incident Management
    7) 701-4 Photography Policy
    8) 701-xx IAM and Password Policy

IX ADJOURN PUBLIC PORTION

Kenny Biermann
Secretary of the Board of Directors

Date/Time Posted: 07.26.2023 @ 12 noon

NOTICE OF MEETING

Public notice is hereby given that a public meeting of the Board of Directors of the St. Charles County Ambulance District will be held at the District's Offices, 2000 Salt River Road in St. Peters, Missouri, on Thursday July 27th, 2023 at 6:00 p.m., to consider and act upon the matters on the following tentative agenda and such other matters as may be presented at the meeting and determined to be appropriate for discussion at that time.

I CALL TO ORDER – PUBLIC PORTION

II MOTION TO CLOSE PUBLIC MEETING – PUBLIC PORTION AND GO TO CLOSED SESSION Pursuant to: A. Attorney Client Sec.610.021 (1)RSMo (1986) B. Personnel Sec. 610.021(3&13) RSMo(1986)

III ADJOURNMENT - PUBLIC PORTION

Kenny Biermann
Secretary of the Board of Directors

Date/Time Posted: 07.26.2023 @ 12 noon

By:

ST. CHARLES COUNTY AMBULANCE DISTRICT
BOARD MEETING MINUTES
THURSDAY, July 13th 2023

#2

I. CALL TO ORDER

Ronald Reguly, called the meeting to order at headquarters at 6:00 p.m. In attendance were Sean Treece, Mark Johnson, John Whitworth, Ronald Reguly, Kenneth Biermann, and Teresa Reynolds.

II. PLEDGE OF ALLEGIANCE

III. PUBLIC COMMENTS

Mr. Arnie Diehnoff provided public comments.

IV. AWARDS AND ANNOUNCEMENTS

Chief Cope announced that SCCAD recently achieving the 2023 Mission Lifeline Gold Award from the American Heart Association.

Chuck Krueger received an Award of Recognition for recently earning his Master's Degree in Business Administration.

Employee Picnic moved to Sunday, September 17th

V. CONSENT AGENDA

A. Agenda Approval

Mark Johnson made a motion to approve the July 13th, 2023 agenda as presented, Kenny Biermann seconded; the motion carried 6 to 0.

B. Meeting Minute Approval

Mark Johnson made a motion to approve the Board Meeting Minutes from Thursday, June 22nd 2023. Kenny Biermann seconded; the motion carried 6 to 0.

VI. STAFF REPORTS

A. Call Volume & Revenue Report

Assistant Chief Dave Lewis provided the monthly call volume report for June and Director, Angie Dollens provided revenue report for June 2023. No Board Action.

B. Community Relations Q2 Report

Attached in the Board Packet is the Q2 Community Report from Director Gaines.

VII. OLD BUSINESS

No Old Business

VIII. NEW BUSINESS

A. Desktop Support Technician Job Description #102-22d

Mark Johnson made a motion to approve Desktop Support Technician Job Description #102-22d, Teresa Reynolds seconded; the motion carried 6 to 0.

B. Social Media Policy #701-7

Mark Johnson made a motion to approve Social Media Policy #701-7, Kenny Biermann seconded; the motion carried 6 to 0.

C. COVID Vaccination Policy #606-4

Teresa Reynolds made a motion to rescind COVID Vaccination Policy #606-4, requiring Covid-19 immunizations as a condition of employment, doing so effective immediately; however, this will not relieve students or employees of any vaccine requirement as a condition of participation in clinical activities or vaccination requirements as a pre-requisite to EMT or Paramedic Program application. John Whitworth seconded; the motion carried 6 to 0.

D. Clinic RFQ

At the end of May, the District published an RFP for employee clinic services which closed on July 1. Both BJC and SSM were directly solicited. Four responses were received, with Rezillient Health being considerably lower bid than all others.

Given the success of our pilot, employee satisfaction, and demonstrated cost savings, management is requesting approval to award the competitive bid to Rezillient Health, low bidder, to provide concierge primary care and urgent care clinic services to employees and their families in an amount not to exceed $18,000 per month (net of leased space offset).

Teresa Reynolds made a motion: Given the success of our pilot, employee satisfaction, and demonstrated cost savings, management is requesting approval to award the competitive bid to Rezillient Health, low bidder, to provide concierge primary care and urgent care clinic services to employees and their families in an amount not to exceed $18,000 per month (net of leased space offset). Mark Johnson seconded; the motion carried 6 to 0.

IX. ADJOURNMENT - PUBLIC PORTION

John Whitworth moved to adjourn the Board Meeting, Kenny Biermann seconded; roll call vote was taken; Ronald Reguly - yea, Teresa Reynolds - yea, Kenneth Biermann - yea, Sean Treece-yea, Mark Johnson-yea, John Whitworth – yea, the motion carried 6 to 0.

ST. CHARLES COUNTY AMBULANCE DISTRICT
BOARD MEETING MINUTES
THURSDAY, July 13th, 2023

NOTICE OF MEETING

I. CALL TO ORDER – PUBLIC PORTION

Teresa Reynolds called to order the Public Portion. In attendance were Ronald Reguly, Teresa Reynolds, Kenneth Biermann, Sean Treece, Mark Johnson, and John Whitworth.

II. MOTION TO SUSPEND MEETING – PUBLIC PORTION

Teresa Reynolds moved to suspend the open meeting and go into Closed Meeting-pursuant to A. Attorney Client Sec. 610.021(1) RSMo(1986) B. Personnel Sec. 610.021(3&13) RSMo(1986) Sean Treece seconded; roll call vote was taken.

Ronald Reguly - yea, Teresa Reynolds - yea, Kenneth Biermann - yea, Sean Treece-yea, Mark Johnson-yea, John Whitworth – yea, the motion carried 6 to 0.

III. ADJOURNMENT – PUBLIC PORTION

Teresa Reynolds moved to adjourn the Board Meeting; Kenny Biermann seconded; roll call vote was taken. Ronald Reguly - yea, Teresa Reynolds - yea, Kenneth Biermann - yea, Sean Treece-yea, Mark Johnson-yea, John Whitworth – yea, the motion carried 6 to 0.

Next Regular Board Meeting
July 27th, 2023

_____
Ronald Reguly, Chair

Submitted by Tammy Dixon

_____
Kenneth Biermann, Secretary/Treasurer

ST. CHARLES COUNTY AMBULANCE DISTRICT
PUBLIC HEARING NOTICE

#4

	1 POST B-O-E 07/01/2023 2023	2 POST B-O-E 08/26/2022 2022	3 $	4 %	P
Combined Real Estate, net of TIF:	11,057,933,061	9,142,486,478	1,915,446,583	20.95%	
Total Combined Real Estate, net of TIF	11,057,933,061	9,142,486,478	**1,915,446,583**	**20.95%**	
Combined Personal Property:	2,088,966,169	2,021,670,976	67,295,193	3.33%	
Total Combined Personal Property	2,088,966,169	2,021,670,976	**67,295,193**	**3.33%**	
Total Tax Assessments	13,146,899,230	11,164,157,454	**1,982,741,776**	**17.76%**	
NEW Construction	162,052,444	131,347,941	**30,704,503**	**23.38%**	
CPI	**6.50%**	**7.00%**	**-0.50%**	**-7.14%**	

ROGNAN & ASSOCIATES
Certified Public Accountants/International Consultants
616 Applecross Ct.
Saint Louis, MO 63021
Telephone (636) 391-9831
Fax (636) 391-9835
"Client Service Driven"
Website: Rognanandassociates.com

To all Districts:

SB 190 (eligible taxpayers - senior citizen residential real estate tax freeze) was signed by the governor on Thursday - July 6 - what happens next - and what are the implications to the Districts?

First, by state statute, SB 190 becomes law on August 28, 2023.

Second, the senior citizen residential real estate tax freeze commences when your county adopts an ordinance authorizing such credit - the bill reads as follows - "Any county authorized to impose a property tax may grant a property tax credit to eligible taxpayers residing in such county in an amount equal to the taxpayer's eligible credit amount, provided that: such county adopts an ordinance authorizing such credit."

Third, SB 190 defines an eligible taxpayer and "homestead" as follows - "**Eligible taxpayer**, a Missouri resident who:
(a) Is **eligible for Social Security retirement benefits**;
(b) Is an **owner of record of a homestead or has a legal or equitable interest in such property** as evidenced by a written instrument; and
(c)Is **liable for the payment of real property taxes on such homestead**; "Homestead", **real property actually occupied by an eligible taxpayer as the primary residence**. An **eligible taxpayer shall not claim more than one primary residence**."

Fourth, this means any residential property owner (**regardless of income or house value**) sixty-two (62) years or older. This also means, regardless of what transpires from that date forward said senior will pay no more in any given year thereafter - senior residential real estate tax freeze.

Fifth, the bill reads in such a manner that landlords sixty-two (62) years and older will attempt to qualify for this residential tax freeze. Cities and counties will be required to identify residential rental properties to ensure these landlords are not afforded such benefit. Future revisions to this bill should consider adopting a "residency requirement" similar to federal and state statutes. Such residency requirements should require the taxpayer occupy said primary residence six (6) months and one (1) day and be a "registered voter" from said primary residence.

Sixth, this bill will most likely be **legally challenged based on Hancock** concerns. The bill reads that the "Eligible credit amount, represents the difference between an eligible taxpayer's real property tax liability on such taxpayer's homestead for a given tax year, minus the real property tax liability on such homestead in the year that the taxpayer became an eligible taxpayer. A county granting an exemption pursuant to this section shall apply such exemption when calculating the eligible taxpayer's property tax liability for the tax year. The amount of the credit shall be noted on the statement of tax due sent to the eligible taxpayer by the county collector. For the purposes of calculating property tax levies pursuant to section 137.073, the total amount of credits authorized by a county pursuant to this section shall be considered tax revenue, as such term is defined in section 137.073, actually received by the county."

Lastly, since this applies only to new growth, taxing authorities need to reach out **annually** to the county and ascertain what percent of your residents qualify as seniors - sixty-two (62) or older. Please ensure when preparing the annual budget the estimated impact of SB 190 is discussed and taken into consideration when arriving at tax revenue.

Sincerely,

Rognan & Associates

Richard A. Rognan, CPA
Managing Partner

ST. CHARLES COUNTY AMBULANCE DISTRICT
POLICY AND PROCEDURE MANUAL

CHAPTER 100 Personnel Policies & Procedures
SECTION 02 Job Descriptions
TITLE **Division Chief, Clinical Practice & Standards**
NUMBER 102-63

DISTRIBUTION
All personnel.

PURPOSE
Responsible for the design, construction, and oversight of EMS clinical practice and continuing education standards. Additionally, oversees professional development and compliance for district clinicians, patient safety, and quality improvement/assurance programs for the district.

DESCRIPTION
A full-time, exempt, salaried employee who reports directly to the Deputy Chief-Medical Officer.

ESSENTIAL DUTIES AND RESPONSIBILITIES

1. Ensures the district incorporates and utilizes cutting-edge strategies and methods to improve all aspects of clinical practice, quality, and patient safety through the employment of national guidelines, clinical standards, and evidence-based practices, in partnership with national experts in quality and safety.

2. Directs clinical, operational, administrative, and strategic coordination for reporting and decision making that involves clinical practice, education, quality improvement and patient safety (QIPS).

3. Leads a team of training and compliance officers dedicated to the professional development and QIPS needs of the front-line paramedics. Mentors and provides leadership for clinical practice, quality improvement, and patient safety teams through coaching and assuring that members fulfill their roles on project teams.

4. Measures and evaluates data to determine impact of EMS provider performance. Develops metrics and tools to track, trend and report on system risk and patient safety processes for common opportunities for improvements to mitigate risk.

5. Works collaboratively with external (local, regional, and national) to promote, design, and implement improvements and innovations.

6. Undertakes quality initiatives, audits, risk management, and performance improvement plans as assigned.

7. Creates a supportive environment in the department with a sensitivity to the issues and needs of that area by regularly consulting with front-line EMS providers.

8. Assures application of a tracking method to monitor progress towards goals by collecting accurate, timely data to display the quality, cost, and service outcomes.

9. Communicates effectively improvements made to work teams, staff, managers, and administrators throughout the organization.

DRAFT

TITLE **Division Chief, Clinical Practice & Standards**
NUMBER 102-63

10. Completes special projects and performs other related duties according to delegated goals and parameters.
11. Develops a Clinical Practice Oversight Framework and updates it regularly, based on collaboration with Medical Director, Deputy Chief Medical Officer, and peer reviewed evidence-based medicine. Also develops clinical practice scorecards for individuals and team performance monitoring.
12. Designs, plans, implements, and monitors an effective Patient Safety Monitoring and Risk Management program to include a patient safety plan, with annual review, risk assessment and revision to meet organizational goals and changes in industry regulations/standards.
13. Directs the organization's Root Cause Analysis (RCA) activities. Reports aggregate RCA events, findings, and action plans to appropriate committees and leadership.
14. Reports to the Deputy Chief, Medical Officer on organizational compliance with Federal, State or Accrediting Body risk management and patient safety regulations and standards.
15. Designs, develops, implement a curriculum that meets the national registry and state of Missouri requirements for maintaining license and registration for SCCAD EMS providers.
16. Oversees IBSC curriculum programs for critical care and community paramedicine professional development/continuing education programs.
17. Provides oversight, mentoring, and organization-wide education on clinical practice, professional development, quality improvement, and patient safety.

Deleted: <#>Serves as the District's Health Insurance Portability and Accountability Act (HIPAA) Officer.¶

QUALIFICATIONS

To perform this job successfully, an individual must be able to perform each essential duty satisfactorily. The requirements listed below are representative of the knowledge, skill, and/or ability required. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

1. Education and Experience:
   a. Bachelor's degree in a related field of education or management from an accredited post-secondary institution is required. Master's Degree is preferred. The individual selected for the position who does not meet this qualification must acquire a Master's degree within four (4) years of his / her promotion date.
   b. Five (5) years previous experience as a licensed paramedic.
   c. Three (3) years' experience performing duties related to quality improvement.
   d. Previous education in adult learning theory, techniques and practices of adult education and skills training.

DRAFT

c. Previous experience in a supervisory role is preferred.

d. Three (3) years' experience performing duties related to the coordination, design, and development of EMS professional development and continuing education programs.

2. Certificates, Licenses, Registrations:
   a. Instructor certifications in BLS, ACLS, PHTLS or ITLS.

   b. Missouri EMT and Paramedic Instructor/Coordinator or an equivalent course (NAEMSE) is required.

QUALIFICATIONS (continued)

a. Valid Missouri or Illinois driver's license.

b. Valid Missouri EMT-Paramedic license. National Registry Paramedic certification may be accepted initially. Must obtain Missouri EMT-P license upon hire.

c. A formal critical care education program is required. The individual selected for the position who does not meet this qualification must acquire a critical care paramedic certification within four (4) years of promotion and maintain the certification while holding this position.

d. Just Culture Certification is required (must obtain within 1 year of promotion).

e. IHI Basic Certificate in Quality and Safety required (must obtain within 1 year). (The National Association of EMS Physicians Quality and Safety year-long course is preferred.)

f. NIMS/ICS 300 & 400 required (must obtain within 1 year of promotion).

g. Certified Ambulance Compliance Officer required (must obtain within 1 year of promotion).

3. Skills
   a. Analytical - Synthesizes complex or diverse information; Collects and researches data; Uses intuition and experience to complement data; Designs workflows and procedures.

   b. Problem Solving - Identifies and resolves problems in a timely manner; Gathers and analyzes information skillfully; Develops alternative solutions; Works well in-group problem solving situations; Uses reason even when dealing with emotional topics.

   c. Interpersonal Skills - Focuses on solving conflict, not blaming; Maintains confidentiality; Listens to others without interrupting; Keeps emotions under control; Remains open to others' ideas and tries new things.

   d. Oral Communication - Speaks clearly and persuasively in positive or negative situations; Listens and gets clarification; Responds well to questions; Demonstrates group presentation skills; Participates in meetings.

DRAFT

e. Written Communication - Writes clearly and informatively; Edits work for spelling and grammar; Varies writing style to meet needs; Presents numerical data effectively; Able to read and interpret written information; maintain accurate records and documentation.

f. Teamwork - Balances team and individual responsibilities; Exhibits objectivity and openness to others' views; Gives and welcomes feedback; Contributes to building a positive team spirit; Puts success of team above own interests; Able to build morale and group commitments to goals and objectives develops and maintains working relationship with fellow employees, other healthcare providers and general public.

h. Judgment - Displays willingness to make decisions; Exhibits sound and accurate judgment; Supports and explains reasoning for decisions; Includes appropriate people in decision-making process; Makes timely decisions; effectively manage time to achieve desired results and minimize stress; independently plan, organize, schedule and coordinate assigned projects and make decisions and judgments relating to assigned projects and other responsibilities.

QUALIFICATIONS (continued)

h. Professionalism - Approaches others in a tactful manner; Reacts well under pressure; Treats others with respect and consideration regardless of their status or position; Accepts responsibility for own actions; Follows through on commitments.

i. Language - Ability to read and comprehend instructions, correspondence, and memos. Ability to write correspondence, and effectively present information in one-on-one situation, small group situations and to third parties and employees of the organization.

j. Mathematical – Ability to add, subtract, multiply, and divide in all units of measure, using whole numbers, common fractions, and decimals. Ability to perform clinical calculations, compute rates, ratios, and percent and can draw and interpret bar graphs.

k. Computer - Knowledge of Database software; Internet software; Project Management software; Spreadsheet software and Word Processing software.

l. Other – Thorough understanding of EMS system, personnel management, supervision and employment law.

PHYSICAL DEMANDS

The physical demands described here are representative of those that must be met by an employee to successfully perform the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

DRAFT

While performing the duties of this job, the employee is frequently required to stand; walk; use hands to finger, handle, or feel; reach with hands and arms and stoop, kneel, crouch or crawl. This requirement includes, but is not limited to, an ability to perform the following: reaching above the shoulders and over 18", reaching below the shoulders and to the floor, pushing with maximum force of 37.5 pounds and pulling with a maximum force of 33.5 pounds. The employee is occasionally required to climb or balance.

The employee must regularly lift and/or move up to 100 pounds and frequently lift and/or move more than 100 pounds. This requirement includes, but is not limited to, an ability to perform the following: lifting floor to knuckle of 90 pounds and 12" to knuckle of 98 pounds, carrying 98 pounds while ascending/descending six (6) stairs. Specific vision abilities required by this job include close vision, distance vision, color vision, peripheral vision, depth perception and ability to adjust focus.

WORK ENVIRONMENT

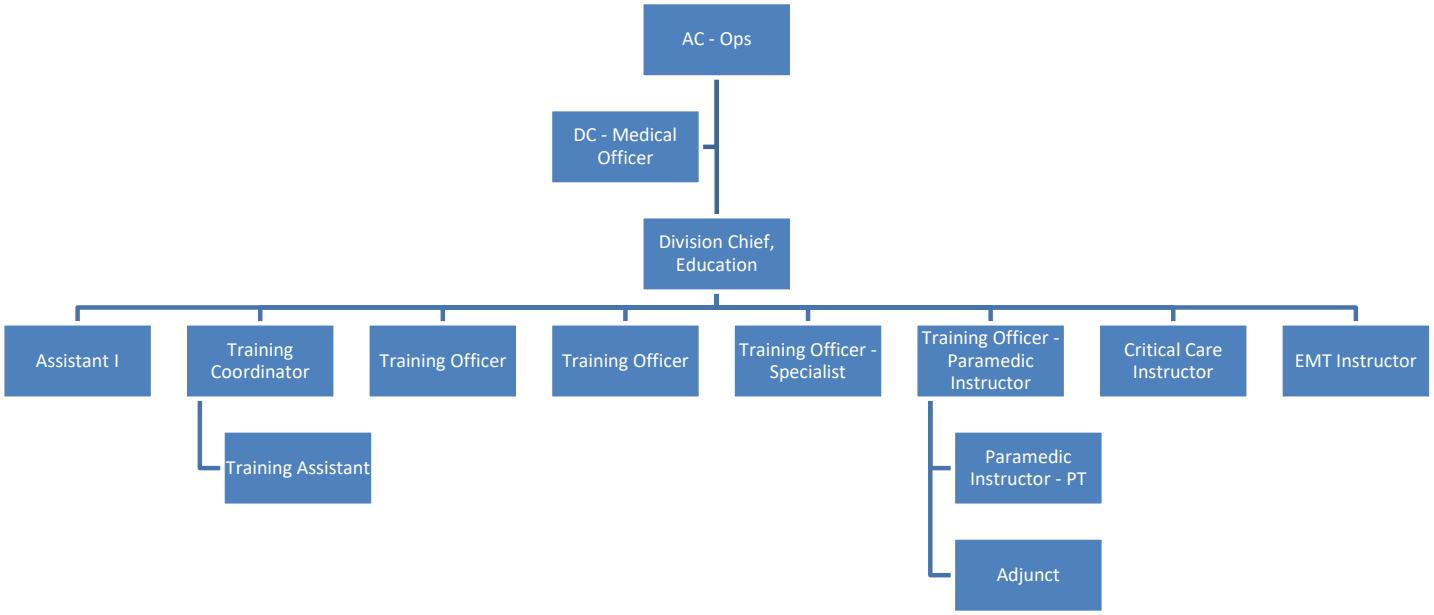
The work environment characteristics described here are representative of those an employee encounters while performing the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions. While performing the duties of this job, the employee is frequently exposed to moving mechanical parts and risk of electrical shock. The employee is occasionally exposed to wet and/or humid conditions; fumes or airborne particles; toxic or caustic chemicals; outside weather conditions; extreme cold; extreme heat and risk of radiation. The noise level in the work environment is usually moderate.

Adopted by Board of Directors:
Revised:

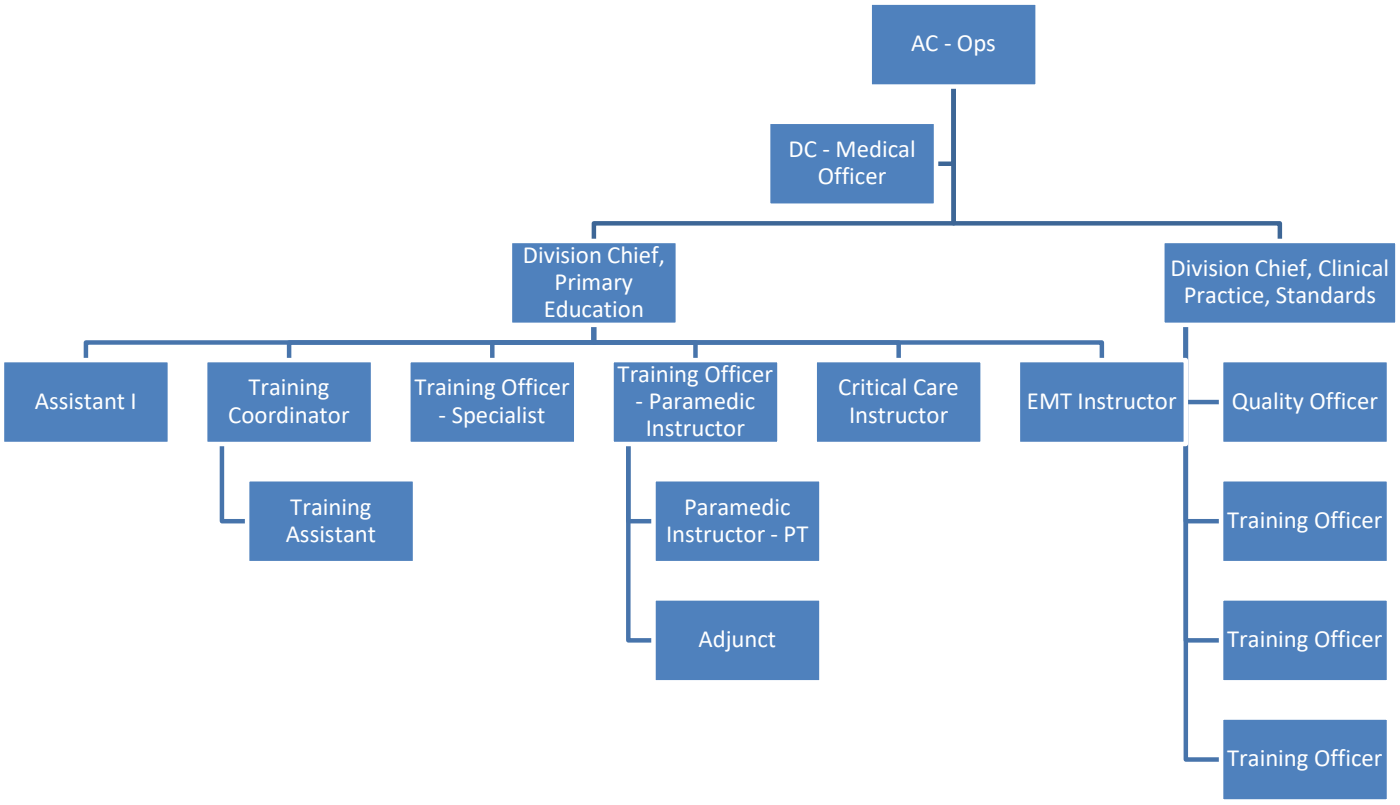
This policy/procedure supersedes any previous policy or memorandum on this topic.

DRAFT

Preexisting Organizational Chart



New Organizational Chart



Memo

To: Chief Kelly Cope

From: Brooke Snyder, HR Director

Date: 7/24/2023

Re: Broker Services

SCCAD has a robust medical, dental, vision and ancillary plan (STD, LTD, Life and Disability) that has been covered under brokered services since 2015. Partnering with a broker allows for best practices, on-going compliance, and the ability to negotiate the best rates for our insurance plans, ultimately saving the District money.

In June, SCCAD deployed an RFP for brokered services and received two bids: NFP and MMA. Both brokers presented bids for similar services with a $5,000 difference in the cost of their services.

SCCAD currently uses MMA for brokerage services and has since 2018. MMA has been an excellent partner for the District, exceeding customer service expectations, best practices and negotiating low administrative rates for the District. MMA came in $5,000 lower than NFP and kept their brokerage fees at $60,000 and hasn't increased this price in the last five years. All current medical file feeds are in place with MMA, which will save the District administrative costs of switching to a different broker.

Given the success of using MMA as our broker since 2018 and the excellent customer service provided to SCCAD, management is requesting approval of awarding the competitive bid to MMA to provide brokerage services for Medical, Dental, Vision, Short-Term Disability, Long Term Disability, Life and Disability and FSA administration, not to exceed $60,000 per year, for a term of three years (36 months).

ST. CHARLES COUNTY AMBULANCE DISTRICT
POLICY AND PROCEDURE MANUAL

CHAPTER 100 Personnel Policies & Procedures
SECTION 02 Job Descriptions
TITLE **PRIVACY OFFICER**
NUMBER 102-25a

DISTRIBUTION
All personnel.

PURPOSE
The Privacy Officer is responsible for the District's HIPAA privacy compliance program and SCCAD's Identity Theft Prevention Program. The Privacy Officer oversees the development, implementation, maintenance, and adherence with these compliance programs.

Deleted: compliance

DESCRIPTION
An individual designated by the District's CEO to serve as the District's Privacy and Red Flag Rule Compliance Officer. This position shall at all times be assumed by an existing management position within the District. In addition, this position is not considered remunerative in nature nor provides any rank above and beyond that of the person assuming the responsibility, therefore, it is not reflected in the District's organizational structure.

QUALIFICATIONS

- At least five years experience in EMS management at a mid-supervisory level or above.
- Knowledge and experience in federal and state information privacy, security, and identity theft laws and regulations.
- Knowledge and experience with access and release of information.
- Demonstrated organization, facilitation, communication and presentation skills.

Deleted: s,
Deleted: ,
Formatted: Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

TYPICAL DUTIES AND RESPONSIBILITIES

1. Works with management to establish a HIPAA privacy/security team charged with the development and implementation of a privacy/security and identity theft prevention compliance program.

2. Coordinate and facilitate the HIPAA team's activities in conjunction with the District's Chief Information Security Officer.

Deleted: Security

3. Collaborate with the HIPAA team, management, legal counsel, and appropriate staff to create, implement, and monitor the District's privacy policies, including policies for the following:

   a. Notice of privacy practices
   b. Handling protected health information (PHI and ePHI)
   c. Minimum necessary use and disclosure of PHI and ePHI
   d. Identity verification of individuals requesting PHI and ePHI
   e. Access, inspection, and copying of PHI and ePHI
   f. Amendment of PHI and ePHI

TITLE **PRIVACY OFFICER**
NUMBER 102-25a

Deleted: Accounting for disclosures of PHI and ePHI¶
Security and Level of Access to PHI and ePHI¶

TYPICAL DUTIES AND RESPONSIBILITIES (Continued)

g. Accounting for disclosures of PHI and ePHI
h. Security and Level of Access to PHI and ePHI.
i. Reporting and initiate investigation of potential breaches of PHI and ePHI
j. Record-keeping procedures and other administrative procedures.

4. Monitor all departments, divisions, and operations to ensure compliance with all applicable state and federal privacy laws.

5. Collaborate with other departments, divisions, and committees of the District (such as human resources, accounting, legal counsel and information systems) to ensure compliance with specific privacy and security requirements related to HIPAA and Identity Theft Prevention.

6. Assist in the development, implementation, and monitoring of business associate agreements to ensure that all privacy and security requirements related to HIPAA and Identity Theft Prevention compliance are adequately addressed.

7. Collaborate with the District's Training Division to develop and implement an organization-wide privacy training program and a certification program to ensure that all workforce members certify their recognition of and compliance with the organization's privacy and security policies and procedures related to HIPAA and Identity Theft Prevention compliance.

8. Establish and monitor a system for receiving questions and complaints regarding the privacy and security program from patients and the general public, ensure that the notice of privacy practices includes a method for contacting the organization regarding privacy matters, and document complaints and their resolution relating to HIPAA and Identity Theft Prevention compliance.

9. Work with management and legal counsel to develop methods of investigating allegations of non-compliance with the District's privacy policies, and develop appropriate sanctions for non-compliance by employees and business associates.

10. Conduct annual audits to ensure effectiveness and compliance with District privacy and security policies related to HIPAA and Identity Theft Prevention.

11. Make periodic reports to management and make recommendations on the status of the privacy and security program related to HIPAA and Identity Theft Prevention.

TITLE **PRIVACY OFFICER**
NUMBER 102-25a

TYPICAL DUTIES AND RESPONSIBILITIES (Continued)

12. Develop, monitor, and implement corrective action procedures to mitigate the effects of prohibited use of disclosure of PHI and ePHI by workforce members or business associates related to HIPAA and Identity Theft Prevention compliance.

13. Maintain current knowledge of applicable standards and revise the privacy and security compliance programs as necessary to reflect changes in the law or District policy as related to HIPAA and Identity Theft Prevention compliance.

14. Serve as an internal resource for all privacy and security-related matters and cooperate with external parties in any compliance reviews or investigations related to HIPAA and Identity Theft Prevention compliance.

Adopted by Board of Directors: 12/18/02
Revised: 7/1/09

This policy/procedure supersedes any previous policy or memorandum on this topic.

ST. CHARLES COUNTY AMBULANCE DISTRICT
POLICY AND PROCEDURE MANUAL

CHAPTER 100 Personnel Policies & Procedures
SECTION 02 Job Descriptions
TITLE **Chief Information Security Officer (CISO)**
NUMBER 102-25b

DISTRIBUTION
TBD

PURPOSE
The District's CEO designates this individual as the District's Chief Information Security Officer. An existing management position within the District shall always assume this position. The Chief Information Security Officer serves in this role to comply with HIPAA requirements to designate an information security officer.

DESCRIPTION
The Chief Information Security Officer (CISO) is responsible for the District's HIPAA Security compliance program. The CISO is responsible for the organization's Security Program, including but not limited to daily operations of the IT security program, oversight of the annual and ongoing risk assessment process, development, implementation, and maintenance of policies and procedures, ensuring the confidentiality, integrity, and access of electronically protected health information and of monitoring program compliance as well as investigation and tracking of incidents and breaches and in compliance with federal and state laws.

QUALIFICATIONS

- At least 5 years of information security work experience is required, with both public and private sector experience preferred.
- At least 7 year's experience of managing Enterprise Technology infrastructure
- Knowledge and experience in state and federal information security laws, including but not limited to HIPAA, including NIST, PCI, and all other applicable regulations.
- Recommended Security certification such as Certified in Healthcare Privacy and Security (CHPS) and/or other healthcare industry-related security credentials.
- Knowledge of HIPAA, state and federal guidelines on security, transactions and security.

TYPICAL DUTIES AND RESPONSIBILITIES

1. Builds a strategic and comprehensive information security program that defines, develops, maintains and implements policies and processes that enable consistent, effective information security practices which minimize risk and ensure the integrity, confidentiality and availability of information that is owned, controlled and processed within the organization. Ensures information security policies, standards, and procedures are up-to-date.

2. Manages security incidents and events involving electronically protected health information (ePHI)

3. Ensure that the disaster recovery, business continuity, risk management, and access controls needs of the facility are addressed.

4. Ensures the District complies with the administrative, technical, and physical safeguards.

5. Collaborates with District senior management, Privacy Officer, and General Counsel to establish governance for the security program.

6. Serves in a leadership role for security compliance

7. Works closely with the Privacy Officer to ensure alignment between security and privacy compliance programs, including policies, practices, and investigations.

8. Responsible for initial and periodic information security risk assessment/analysis, mitigation, and remediation. Responsible for the development and implementation of a security risk management plan.

9. Participates in the development, implementation, and ongoing compliance monitoring of all BAs and business associate agreements to address security concerns, requirements, and responsibilities.

10. Assists Privacy Officer as needed with breach determination and notification processes under HIPAA and applicable State breach rules and requirements.

11. Establishes and administers a process for investigating and acting on security incidents that may result in a privacy breach breaches.

12. Participates in all aspects of discovery and investigations involving allegations of privacy and/or security breaches.

13. Partners with Human Resources and Privacy Officer to ensure consistent sanctions for security violations

14. Maintains current knowledge of applicable federal and state security laws, licensing and certification requirements, and accreditation standards.

15. Cooperates with the U.S. Department of Health and Human Service's Office for Civil Rights, State regulators and/or other legal entities, and organizations on officers in any compliance reviews or investigations.

16. Serves as an information security consultant to all departments for all data security-related issues.

17. Project manager for Technology initiatives.

ST. CHARLES COUNTY AMBULANCE DISTRICT
POLICY AND PROCEDURE MANUAL

CHAPTER 200 Operating Policies & Procedures
SECTION 09 Health Insurance Portability & Accountability Act (HIPAA)
TITLE **SECURITY INCIDENT MANAGEMENT**

NUMBER 209-11

DISTRIBUTION
All Personnel.

PURPOSE
Incidents that could compromise our electronic information system are serious as critical patient information may be damaged or lost. This policy establishes St. Charles County Ambulance District's general policy on how to report a security incident and references the procedural responsibilities and process if a potential or actual security incident occurs.

POLICY

Security Incident Defined

A "Security Incident" is a suspected, attempted, or imminent threat of unauthorized access, use, disclosure, breach, modification, disruption or destruction to or of District Data.
Security incidents may include such things as a virus, email phishing event or unauthorized use of computer accounts and computer systems. It may also include complaints or reports of improper use of our information system.

Reporting a Security Incident

All staff members are responsible for immediately reporting a security incident or suspected security incident immediately. When a suspected security incident occurs, the Office of Information Technology must be contacted via phone to report the incident. If the reporting party is unable to reach anyone from the Technology team, contact your immediate supervisor for escalation notifications.

The Chief Information Security Officer will be responsible for initiating an immediate investigation to isolate the problem and take whatever action is necessary to protect the information system and e-PHI and other vital electronic information. If indicating factors reveal the possibility of ePHI data being involved. The Chief Information Security Officer will notify The Privacy Officer of such.

The Office of Information Technology and the Security Operations Center (SOC)will follow the departments procedurals process outlined in the Cyber Incident Response Plan. This plan is maintained updated on a quarterly basis to ensure current processes.

The Chief Information Security Officer will notify management immediately in the event the incident cannot be immediately corrected, or if any e-PHI or other vital information is altered or destroyed. Management will also be notified of any completed investigation and the outcome of the investigation. In the event of a suspected computer crime, or other unlawful activity via the use of the information system, local, state, or federal law enforcement may need to be notified. That determination will be made by management.

Deleted: the

Deleted: steps that will be taken by the District to investigate and take action when

Deleted: The "Computer Incident Reporting Form" (attached) should be used in conjunction with this policy. ¶

Deleted: is

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt

Deleted: an attempted entry, unauthorized entry, or an information breach or attack on our electronic information system. It includes unauthorized probing and browsing of the files, a disruption of service from any cause, and incidents where electronic information has been altered or destroyed.¶

Deleted: or a worm,

Deleted: a "Computer Security Incident Form" will be completed.…

Deleted: Privacy/

Deleted: Privacy/

Administration is responsible for coordinating communications with outside organizations and law enforcement.

TITLE **SECURITY INCIDENT MANAGEMENT**
NUMBER 209-11

POLICY (Continued)

Whenever a security incident, such as a virus, , phishing e-mail, discovery of hacking tools, altered data, or other event that could harm the information system is suspected or confirmed, remedial action will be taken, in accordance with District Policy 108-4 when it has been confirmed that a staff member caused or contributed to the incident.

Deleted: worm

Deleted: hoax

Privacy/ Chief Information Security Officer Responsibility

The Privacy/ Chief Information Security Officer is responsible for the following:

- Initiating the appropriate incident management action, including restoration as defined in the Cyber Incident Response Plan.
- Determining the physical and electronic evidence to be gathered as part of the incident investigation.
- Monitoring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.
- Determining if a widespread communication is required, the content of the communication, and how best to distribute the communication.
- Communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability.
- Initiating, completing, and documenting the incident investigation.

Deleted: Incident Management

Deleted: Procedures

Enforcement

St. Charles County Ambulance District's Privacy/ Chief Information Security Officer and all members of management are responsible for enforcing this policy. Staff members who violate this policy will be subject to disciplinary action in accordance with District Policy 108-4.

Adopted by Board of Directors: 06/22/2005

This policy/procedure supercedes any previous policy or memorandum on this topic.

ST. CHARLES COUNTY AMBULANCE DISTRICT
POLICY AND PROCEDURE MANUAL

CHAPTER 200	Operating Policies & Procedures
SECTION 09	Health Insurance Portability & Accountability Act (HIPAA)
TITLE	**PRESERVING DATA AND ELECTRONICALLY STORED INFORMATION: CREATING BACKUPS**
NUMBER	209-14

DISTRIBUTION

This policy applies to all electronically stored data and information created, received, used or stored by St. Charles County Ambulance District. Creating backups will be the responsibility of the IT Department. This policy applies to all electronic equipment and storage devices that are owned or leased by St. Charles County Ambulance District. The procedures apply to all staff members and vendors or contracted parties who are responsible for completing backups.

PURPOSE

The purpose of this policy is to outline the procedures for preserving and protecting e-PHI and other important business information from tampering, theft, fire, flood, and other physical damage. A key to this process is the proper replication of exact copies of data in a secondary system so that if the primary system fails, the data will be completely preserved and accessible.

POLICY

Identification of Critical Data

The District must identify what data is most critical to its organization. This can be done through a formal data classification process or through an informal review of information assets. Regardless of the method, critical data should be identified so that it can be given the highest priority during the backup process.

Formatted: Font: (Default) Times New Roman, 12 pt

Data to be backed up will include:

- All data determined to be critical to the District operation and/or employee job function
- All information storage on the Districts file storage servers (i.e. network drives). It is the end user's responsibility to ensure that any data of importance is moved and stored in network or secure cloud storage area identified within this policy.
- All information stored on District managed cloud solutions, (such as Microsoft SharePoint, OneDrive, Microsoft Teams),
- NOTE: Data stored locally on a end users computer is NOT backed up by the District unless that data path is replicated in a District managed cloud solution (such as Microsoft SharePoint, OneDrive, Microsoft Teams),
-

Formatted: Line spacing: 1.5 lines

Formatted: Line spacing: 1.5 lines, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Physical Access Controls

All on-premises backup solutions will be located in a secure area, with limited access so that only those with responsibility for the backup system will have access to it. Servers, backup drives and other data and information saving hardware will be located in a secureable room.

Backup Schedule

Data and information stored on any servers or electronic devices will be backed up incrementally on a daily basis and full backups will be compelted on a weekly basis, to ensure that critical data (especially PHI and e-PHI) can be restored and recovered immediately.

TITLE **PRESERVING DATA AND ELECTRONICALLY STORED INFORMATION: CREATING BACKUPS**

NUMBER 209-14

POLICY

Backup Schedule Logs

Logs, when and where the media was sent off-site, the success or failure of restore tests and bad media encountered which may affect our ability to obtain files from a previous backup.

The Office of Information Technology will rotate the media used for backups. This staff member will review the backup for successful completion, research any problems encountered and enter on the log: 1) the tape descriptionand 2)the backup date.

Marking and Storage of Backup Media

All backup disks, drives, tapes or other devices will be legibly and clearly marked with the fact that it is a backup.

Backup devices and storage units will be stored in containers that help protect the backup from damage due to moisture or other environmental concerns.

Backup media will be stored in a manner that protects it from tampering, theft, fire, flood, and other physical damage.

Encryption of Backups

It is the policy of St. Charles County Ambulance District to use encryption or decryption techniques wherever possible, in particular all external backup media will be encrypted, as required by HIPAA regulatory compliance.

Data Retention

Archived backups must be periodically tested to ensure that they are recoverable.

Deleted: systems

Deleted: locked

Deleted: The Computer Support Specialist in coordination with the Privacy/Security Officer will maintain a current list of all individuals who are approved for access and this list will be reviewed periodically.

Deleted: at the end of each work day whenever possible

Deleted: ,

Deleted: but at a minimum, backups must be made at sufficient intervals

Deleted: A full system backup will be completed at least monthly.

Deleted: Two sets of daily (Monday-Thursday)backup tapes will be alternated between during the month until the month-end backup has been completed. The Friday daily backup tapes will be removed from the premises and stored at a secure off-site location on a weekly basis. This will ensure the preservation of all but the most recent data and information in the event of a catastrophic fire, flood, or other damage to the primary backup location. ¶
¶
There will be verification that the backup was successfully completed at the end of each backup process, to ensure that a complete replication of the data and information backed up has actually been created. ¶

Deleted: The backup software will capture a list of all files and directories encountered and saved.

Deleted: will be maintained and will contain information about successful backups, unsuccessful backups, backup media that was left in place accidentally and overwritten

Deleted: IT Department

Formatted: Justified

Deleted: (Mon1, Tues2, etc.)

Deleted: The log sheet will be stored in the backup tape security box. ¶

Deleted: Backup devices and storage units will be ultimately stored in a secure location and in cabinets or shelving that is conducive to its identification and protection within that location

Deleted: While we are not legally required to "encrypt" electronic information or files in most cases, we are obligated to ensure that e-PHI, PHI, and other important patient or Company information does not fall into the wrong hands or is viewed or used by those who should not have access to it. Thus,

Deleted: i

Deleted: .

Deleted: Full system backups will be copied and/or archived at least weekly and will not be stored in the same geographic location as the source systems.

Deleted: Friday backups will be kept until a month-end is completed and all month-end backups will be kept until a year-end is completed. Year-end backups will be kept indefinitely.¶

ST. CHARLES COUNTY AMBULANCE DISTRICT
POLICY AND PROCEDURE MANUAL

TITLE **PRESERVING DATA AND ELECTRONICALLY STORED INFORMATION: CREATING BACKUPS**
NUMBER 209-14

POLICY

Off-Site Storage Procedures

St. Charles County Ambulance District may contract with a reputable vendor to manage its backup process and media storage. The vendor must execute a Business Associate agreement with St. Charles County Ambulance District to ensure that the vendor will, among other things, protect the integrity of the data stored and protect it from improper use or disclosure.

Security access controls implemented at the off-site backup and storage location must meet or exceed the security access controls of the source systems. In other words, information security at the backup storage location must equal or exceed the security where the primary computers and servers are located.

Documentation

The backup restore and recovery processes must be documented. Backups must be performed in accordance with the documentation provided for the particular backup software or system.

Deleted: with the following critical information in accordance with the procedures established for maintaining paper (hard copy) backup logs.

Storage of Media Other Than Backups

Old hard drives or other media storage devices that have been removed from the information system will be handled as follows: 1) if the device is to retain data, it will be stored in a similar fashion as the backup devices; 2) if the device is to be taken out of service and no longer used to store data, it shall be "sanitized" and erased prior to disposal in accordance with industry standards.

Deleted: Emergency Contact information¶
The administration will maintain a list of designated staff to be contacted in an emergency. A copy of this list will be kept in a secure location, such as the main computer facility. The list must be kept up to date and readily accessible in case of an emergency. The list will also include vendor contacts and support information.¶

Adopted by Board of Directors: 06/22/2005
Revised: 07/01/09

This policy/procedure supersedes any previous policy or memorandum on this topic.

ST. CHARLES COUNTY AMBULANCE DISTRICT
POLICY AND PROCEDURE MANUAL

CHAPTER 200 Operating Policies & Procedures
SECTION 09 Health Insurance Portability & Accountability Act (HIPAA)
TITLE **CONTINGENCY PLANNING**
NUMBER 209-16

DISTRIBUTION
This policy covers the procedures for protecting the integrity of PHI and other essential patient information, billing and business information, and confidential information in the event of an emergency, disaster or other occurrence (i.e., fire, vandalism, system failure and natural disaster) when any system that contains this information is affected, including:

- Applications and data criticality analysis
- Business intelligence related data
- Data backup
- Disaster recovery planning
- Emergency mode operation plan

PURPOSE
St. Charles County Ambulance District is committed to providing all aspects of our service and in conducting our business operations in compliance with all applicable laws and regulations concerning the security and integrity of Protected Health Information (PHI), electronic protected health information (e-PHI) and other essential patient information, billing and business information, and confidential information that is stored electronically or by other means.

This policy describes the approach to ensuring that the District's response to an emergency or other occurrence that threatens or damages our computer, electronic, or other information systems is appropriate. This policy provides for the contingencies necessary to protect and preserve that information in accordance with the HIPAA Security Rule and other regulations.

POLICY
Applications and Data Criticality Analysis

Administration will assess the relative criticality of specific applications and data within the District for purposes of developing its Data Backup Plan, its Disaster Recovery Plan and its Emergency Mode Operation Plan.

The assessment of data and application criticality should be conducted periodically and at least annually to ensure that appropriate procedures are in place for data and applications at each level of risk.

Data Backup Plan

The District data backup plan is fully documente in Data Backup Policy xx-xx

Deleted: Administration will establish and implement a Data Backup Plan that ensures that each area of the District will create and maintain retrievable exact copies of all PHI and other essential business information that is at a medium to high risk for destruction or disruption.

The Data Backup Plan must apply to all medium and high risk files, records, images, voice or video files that may contain PHI and other essential business information.

POLICY (Continued)

Disaster Recovery Plan

To ensure that the District can recover from the loss of data due to an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster affecting information systems containing PHI or other essential business information, the District will establish and implement a Disaster Recovery Plan. The Plan must ensure that each area can restore or recover any loss of this information and the systems needed to make that information available in a timely manner.
The Diaster Recovery Plan is further documented under policy 209-15 Disaster Management and Recovery of E-PHI

Emergency Mode Operation Plan
This is also refered to as a Business Continuty plan and each functional area of the District will have (as needed) procedures to enable continuation of administrative, patient care, and billing and business processes for protection of the security of PHI and other essential business information while operating in emergency mode. Emergency mode operation procedures outlined in the Emergency Mode Operation Plan will be tested periodically to ensure that critical business processes can continue in a satisfactory manner while operating in emergency mode.

Adopted by Board of Directors: 06/22/2005
This policy/procedure supercedes any previous policy or memorandum on this topic.

Deleted: The Data Backup Plan must require that all media used for backing up PHI and other essential business information be stored in a physically secure environment. Where backup media remains on site, it will be kept in a physically secure location, different from the location of the computer systems have been backed up.
¶
Data backup procedures and contingency plan shall be tested on a periodic basis to ensure that exact copies of PHI and other essential business information can be retrieved and made available whenever it is needed.

Deleted: The Disaster Recovery Plan will include procedures to restore PHI and other essential business information from data backups in the case of a disaster causing data loss.

The Disaster Recovery Plan will include procedures to log system outages, failures, and data loss to critical systems, and procedures to train the appropriate personnel to implement the disaster recovery plan.

The Disaster Recovery Plan must be documented and easily available to the necessary personnel at all time, who should be trained to implement the Disaster Recovery Plan.

The disaster recovery procedures outlined in the Disaster Recovery Plan will be tested on a periodic basis to ensure that PHI and other essential business information and the systems needed to make e-PHI available can be fully restored or recovered.

Each area at a medium and high risk of compromise of PHI and other essential business information will have a Disaster Recovery Plan as set forth by administration.

Deleted: Each

CHAPTER 200 Operating Policies & Procedures
SECTION 09 Health Insurance Portability & Accountability Act (HIPAA)
TITLE **HIPAA BREACH INCIDENT RESPONSE AND REPORTING**

NUMBER 209-19

DISTRIBUTION
All Personnel.

PURPOSE
This policy is intended to address the regulatory requirements related to a breach of unsecured protected health information (PHI) under the Health Insurance Portability and Accountability Act of 1996 and establishes a process to investigate and provide required notification in the event of a breach of (PHI).

The "HIPAA Privacy Complaint Form" (attached) should be used in conjunction with this policy.

POLICY
It is the policy of the District to make certain that compliance efforts are in place as it relates to PHI, as well as to ensure that such information is used and disclosed in accordance with all applicable laws and regulations.

Any concerned individual, patient, or employee has the right to file a formal complaint concerning any suspected violation of the HIPAA regulations.

The District's Privacy Officer will document all complaints received and their disposition, if any.

The District will investigate, follow-up, and resolve individual, patient, or employee complaints related to privacy rights, the District's policies and procedures, and the District's compliance with privacy policies and procedures without threat or retaliation against the complainant or concerned party.

If there is an access, acquisition, use or disclosure of unsecured PHI that is not permitted by the Privacy Rule and which compromises the security or privacy of the PHI, a breach will have been presumed to have occurred unless the District can demonstrate that there is a low probability that the PHI has been compromised or an exception to the breach applies.

PROCEDURE

Reporting a Security Incident

1. All staff members are responsible for immediately reporting a suspected impermissible access, use, or disclosure under the Privacy Rule that may compromise the privacy or security of unsecured PHI to the District's Privacy Officer.
2. The Privacy Officer will gather any preliminary information and identify which (if any) other members of the HIPAA Response Team should be notified and involved in the investigation.

SCCAD's HIPAA Response Team may include the following representatives:

Privacy Officer
Security Officer
District Counsel
Human Resource Director
Department Leadership
Chief of Department

3. The Privacy Officer will access and investigate concerns and complaints in accordance with the requirements of HIPAA and include:
    a. A written collection of relevant facts
    b. A determination as to whether there was a violation of the Privacy Rule and/or District Policy.
    c. The completion of a risk assessment to determine the probability of whether PHI was compromised, such that a breach of presumption can be refuted.
    d. A determination as to whether a Breach exception applies.
4. To determine the probability that PHI has been compromised, a risk assessment containing the following elements shall be conducted, documented, and maintained by the Privacy Officer:
    a. The nature and extent of PHI involved, including the identifiers and likelihood of re-identification;
    b. The unauthorized person(s) who accessed PHI or to whom the disclosure was made;
    c. Whether the PHI was actually acquired or viewed; and
    d. The extent to which the risk to the PHI has been mitigated.
5. If the risk assessment demonstrates that there is a low probability that PHI has been compromised, then the incident will be determined to have not been a breach and no notification is necessary under HIPAA. If the risk assessment demonstrates that there is more than a low probability that PHI was compromised, then the Privacy Officer will determine if one or more of the breach exceptions applies from below:
    a. Unintentional acquisition, access, or use of PHI by an employee, staff, or person acting under the authority of the District or a Business Associate, if such acquisition, access, or use was made in good faith, within the scope of the person's authority, and does not result in further use or disclosure in a manner not permitted by the Privacy Rule.
    b. The inadvertent disclosure of PHI by a person authorized to access PHI at the District or a Business Associate to another person authorized to access PHI at the District or the same Business Associate, or organized health care arrangement that the District may participate in.

c. The District has a good faith belief that the unauthorized person to whom the impermissible disclosure was made would not reasonably have been able to retain that information.

6. If a breach of unsecured PHI is determined to have occurred, the District must provide notification, as described below, to:
    a. The affected individual(s) by either written or electronic means within sixty (60) days; and
    b. The Secretary of Health and Human Services (HHS) annually, unless the breach involves more than five hundred (500) affected individuals which would require notification without delay, but in no case more than sixty (60) days following discovery of the breach.
    c. The media when the breach involves more than five hundred (500) affected individuals.
7. Required notification of the breach should include the following, at minimum:
    a. A brief description of the breach.
    b. Date of the breach and date of discovery (when known)
    c. A description of the types of PHI involved in the breach
    d. The steps affected individuals should take to protect themselves from potential harm
    e. A brief description of what the District is doing to investigate the breach, mitigate harm to affected individuals, and prevent further breaches
    f. Contact information for the affected individuals to ask questions and learn more information

Enforcement

St. Charles County Ambulance District's Privacy Officer and all members of management are responsible for enforcing this policy. Staff members who violate this policy will be subject to disciplinary action in accordance with District Policy 108-4.

Adopted by Board of Directors:

This policy/procedure supercedes any previous policy or memorandum on this topic.

ST. CHARLES COUNTY AMBULANCE DISTRICT
POLICY AND PROCEDURE MANUAL

CHAPTER 700 Information Systems Policies and Procedures
SECTION 01 General
TITLE **PHOTOGRAPHY POLICY**
NUMBER 701-4

DISTRIBUTION
All personnel.

PURPOSE
The intent of the policy is to regulate the creation and distribution of photographs including but not limited to photographs and digital images that are taken by SCCAD employees, in the course of and scope of their job functions, including, emergency and medical scenes, and/or of SCCAD patients. The respect of patient privacy and maintaining the integrity of any incident are essential to this policy. Protecting the District's reputation and ensuring that an employee's communication with people outside the District, not only reflect positively on the employee as an individual, but also on the District.

POLICY

1. SCCAD retains strict requirements on the security, access, disclosure and use of photographs. Access, disclosure and use of PHI via photographic or video recording devices will be based on the individual role of the staff member and only to the extent that the person needs access to PHI to complete the necessary job functions.

2. When PHI is accessed, disclosed, and used, the individuals involved will make every effort to use the PHI to the extent that only the minimum necessary information is used to accomplish the intended purpose.

3. Cellular Phones – No person shall use their District or personal cell phone to take photographs or video recordings at any SCCAD scene depicting a patient or patient care being performed.

4. Personal Cameras – No person shall use their personal camera while performing duties within the course or scope of their employment. Only district issued and owned cameras may be used under such circumstances and in compliance with this Policy. Personal cameras may be used for personal projects while on duty only when the person is not performing their duties or is not otherwise acting within the course and scope of their employment provided that doing so does not interfere with anyone's (themselves or others) performance of their job duties and further that the use complies with this and other applicable District Policies.

5. Photographs or recordings of any scene or patient taken on duty or in the course and scope of employment may not be captured, copied, stored or transmitted onto any device not owned by SCCAD. This specifically means that photographs may not be copied or transmitted onto other computers, hard drives, portable media drives or storage device of any kind not owned by SCCAD. Such photographs shall not be sent via e-mail, fax, scanned copied or duplicated unless specifically approved by the Privacy Officer or their designee.

Deleted: .
Deleted: CEO, PIO
Deleted: ate

TITLE **PHOTOGRAPHY POLICY**
NUMBER 701-4

POLICY (continued)

6. The District recognizes the occasional benefit of **scene** photography for documentation of MOI, scene description, or continuing education. As such, photographs may be taken on scene using only District equipment for these reasons so long as by doing so will not delay or impede patient care. Scene photographs shall be attached to and become part of the patient care record and/or accident investigation record as applicable and then permanently deleted from the District device that it was captured on. Scene photographs are not to be confused with photographs depicting patient s or patient care.

7. Photographs should be handled in the same manner as patient care reports and cannot be used or disclosed for any other purpose other than those permitted by law.

8. Requests for copies of photographs taken subject to this policy shall be referred to the Privacy Officer.

9. Only approved personnel may take photographs. Licensed EMT-B, EMT-Ps, and FAA credentialed drone pilots are approved to take scene photography as outlined in this policy provided they have not had that right revoked for improper application of this policy.

10. Scene content may include MOI if it is necessary to accomplish the purpose of this policy. No photographs or recordings depicting PHI will be used outside of this policy by SCCAD without a signed patient authorization / release form.

11. Scene locations may include, but are not limited to private residences, businesses, public areas and the back of the ambulance.

12. No photographs may be taken of patients or patient care without expressed permission from the Privacy Officer or their designee.

13. All photographs taken by a SCCAD employee of an incident, accident scene, patient or any other photographs / recording taken on duty and in the scope of employment with SCCAD shall constitute the sole and exclusive property of SCCAD. SCCAD retains all copyrights to all scene photographs or recordings taken in conjunction with this policy.

14. The following matters will be treated as gross misconduct capable of disciplinary action per Policy 108-4:

    A. Acquiring or sharing of any photograph, digital image, or video recording depicting a SCCAD scene or patient without written authorization and release from the patient and Privacy Officer.
    B. Posting or sharing of any photograph, digital image or video recording depicting a SCCAD scene or patient is strictly prohibited, as already discussed in this policy. Consult your supervisor if you are unclear about what might be confidential.

Deleted: s
Formatted: Font: Bold, Underline
Deleted: Public Information Officer.
Deleted: EMTB and paramedic
Deleted: s
Deleted: or patient care
Formatted: List Paragraph, Left, No bullets or numbering
Deleted: <#>SCCAD retains all copyrights to all scene photographs or recordings taken in conjunction with this policy.¶ ¶
Deleted: SCCAD
Deleted: ¶
¶
PROCEDURE¶
¶
The PIO will act as the post scene photography control officer. All photos taken will be submitted to the PIO via the shift officer or supervisor at the end of each shift. The shift officer or supervisor will collect the digital recording card from the crew and provide the crew with a new card. Immediately following the call, crews should contact the supervisor to obtain a new camera card.¶
¶
TITLE **PHOTOGRAPHY POLICY**¶
NUMBER 701-4¶
¶
PROCEDURE (continued)¶
¶
The digital card collected will be placed in a sealed envelope with the supervisor's signature on the envelope, then delivered or sent to the PIO via interoffice mail for review. The PIO will either save or destroy the image. If the image is saved it will be cataloged by date and incident number. The digital card will be erased, reformatted and returned to the supervisor for reuse.¶
¶
The images will be coded as:¶
No release mark for destruction¶
No release patient documentation only¶
No release pending signed release¶
Release for internal training¶
Release for public dissemination¶
¶
If you already have a personal blog or website which contains images that are not permitted under this Policy you must remove those images to remain in compliance with this policy or contact the PIO in those situations that may warrant an exception to the policy. ¶
¶
If someone from the public, media or press contacts you about your non-union related online publications that relate to St. Charles County Ambulance District you should report this immediately to the Chief Executive Officer and Public Information Officer.¶
¶

ST. CHARLES COUNTY AMBULANCE DISTRICT
POLICY AND PROCEDURE MANUAL

Adopted by the Board of Directors: 1/27/2010

This policy/procedure supersedes any previous policy or memorandum on this topic.

Deleted: ¶
¶
¶

Deleted: ¶
¶

ST. CHARLES COUNTY AMBULANCE DISTRICT
POLICY AND PROCEDURE MANUAL

CHAPTER 700	Operating Policies & Procedures
SECTION 01	Information Systems Policies & Procedures
TITLE	**IDENTITY ACCESS MANAGEMENT & PASSWORD REQUIREMENTS**
NUMBER	701-08

Deleted: xx

DISTRIBUTION

The Policy applies to all staff members and vendors or contracted parties who are responsible for completing backups. Assigning unique user logins and requiring password protection is a primary safeguard to restrict access to the SCCAD data network and the data stored within it to only authorized users. If a password is compromised, access to information systems can be obtained by an unauthorized individual, either inadvertently or maliciously. Individuals with SCCAD are responsible for safeguarding against unauthorized access to their account and as such, must conform to this policy to ensure passwords are kept confidential and are designed to be strong and difficult to breach.

PURPOSE

The purpose of this policy is to specify guidelines and requirements for the use of SCCAD District network passwords. Most importantly, this policy will help users understand why strong passwords are necessary and help them create secure and useable passwords. The parameters in this policy are designed to comply with legal and regulatory standards, including but not limited to the Health Insurance Portability and Accountability Act (HIPAA), and align with national Cybersecurity Framework (CSF) standards based on the guidelines of the National Institute of Standards and Technology (NIST).

POLICY

Individual Responsibilities

Individuals are responsible for keeping passwords secure and confidential. As such, the following principles must be adhered to for creating and safeguarding passwords:

- SCCAD passwords must be changed immediately upon issuance for the first use. Initial passwords must be securely transmitted to the individual, either via the individual's supervisor, direct communication (via phone) with IT Support Services (ITS), or Human Resources at New Hire Orientation.

- SCCAD passwords must never be shared with another individual for any reason or in any manner not consistent with this policy. A shared or compromised SCCAD password is a reportable ITS security incident.

- Employees—including vendors, and supervisors—as well as students and other SCCAD personnel, must never ask anyone else for their password. If you are asked to provide your password to an individual or sign into a system and provide access to someone else under your login, you are obligated to report this to the Director of IT immediately.

- SCCAD passwords must never be written down and left in a location easily accessible or visible to others. Passwords should not be stored in a web browser's password manager on an untagged device.

- Individuals must never leave themselves logged into an application or system where someone else can unknowingly use their account.

- ITS will never ask for a password. In ITS support scenarios where an ITS account cannot be used, an individual may allow a technician to utilize his/her computer under the individual's account even if the individual is unable to be present during the entire support session. The individual should not share his/her password with the technician.

- Passwords for SCCAD must be unique and different from passwords used for other personal services (e.g., banking).

- SCCAD passwords must meet the composition requirements outlined in this policy.

- SCCAD passwords must be changed regularly, as outlined in this policy, at the regularly scheduled time interval or sooner if there is suspicion of a compromise.

- In the event a breach or compromise is suspected, the incident must be reported to ITS Security immediately using one of the methods outlined in the Procedures section below.

2 Responsibilities of Systems Processing Passwords

All SCCAD systems—including servers, applications, and websites that are hosted by or for SCCAD—must be designed to accept passwords and transmit them with proper safeguards.

- Passwords must be prohibited from being displayed when entered.

- Passwords must never be stored or transmitted in clear, readable format (encryption must always be used).

- Passwords must never be stored as part of a login script, program, or automated process unless encrypted.

- Systems storing or providing access to confidential data or remote access to the internal network should be secured with multifactor authentication whenever possible.

- Encrypted password hashes must never be accessible to unauthorized individuals.

- Where possible, salted hashes should be used for password encryption. Exceptions should be filed and reviewed on a regular basis.

- Where any of the above items are not supported, appropriate authorizations and access control methods must be implemented to ensure only a limited number of authorized individuals have access to readable passwords.

3 Password Requirements

The following parameters indicate the minimum requirements for passwords for all individual accounts where passwords are:

- At least ten (10) characters;
- Not based on anything somebody else could easily guess or obtain using person related information (e.g., names, SCCAD, telephone numbers, dates of birth, etc.);
- Not vulnerable to a dictionary attack (see Recommendations for Creating Compliant Passwords section); and,
- Cannot be a commonly used word and/or a previously exposed breached/compromised passwords (enforced with quarterly updated against national database of compromised passwords)

Password Expiration

In order to prevent an attacker from making use of a password that may have been discovered, passwords are deemed temporary and must be changed regularly. ITS Security reserves the right to reset a user's password in the event a compromise is suspected or reported. The required frequency at which passwords must be changed varies based on the type of user, as defined below.

Standard Users

Standard users consist of SCCAD employees, (including temps, vendors, and consultants), that are not (1) system administrators.

- Passwords must be changed every four (4) months.
- Passwords must not be reused for at least ten (10) generations.
- Passwords must not be changed more than one (1) time per day.
- New passwords must comply with the password requirements defined in the previous section.

Privileged Users

Privileged users consist of users with elevated access to administer information systems and applications, most often in the Information Technologies & Services Department. Such users have administrator access and these accounts are at a higher risk for compromise.

- Passwords must be changed every ninety (90) days.
- Passwords must not be reused for at least six (6) generations.
- Passwords must not be changed more than one (1) time per day.
- New passwords must comply with the password requirements defined in the previous section.

System / service accounts

System and/or service account passwords are accounts assigned for system or application operations. The least privileged access level and device restrictions should be used at all times and be limited to a specific device or service requiring domain access permissions.

- Passwords must be changed every six (6) months
- Passwords must be a minimum of 14 characters
- Passwords must not be reused for at least ten (10) generations.

Account Lockout

In order to limit attempts at guessing passwords or compromising accounts, an account lockout policy is in effect for all systems. Account lockout thresholds and durations defined below:

- Accounts will lockout after five (5) invalid password attempts in fifteen (15) minutes.
- Accounts will remain locked for a duration of sixty (60) minutes, unless the ITS Service Desk is contacted, and the user's identity is verified in order for the account to be unlocked sooner.

Recommendations for Creating Compliant Passwords

To create a password that is compliant with the parameters specified in this policy, use one of the three methods below.

Use a Passphrase

A passphrase is similar to a password, but it is generally longer and contains a sequence of words or other text to make the passphrase more memorable. A longer passphrase that is combined with a variety of character types is exponentially harder to breach than a shorter password. However, it is important to note that passphrases that are based on commonly referenced quotes, lyrics, or other sayings are easily guessable. Passphrases should be unique to you.

- Try to use at least twenty (20) characters
- Incorporate the four-character types (a space or special character can be used to separate words or phrases to add complexity)
- Use a phrase that is easy to remember
- Abbreviate most of the words in the phrase to increase complexity
- Examples:
  - Phrase:"When I was five, I learned how to ride a bike."
  - Password: When I was 5, I learned to ride a bike.
  - Phrase:"When I was five, I learned how to ride a bike."
  - Password: WheIwas5,Ilear2ridabik.

Password Reset Options

If you do not change your password before it expires, you could be locked out from accessing internal company resources until an Administrator unlocks your account. Please follow the password reset instructions below, depending on your job role. If you experience any problems, please contact send an email to help@sccad.com.

For road personnel and remote staff, log into your Office365 account at https://Outlook.Office365.com

For office staff, press the Ctrl + Alt + Delete keys simultaneously from your Windows workstation and select 'Change Password' and enter your information.

Reporting a Suspected Compromise or Breach

If you believe your password has been compromised or if you have been asked to provide your password to another individual, including OIT, promptly notify the help@sccad.com

Applicability of Other Policies

This document is part of the District's cohesive set of security policies. Other policies may apply to the topics covered in this document, so the applicable policies should be reviewed as needed.

Enforcement

This policy will be enforced by the Director of Technology and/or Executive Team. Violations may result in disciplinary action, including suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of District property (physical or intellectual) are suspected, the District may report such activities to the applicable authorities.

**Add 209-10 sections