TABLE OF CONTENTS

Section **Page**

I. POLICY 2

II. AUTHORITY 2

III. SUPPORTIVE DATA 2

IV. SIGNATURE BLOCK WITH EFFECTIVE DATE 2

V. DEFINITIONS 2

VI. PROTOCOL 2

A. Outcome 2
B. Personnel 2
C. Competencies 3
D. Areas of Responsibility 3

VII. PROCEDURE 3

A. Control Access to SSNs 3
B. Protecting SSNs With Security Safeguards 4

VIII. DISTRIBUTION LIST 5

IX. HISTORY NOTES 5

I. Policy

The Florida Department of Health (Department) is committed to maintaining the privacy and confidentiality of Social Security numbers (SSNs). This is accomplished through proper restriction and monitoring. The intent of this policy is to define the procedures associated with managing access controls to which Department employees must adhere in order to ensure the collection, management, and display of SSNs.

II. Authority

A. Florida Administrative Code Rule 71A-1.006

B. Chapter 119, Florida Statutes

C. Public Law (PL) 93-579, Privacy Act of 1974

D. 45 Code of Federal Regulations (CFR), Parts 160 and 164

III. Supportive Data

A. Department of Health, Information Security and Privacy Policy, DOHP 50-10

IV. Signature Block with Effective Date

Jennifer Tschetter
Chief Operating Officer

10/09/15
Date

V. Definitions

A. **Department:** Use of the capitalized word Department shall be used to represent the Florida Department of Health throughout this policy

VI. Protocol

A. Outcome

Access control to SSN will only be administered per the procedures identified in this policy.

B. Personnel

This policy is applicable to all Department employees, contractors, students, volunteers, or anyone with access to Department employee or client records or applications.

C. Competencies

1. Knowledge of federal and state statutes, rules, and regulations related to the collection of SSNs
2. Knowledge of federal and state laws relating to the disclosure of Protected Health Information (PHI)
3. Knowledge of Florida Patient's Bill of Rights
4. Knowledge of the Department's Information Security and Privacy Policy
5. Knowledge of equipment and technology used to access and document electronic health records

D. Areas of Responsibility

1. This policy is applicable to all DOH employees, contractors, students, and volunteers.
2. The Information Security Manager is responsible for reviewing and maintaining this policy.

VII. Procedure

A. Control Access to SSNs

1. Limit access to records containing SSNs only to those employees with duties requiring that information for the performance of their duties.
2. Protect records containing SSNs, including back-ups, during storage by encrypting the numbers in electronic records or storing records in other media in locked areas.
3. Mask SSNs to only the last four digits in any electronic or paper based documentation utilized by the Department.
4. Do not store records containing SSNs on computers, laptops, tablets, mobile smart-phones or other electronic devices that are not password protected and encrypted using agency standard encryption technology.
5. Do not share SSNs with other entities except:
    a. As authorized by federal or state law or Florida Administrative Code
    b. As authorized through Interagency Agreement
    c. As approved by Department Internal Review Board

d. As approved by agency General Counsel

e. As authorized by the individual

6. Ensure that all Department systems and applications that store SSNs are compliant with Department security and confidentiality standards.

7. Division Directors, County Health Department Directors/Administrators, and Children's Medical Services Medical Directors, who have responsibility for employees who have access to Department systems applications which store SSNs, will:

a. Conduct quarterly review of all registered users with access to each system/application to:

i. Ensure all users are current and active.

ii. Ensure that all user's privileges and rights to personal identifiers are appropriate to their current role with the Department.

b. Incorporate as part of personnel actions taken when an employee separates from the Department, or changes jobs within the Department, that all access rights to Department systems outlined as a requirement of their job duties which contain SSNs is reviewed. The supervisor must ensure the removal of access within two working days for any employee whose role no longer requires access or who is no longer with the agency.

B. Protecting SSNs With Security Safeguards

1. Do not leave voicemail messages containing SSNs.

2. Do not fax documents containing SSNs.

3. Do not send text messages containing SSNs.

4. Encrypt all e-mails containing SSNs.

5. Promptly report any unauthorized or inappropriate disclosure or loss of records containing SSNs to your supervisor.

6. The discarding or destroying of documents containing SSNs must be accomplished in accordance with Department sanitization standards.

VIII. Distribution List

Chief of Staff

Deputies
Executive Office Directors
Division Directors
Bureau Chiefs
County Health Department Directors and Administrators
County Health Department Business Managers
County Health Department Medical Directors
County Health Department Nursing Directors
Children's Medical Services Medical Directors
Children's Medical Services Nursing Directors
Policy and Procedures Library
Webmaster
Web Managers

IX. History Notes

Original effective date of the Access Control of Social Security Numbers Policy is September 15, 2014. The Office of Information Technology is responsible for this policy.