ARTICLES OF INCORPORATION

OF

Sunshine Healthcare System

The undersigned Incorporation of Sunshine Healthcare System, a Sunshine Healthcare System adopts the following Articles of Incorporation:

EFFECTIVE DATE OF INCORPORATION: September 7, 2025

I. Article 1 – Corporation Name

The name of the company shall be called Sunshine Healthcare System.

II. Article 2 – Registered Office Address

The office of the Sunshine Healthcare System is to be located at 100 Hospital Way, Atlanta GA 30033. The preferred place of business address is 100 Hospital Way, Atlanta GA 30033. The mailing address of the corporation is P.O 1232 Atlanta, GA 30033.

III. Article 3 – Purpose of the Corporation

The corporation is a non-profit healthcare organization operated to serve the healthcare needs of the local community and surrounding region under 501(C) of the Internal Revenue Code. The corporation is to support the healthcare needs by providing high-quality, accessible and affordable to every needing individual. Profits will not take precedence over promoting and restoring health of the served community.

The organization shall provide emergency care, preventive care, and chronic health management while providing for a person’s physical, mental, and social well-being. Services will be provided through emergency departments, outpatient clinics, inpatient hospitals, urgent care centers, and limited specialty care. The organization shall additionally provide a range of educational and preventative outreach services to the community.

All employees providing patient care in the organization will receive ongoing education and training promoting clinical excellence. Training will include hands-on training, lab stimulation, and on-line module training. Training will be provided in a timely manner, consistent with all evidence-based guidelines.

To ensure the highest quality standards, care will be data-driven and continuously evaluated to align with current guidelines and evidence-based recommendations. The organization will conduct retrospective analysis of care performance. Using this analysis, all providers will receive ongoing performance evaluations and feedback, with the aim of optimizing patient care.

IV. Article 4 – Vision Statement

The vision of Sunshine Healthcare System is to be the leading provider of healthcare in the region by providing comprehensive, high-quality healthcare services and be a leading employer of clinical staff for the region.

V. Article 5 – Mission Statement

Sunshine Healthcare System treats patients throughout their lifespan by providing comprehensive and evidence-based healthcare addressing physical, mental, and social well-being. Care will be provided in urgent care centers, emergency rooms, inpatient, outpatient clinics, specialty clinics, and through community outreach.

VI. Article 6 – Value Statement

Sunshine Healthcare System vision is to serve the entire community with dignity, honor, respect, and compassion. To strive for excellence in healthcare quality outcomes by providing care that is wholistic and evidence based. Sunshine Healthcare System will be the leader in healthcare quality outcomes compared to state and national standards. It will be the top choice for patients seeking care for their health and wellbeing. It will be consistently top ranked in patient satisfaction scores.

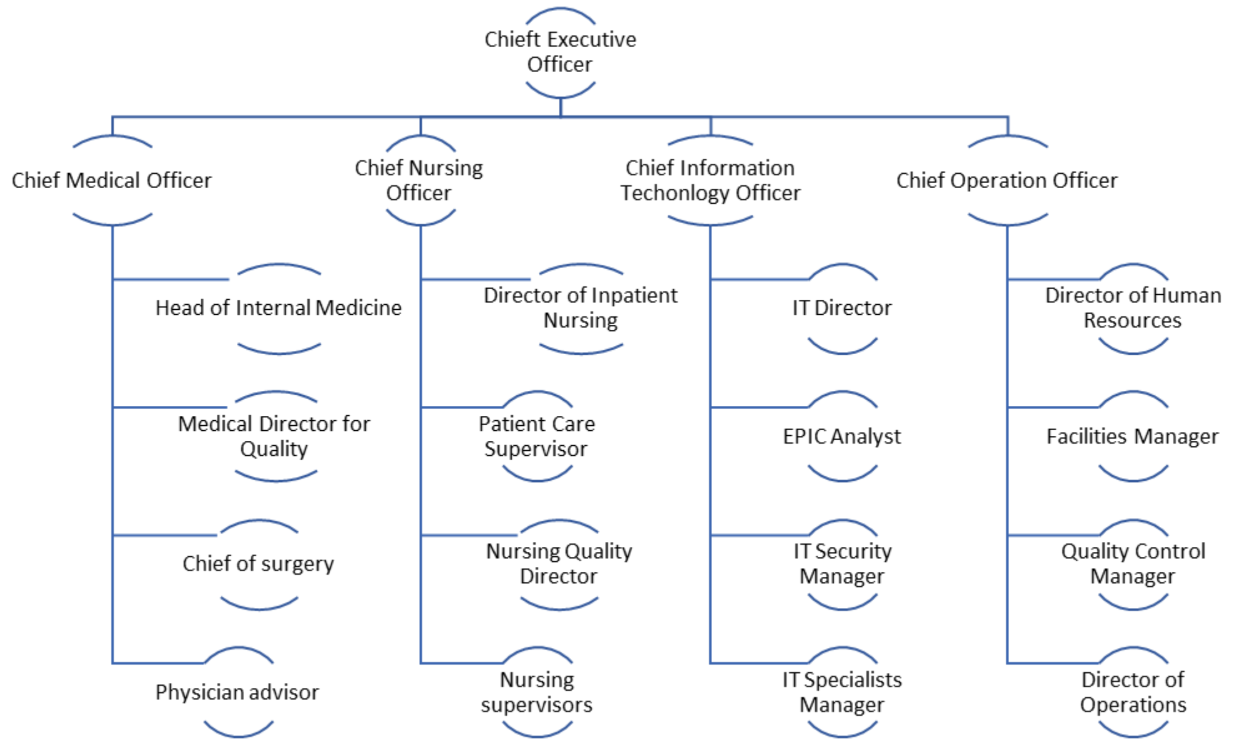
VII. Article 7 – Corporation Strategic Goals and Objectives.

Sunshine Healthcare System shall aim to achieve the following objectives:

- *Top ranked hospital*
    - Sunshine Healthcare System will become a top ranked hospital for cardiac, stroke, trauma, and orthopedic based on evidenced based outcomes and national registry standards
- *Best patient experience*
    - Sunshine Healthcare System will become the chosen hospital by patients based on volume and Press Ganey patient satisfaction ratings

- Best patient outcomes
    - Sunshine Healthcare System will achieve the best patient health care outcomes based on, but not limited to, mortality, length of stay, and readmission rates
- *Best place to work*
    - Sunshine Healthcare System will be a top destination for clinical staff within the region as measured by employee satisfaction surveys and employee retention ratings

VIII. Article 8 – Major Business Units and Governance Structure



ISSP on Fair and Responsible Use of Information Systems for Sunshine Healthcare System

1. Statement of Purpose

a. Scope and Applicability

Policy Overview

The purpose of this document is to articulate clear expectations for the equitable and responsible utilization of Sunshine Healthcare System's (SHS) information systems. These systems serve as critical instruments in the delivery of safe, efficient, and high-quality healthcare services. They facilitate clinical decision-making, patient record management, billing processes, scheduling, communication, and the overall functioning of daily operations.

Scope of the Policy

This policy applies to all individuals who utilize or access SHS technology resources, including full-time and part-time employees, contractors and consultants, temporary staff and volunteers, students, trainees, interns, business associates, vendors, and/or partners who engage with SHS systems under contractual agreements.

Policy Objectives

This policy is established to ensure that SHS technology resources are employed exclusively for legitimate organizational purposes. This policy also aims to ensure that confidential patient and organizational information are maintained in a secure and protected manner, that all users adhere to federal and state regulations, including HIPAA, as well as internal SHS standards, and that the use of technology aligns with SHS's mission to provide exemplary patient care while preserving privacy and fostering trust.

Usage Privilege

Access to SHS systems is regarded as a privilege rather than an inherent right. By accessing SHS resources, users formally agree to continuously comply with this policy.

b. Definition of Technology Addressed

In relation to this policy, the following technology resources are covered:

- **Computers and Mobile Devices:** This includes all desktops, laptops, tablets, and smartphones that are owned, leased, or issued by SHS for clinical or administrative purposes.
- **Networks and Servers:** This encompasses SHS-managed wired and wireless networks, firewalls, routers, switches, and servers that host applications or store information.
- **Electronic Health Record (EHR) Systems:** This pertains to all platforms utilized for the documentation, transmission, or storage of patient health information, including medical imaging systems and specialty modules.

- **Email and Messaging Systems:** This includes SHS-issued email accounts, secure messaging applications, instant messaging, and approved collaboration platforms.
- **Cloud Services and Storage:** This refers to authorized third-party platforms employed to process, share, or store SHS data, including both patient and business information.
- **Peripheral Devices:** This includes printers, scanners, medical equipment with digital storage, and removable media (such as USB drives and external hard drives) that are permitted for use in SHS operations.
- **Other Connected Devices:** This encompasses any approved Internet of Things (IoT) devices, telehealth systems, or medical devices that are connected to the SHS network.

Any technologies not explicitly authorized by SHS, such as personal laptops and personal cloud storage accounts, are not covered under this policy and are prohibited from accessing SHS data or systems.

c. Responsibilities

To ensure the responsible utilization of technology and the safeguarding of sensitive data, the following delineation of roles and responsibilities is established.

The Executive Leadership is responsible for providing strategic oversight, allocating financial resources, and ensuring the organization’s adherence to security and compliance requirements. Within this framework, the Information Security Office (ISO) plays a crucial role in establishing security standards, monitoring system usage, investigating incidents, conducting risk assessments, and spearheading annual security awareness training initiatives.

The Information Technology (IT) Department is tasked with managing user accounts, granting and revoking access, maintaining system functionality, and implementing protective measures such as encryption, firewalls, intrusion detection systems, and backup protocols.

Managers and supervisors are mandated to ensure their teams adhere to security policies, escalate any violations or concerns, and foster a culture of accountability and responsible technology use within their respective departments. Data Owners from both clinical and administrative sectors are responsible for determining data classifications, establishing access rights, and ensuring that only authorized individuals are permitted to view or modify sensitive information. Compliance and Privacy Officers oversee adherence to HIPAA regulations and other relevant frameworks, offer guidance on the management of sensitive data, and coordinate privacy training sessions.

All authorized users must utilize SHS technology exclusively for approved work-related purposes. Users are expected to safeguard their login credentials by refraining from sharing usernames or passwords, logging out or locking devices when unattended, and promptly reporting any suspected security incidents, phishing attempts, or incidents involving lost or stolen devices. Furthermore, they must handle patient and organizational data with the utmost care, acknowledging that privacy constitutes a critical aspect of patient safety.

Every individual must recognize their role in safeguarding SHS's information systems. Failure to adhere to these responsibilities may result in disciplinary action, revocation of access, or legal consequences, equivalent to the severity of the violation.

2. Authorized Uses

a. User Access

Access to the information systems of the Sunshine Healthcare System (SHS) is regulated by the IT Department, in accordance with the principles of least privilege and need-to-know. Users are granted access solely to the systems and data essential for the execution of their designated job responsibilities. Each user possesses unique access credentials that must remain confidential and must not, under any circumstances, be disclosed to others. Access to systems is restricted to authorized working hours and approved devices, in compliance with SHS security standards. Remote access is permissible only through SHS-approved secure connections, including Virtual Private Networks (VPNs), which require multifactor authentication to ensure enhanced security.

b. Fair and Responsible Use

Authorized users of the SHS information systems are expected to utilize organizational resources exclusively to support patient care, research, education, administrative functions, and other legitimate business activities. It is important to safeguard against actions that may disrupt operations, such as downloading unauthorized software or accessing harmful websites. Users must ensure that all communications, documentation, and data entry conducted through SHS systems are accurate, professional, and respectful toward patients, colleagues, and business partners. Furthermore, any suspected security incidents, data breaches, or inappropriate use of technology resources must be reported immediately to the Information Security Officer (ISO) or the IT Help Desk. Adherence to all relevant SHS policies, including the Data Classification and Sensitive Data Management Policy, HIPAA Privacy and Security Rules, and applicable state regulations regarding patient information, is mandatory.

c. Protection of Privacy

Sunshine Healthcare System is committed to the confidentiality and privacy of all sensitive data accessed from its email systems, servers, and web applications, such as employee information, patient health information covered by HIPAA, and proprietary business or partner information. Access to this data is restricted to authorized personnel who need it to perform official job functions and is provided on a least privileged, need-to-know basis. The organization employs various controls such as encryption, firewalls, access controls, and real-time monitoring to safeguard sensitive information from disclosure, leakage, alteration, or destruction during transit, storage, or processing. All staff members are required to comply with Sunshine Healthcare Systems' Data Classification and Sensitive Data Management policies, which outlines the way data must be labeled, stored, and destroyed in adherence to federal, state, and industry regulations. Along with technical controls, employees need to be vigilant for phishing, illegal sharing, or handling of printed copies, and need to receive regular training in order to remain aware of best practices concerning privacy. By combining tight access control, regulatory guidelines compliance, and ongoing user accountability, Sunshine Healthcare System ensures the safety of sensitive information and patient, employee, and organizational trust.

3. Prohibited Uses

a. Disruptive Use or Misuse

All Authorized users are prohibited from using ALL company systems and web applications which include but are not limited to company servers, email systems, and websites, for purposes that are not directly tied to the business operations of Sunshine Healthcare System. Misuse includes visiting sites that are not related to work, unless access to such is needed to complete work-related tasks. This includes but is not limited to all social media sites, streaming platforms, and shopping sites. Company resources may not be accessed by anyone when the time is outside of normal business hours, unless prior approval is granted by the Information Security Department. Connecting personal devices or storing data from the company on unauthorized devices is prohibited. Employees are also required to and responsible for staying up to date on security awareness training in order to prevent accidental misuse. This can include but is not limited to clicking on phishing emails or accessing spoofed sites. Failure to maintain compliance with security awareness training will result in severely restricted access to all company systems and websites until the training has been completed.

b. Criminal Use

Sunshine Healthcare System has a zero-tolerance policy for the use of company servers, web applications, or emails for any purpose that is deemed illegal by state and federal law. Examples include but are not limited to attempts to access unauthorized information, intent to distribute malware, or use of any company resource to commit fraud. Any employee that is found to be engaging in illegal activities using company systems will be referred to law enforcement and prosecuted to the fullest extent of the law. Anyone accused of violating said policies will not receive any legal support from the organization.

c. Offensive or Harassing Materials

Sunshine Healthcare System is an equal opportunity/affirmative action agency and is committed to maintaining a professional and respectful working environment. Therefore, the use of company email, servers, or web applications to create, distribute, or view offensive, discriminatory, or harassing content is prohibited. Such activity depicting a hostile working environment shall be investigated through the appropriate compliance and HR office. Such violations shall be cause for disciplinary action including but not limited to suspension, termination, and potential legal proceedings.

d. Copyrighted, Licensed, or Other Intellectual Property

All users must adhere to copyrights, licenses, and intellectual property rights for software and digital content. It is strictly prohibited to install, copy, or distribute copyrighted or licensed material without permission using company systems in software applications, media files, or any other digital content not authorized for use by Sunshine Healthcare System. It is a violation of copyright and intellectual property law, and individuals who are in violation will be subject to disciplinary action and prosecution under U.S. Copyright Law and state law.

e. Other Restrictions

No employee shall share their login credentials or permit any other party, both internally and externally, to use their assigned account or workstation. Users shall not move company-owned servers or technologies without expressed prior approval from the IT department. Unauthorized movement, tampering, or borrowing of access shall void the organizational security and shall be taken seriously as a breach of this policy.

4. Systems Management

a. Management of Stored Materials

Sunshine Healthcare System enforces strict controls regarding the storage, protection, and handling of all information gained through company servers, email, and web applications. Highly sensitive information related to the organization and its patients is only allowed to be stored on approved network drives or designated cloud storage services that have been vetted and secured by the IT department. Employees are strictly prohibited from downloading, printing, or moving information to devices that include but are not limited to individual gadgets, USB devices, or other unauthorized storage devices. Hard copy documents, such as reports, are required to be securely stored at all times as part of compliance with the organization's Clean Desk Policy in order to prevent unauthorized access to company information. Data classification guidelines describe the methodologies for labeling, storage, and limiting materials, thus ensuring that sensitive information is properly protected. In addition, all individuals are required to comply with the organization's Information Retention and Disposal Policy, which details the amount of time for which the data is required to be held and the approved methods for its destruction. These requirements ensure Sunshine Healthcare System remains in compliance with healthcare legislation whilst maintaining the integrity and confidentiality of critical information assets.

b. Employer Monitoring

In order to protect its systems and data, Sunshine Healthcare System reserves the right to monitor all activities performed on its servers, mail systems, company devices, and web applications. This monitoring is conducted in order to detect cases where there is a policy breach, unauthorized usage, criminal conduct, presence of malware, and other security threats for the organization. When accessing these systems, all the employees and approved users give their consent for such monitoring, and it could include inspection of communication, transferring of files, and information storage. The oversight of monitoring activities is done through the IT department, ensuring the surveillance is carried out responsibly and consistently and according to the regulations of privacy and compliance. The purpose of this monitoring extends beyond the organizational infrastructure protection and also entails ensuring the privacy of the patient records, the safeguarding of sensitive business data, and the prevention of disruptions to organizational activities.

c. Virus Protection

Sunshine Healthcare System (SHS) enforces strict and regulated protocols to ensure the safety and integrity of its digital infrastructure. All SHS authorized users of the company's systems, that includes web applications, servers, email platforms, and any connected devices, are required to follow up-to-date malware protection. In addition to this information, all company devises must install operational malware protection technologies. Regularly update system to align with current threat detection standards. Any tampering with, altering, or removing malware software is strictly prohibited. This includes any and all attempts to bypass security protocols, and the uninstallation of protective software. These actions can lead to the massive risk of patient privacy, system functionality and organizational data loss.

d. Physical Security

For the protection of patient data, all information must be used in protected, authorized locations. As well of those who have access to that date must be authorized to do so. These authorized areas of sensitive materials must be stored in safes, locked cabinets, or in a digital cloud with data protection systems in place. Incident reporting will maintain proper and formal protection of data within Sunshine Healthcare System. Training and compliance are mandatory for all Sunshine Healthcare System employees. This includes proper onboarding training that goes beyond basic standards of physical data protection, hands-on training modules, annual refreshers for current employees, and emergency response drills that goes over the situation of potential attacks on date within the company. Here at Sunshine Healthcare System, continuous improvement is something we strive to achieve daily. So, within our company walls, proper security practices will be data-driven and constantly reviewed. Feedback from staff on how to improve physical security protocols as well as an analysis of incidents to inform updated policies and current up-to-date training.

e. Encryption

Purpose of encryption is to safeguard al physical and digital assets within our company, ensuring healthcare delivery, protection of patient data, medical records and technology, and organizational infrastructure to align with federal regulations and internal standards. As all these policies include everyone, only selected authorities have access to certain data and information. The use of keycards, biometric systems and use of physical keys to access information. These authorized personnel are allowed to transmit data associated with an external company, this always healthcare to send patient information to wherever it is needed. All transmissions must be approved by the organization, based on the DoD Advances Encryption Standards (AES). The process of encryption must be in line with organizational encryption policy as well, as that is a set of guidelines for how and when sensitive information should be encrypted to protect it from theft, loss, or unauthorized access.

5. Violations of Policy

a. Procedures for Reporting Violations

The first course of action is immediate action, REPORT IT IMMEDIATELY. Whether it is someone within the company, those actions are dealt with the proper consequences and will be taken care of in a timely manner. If an employee does not feel comfortable reporting an issue directly to management, anonymous reporting is a valid option. Anonymous reports can go the following URL: http://www.sunshinehealthcare.org/anonymous-policy-violation-reporting-form.html

All reports will go to Sunshine Healthcare System Office of Policy-Violation and Reporting, which are responsible for all reports the come in, investigations of these reports, ensuring confidentiality and protection of whistleblowers, and coordination with relevant departments for the proper solutions and steps to improvement

b. Penalties for Violations

Sunshine healthcare System takes pride in the protection of our data, patients and employees. Disciplinary actions will be taken depending on the salutation at hand. Any individual that is found in any violation of our policy, that includes tampering of data, breaking encryption standards, or unauthorized data transmission will be subject to the following disciplinary actions:

- Verbal warning
- Suspension of time
- Mandatory retraining
- Termination of employment

If actions were to go even further, regarding the evolution of criminal activity of anything stated previously. Local, state and/or Federal law enforcement will be called upon to handle the situation.

6. Policy Management

a. Scheduled Review of Policy

The Sunshine Healthcare System Office of Policy-management- and- Scheduled- Review-and-Revision is responsible for the following processes: Conducting yearly reviews of all physical and cloud data security policies, assessing policy effectiveness that is based on audit logs, incident reports and feedback from the staff, changes in technology, updates in government regulation on any level, and best practices in healthcare security and compliance are the goals in revising policies.

Shortly after the policy has been updated and revised, communications to staff will be initiated via email, updated training modules, and team meetings within a timely manner. Also, it will be integrated into new onboarding and in our annual compliance training.

b. Procedures for Modification

The Sunshine Healthcare System Office of Policy-management- and- Scheduled- Review-and-Revision will take in anonymous input from staff and faculty for policy improvements here at Sunshine Healthcare System. All inputs can be sent to the following link:

http://www.SunshineHealthcare.org/anonymous-policy-recommendations-for-revision-and-improvement.html

Our team will review and comment on inputs within 30 days of posting. This is not limited to anyone and is open to all departments and roles. Once an input has been rewvied and shows that it aligns with Sunshine Healthcare System's vision, it will be added to the revised policy and then set out on out Policy administration Site: http://www.SunshineHealthcare.org/policy-training-distribution-comprehension-understanding-and-enforcement.html

Which will then be followed by updated onboarding and our annual compliance trainning modules. Staff that are identified in Sections 1.a and 1.c will then complete any updated material for a yearly updated certificate on the brand-new policy that has been implemented.

7. Limitations of Liability

a. Statements of Liability

Sunshine Healthcare System aims to protect the organization and its stakeholders but set clear boundaries regarding liability. In cases where the Indvidual's commit criminal acts and/or violate security policies. Sunshine Healthcare System does not approve liability over those who commit or act in violating our policy or commit crimes to the organization resources, date or technology.

Furthermore, Sunshine Healthcare System will assist in the persecution of any individual who does go against policy and legal action will take place. This is for the protection of the organization and its stakeholders.

b. Other Disclaimers

Sunshine Healthcare System will provide the following general disclaimers to ensure transparency and adaptability. As policy is developed and in line with the current local, state and federal laws and regulations that is in governance with healthcare operations, data protection and physical security, Sunshine Healthcare System notices these changes and will review accordioning to make sure policies are up to date and need to make changes at any time with the proper procedures. Sunshine Healthcare Systemholds the right to make modifications, expand on existing policy or retire any part that the organization may see fits the current standards. Standards that align with organizational needs, technological advances, and stakeholder feedback.

References

HIPAA violations & enforcement. American Medical Association. (n.d.). https://www.ama-assn.org/practice-management/hipaa/hipaa-violations-enforcement

HIPAA encryption requirements - 2025 update. (n.d.-b). https://www.hipaajournal.com/hipaa-encryption-requirements/

Acceptable use policy policy . (n.d.-a). https://www.hcdpbc.org/ArticleDocuments/224/Acceptable%20Use%20Policy.pdf.aspx?Embed=Y

(OCR), O. for C. R. (2025, August 13). *HIPAA compliance and Enforcement*. HHS.gov. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html

Cristian Oana Full Bio. (2025, July 8). *9 types of organizational structures [+ visualization tips]*. Venngage. https://venngage.com/blog/organizational-structure/

OGC. (2025, March 18). *Limitation of liability and insurance policy limits: A risky business strategy*. Outside GC. https://www.outsidegc.com/blog/limitation-of-liability-and-insurance-policy-limits-a-risky-business-strategy