SPECIAL DISTRICTS INSURANCE SERVICES
EMPLOYEE BENEFIT PLAN

HIPAA ELECTRONIC PROTECTED HEALTH INFORMATION SECURITY POLICIES

SPECIAL DISTRICTS INSURANCE SERVICES
EMPLOYEE BENEFIT PLAN

HIPAA ELECTRONIC PROTECTED HEALTH INFORMATION SECURITY RULE POLICY MANUAL

Table of Contents

Page

SPECIAL DISTRICTS INSURANCE SERVICES
EMPLOYEE BENEFIT PLAN

HIPAA HEALTH INFORMATION SECURITY POLICIES

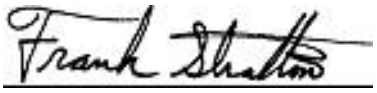
Preamble

WHEREAS, the Special Districts Insurance Services Employee Benefit Plan (the "Plan") is maintained for the benefit of eligible active and former employees; and

WHEREAS, the Plan has designated a Security Official to develop and implement policies with respect to protected health information maintained under the Plan, (the "Security Policies"), which Security Policies are designed to comply with the HIPAA Security Rule standards prescribed by federal regulations issued by the U.S. Department of Health and Human Services.

NOW, THEREFORE, in consideration of the foregoing, the Security Official hereby adopts the Security Policies prescribed herein, effective generally as of July 1, 2022.

SPECIAL DISTRICTS INSURANCE SERVICES
EMPLOYEE BENEFIT PLAN

By: 
Frank Stratton, Security Official

Dated: July 1st, 2022

PDX\126319\191678\WWM\16089539.1

ARTICLE 1

GENERAL

1.1 Purpose. Special Districts Insurance Services Trust ("SDIS"), on behalf of the Special District Insurance Services Employee Benefit Plan (the "Plan"), performs or assists in the performance of a function or activity involving the use or disclosure of an individual's Protected Health Information. The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations require that SDIS implement policies and procedures to safeguard the confidentiality, integrity and availability of such health information that is transmitted or maintained by SDIS in electronic form. The purpose of these security policies (the "Security Policies") is to facilitate the compliance with the health information security standards of HIPAA.

1.2 Scope of Security Policies. To the extent these Security Policies establish requirements and obligations above and beyond those required by HIPAA, the Security Policies will not be binding upon SDIS. These Security Policies do not address any obligations prescribed under other federal or state laws.

1.3 Hybrid Plan Safeguards. The Plan is a hybrid plan consisting of Health Care Components and benefit programs that are not Health Care Components. The benefit programs that are not Health Care Components are not subject to these Privacy Policies.

1.4 No Third-Party Rights. No third-party rights (including, but not limited to, rights of individuals covered under a health plan) are intended to be created by these Security Policies.

1.5 Security Official. SDIS has appointed a Security Official (the "Security Official" to undertake responsibility for the development and implementation of policies and procedures relating to the Security Rules.

1.6 Amendment. The Security Official may, at any time or from time to time, amend these Security Policies in whole or in part. Any amendment of these Security Policies will be effectuated by a written instrument signed by the Security Official.

1.7 Document Retention. The Security Official will maintain the Security Policies, as may be amended from time to time, in written or in electronic form. The documentation will be maintained for no less than six years from the date the document was created or the date when it was last in effect, whichever is later.

1.8 Effective Date. The provisions of these Security Policies as herein stated will be effective as of June 1, 2015, except as may be specifically provided otherwise.

ARTICLE 2

DEFINITIONS

When used in these Security Policies, certain terms have the respective meanings set forth in this Article, or in certain other Articles of these policies.

Business Associate. "Business Associate" means an organization or a person (other than a Workforce Member) who on behalf of the Plan performs or assists in the performance of a function or activity involving the use or disclosure of PHI.

Electronic Protected Health Information ("e-PHI"). "Electronic Protected Health Information" or "e-PHI" means Protected Health Information that is transmitted or maintained in electronic media, except as otherwise prescribed under the Security Rules.

Health Care Components. "Health Care Components" mean a benefit program maintained as part of the Plan that provides medical care to employees or their dependents, either directly or through insurance.

HIPAA. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996.

HIPAA Privacy Rules. "HIPAA Privacy Rules" mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.

Individual Identifiable Health Information. "Individual Identifiable Health Information" means information with respect to any covered individual that is a subset of health information, including demographic information collected from a covered individual, that:

(a) Is created or received by the Plan;

(a) Relates to the past, present, or future physical or mental health or condition of the covered Individual, the provision of health care to the covered Individual, or the past, present or future payment for the provision of health care to the covered Individual; and

(b) Identifies the covered Individual, or for which there is a reasonable basis to believe the information can be used to identify the covered Individual.

Plan. "Plan" means the Special Districts Insurance Services Employee Benefit Plan.

Protected Health Information. "Protected Health Information" means Individually Identifiable Health Information that is:

(a) Transmitted by electronic media;

(b) Maintained in electronic media; or

(c) Transmitted or maintained in any other form or medium.

SDIS. "SDIS" means the Special Districts Insurance Services Trust.

Security Incident. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system through which e-PHI is transmitted or maintained.

Security Official. "Security Official" means the person appointed by SDIS to undertake responsibility for the development and implementation of policies and procedures required by the Security Rules.

Security Policies. "Security Policies" means the health information security policies and procedures applicable to a Plan, as set forth in this document.

Security Rule. "Security Rule" means the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Part 160 and Part 164, Subparts A and C.

Workforce Member. A "Workforce Member" means any employee, volunteer, or trainee whose work performance is under the direct control of SDIS, whether or not the person is paid by SDIS, and whose duties and responsibilities necessitate access to PHI created or received under a Plan.

Workstation. "Workstation" means any electronic computing device, including a laptop or desk computer.

ARTICLE 3

ADMINISTRATIVE POLICIES

3.1 Security Awareness and Training Program. All Workforce Members with access to e-PHI will receive training as to their responsibilities to maintain the confidentiality and security of e-PHI. The training will be coordinated by the Security Official. The education and training will include information regarding the following topics:

(a) Overall discussion of threats and vulnerabilities specific to e-PHI;

(b) Information access control;

(c) Personnel clearance;

(d) Security Incident reporting;

(e) Viruses and other forms of malicious software;

(f) User log-in; and

(g) Password maintenance.

3.2 Risk Analysis and Management. An accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of e-PHI held by the Plan has been performed. The Security Official will cause an evaluation of all aspects of the e-PHI security safeguards to be periodically performed.

3.3 Review and Evaluation. The Security Official will cause a technical and nontechnical evaluation of all aspects of the e-PHI security safeguards to be periodically performed so as to address any environmental or operational changes affecting the security of e-PHI.

3.4 Information Access Management. Access to e-PHI will be restricted through the use of a unique user identifier password and other appropriate safeguards to ensure that e-PHI is available only by Workforce Members having the need for such.

3.5 Contingency Plans. The Security Official will assess the relative criticality of the e-PHI that it maintains. In the event that the possession of any such e-PHI is critical and cannot be readily retrieved from another source, then the Security Official will, to the extent warranted, establish procedures to respond to an emergency or other occurrence that damages SDIS's information systems containing the critical e-PHI that is otherwise not readily retrievable from another source. These procedures include those prescribed below.

(a) Data Backup Plan. Any critical e-PHI on SDIS's information systems will be backed up at regular intervals.

(b) Disaster Recovery Plan. The disaster recovery plan that applies to operations of SDIS in general will include the recovery of any lost critical e-PHI data.

(c) Emergency Mode Operation. In the event of a disaster or emergency situation, the Security Official will work with employees of SDIS to:

(i) Maintain the physical security of information systems containing accessible e-PHI; and

(ii) Coordinate efforts to restore any lost data.

(d) Evaluation. The Security Official will, on a regular basis, conduct a procedural evaluation that establishes the extent to which the contingency plans remain adequate.

3.6 Workforce Security. The Security Official will be responsible for ensuring that Workforce Members with a need for e-PHI have appropriate access to such e-PHI, and for preventing employees who do not have access from obtaining access to e-PHI. Toward this end, the Security Official will:

(a) Be responsible for the authorization and supervision of Workforce Members who work with e-PHI or the locations where such e-PHI might be accessed; and

(b) Determine whether a Workforce Member has a need for access to e-PHI.

3.7 Termination Procedures. The Security Official will implement procedures for terminating a Workforce Member's access to e-PHI when the need for such e-PHI, or the Workforce Member's employment or services to the Plan, ends.

3.8 Reporting of Security Incidents. Any Security Incident that comes to the attention of a Workforce Member having access to e-PHI will be promptly reported to the Security Official.

3.9 Sanctions for Violations of Security Policies. All Workforce Members who have access to e-PHI must comply with the Plan's Security Policies. Sanctions for using or disclosing e-PHI in violation of these Security Policies will be imposed in accordance with SDIS's personnel policies up to and including termination. The nature, severity and repetition of the offense will all be factors in establishing the sanctions. Any discipline will be documented and copies will be kept in the Workforce Member's personnel file.

ARTICLE 4

PHYSICAL SAFEGUARDS

4.1 Facility Access Control. The working locations of Workforce Members that have access to e-PHI will be segregated to the extent possible so as to appropriately restrict the physical access to e-PHI.

4.2 Workstation Use. SDIS will, to the extent reasonable, place and position working locations to only allow viewing of e-PHI by authorized individuals. In addition, the following policies will apply:

(a) Workforce Members with access to e-PHI should not share their Workstations with other individuals who are not authorized to access e-PHI;

(b) Workforce Members with access to e-PHI should be conscious of the placement of their Workstation monitor and try to minimize the screen being seen by other employees and visitors; and

(c) Workforce Members with access to e-PHI are encouraged to use computer privacy screens which make on-screen data visible only to persons directly in front of the monitor.

4.3 Workstation Security. Network access to e-PHI will require a unique identifier and password so as to restrict access to authorized users.

4.4 Device and Media Controls.

(a) The Security Official will be responsible for the proper disposal of all computer hardware and software installed on Workstations containing e-PHI.

(b) If Workstations are transferred from a Workforce Member with access to e-PHI to a Workforce Member or other individual not having a need to access, the e-PHI will be retrieved before the Workstation is moved.

4.5 Data Back-up and Storage. If appropriate, a retrievable copy of e-PHI should be created before the movement of equipment.

ARTICLE 5

TECHNICAL SAFEGUARDS

5.1 Access Control. Each Workforce Member with access to e-PHI will be assigned a unique identifier for identifying and tracking user identity.

5.2 Emergency Access. The Emergency Mode Operation policy referenced in Section 3.5(c) includes procedures for accessing e-PHI during an emergency.

5.3 Audit Control. The information systems of SDIS that are used to transmit or maintain e-PHI will include mechanisms to examine and record the e-PHI activity in such systems.

5.4 Authentication. Each Workforce Member with access to e-PHI will require a unique identifier and password as a means to verify the employee's authorization.

5.5 Other Measures to be Addressed. The Security Official will evaluate the need for the following measures on a periodic basis:

(a) Electronic procedures that terminate an electronic session after a pre-determined time of inactivity;

(b) A mechanism to encrypt and decrypt e-PHI;

(c) Electronic mechanisms to corroborate that e-PHI has not been altered or destroyed in an unauthorized manner; and

(d) Mechanisms to ensure that electronically transmitted e-PHI is not improperly modified without detection until it is disposed.

ARTICLE 6

ORGANIZATIONAL REQUIREMENTS

6.1 Disclosures to Business Associates. The Plan and Workforce Members with access to e-PHI may not disclose e-PHI to any Business Associate in the absence of a written contract assuring that the Business Associate shall:

(a) Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the e-PHI;

(b) Ensure that any agent, including a subcontractor, that creates, receives, maintains or transmits e-PHI on behalf of the Business Associate agrees pursuant to a written contract or other written arrangement to comply with the Security Rule to protect it;

(c) Report to the Security Official any Security Incident of which it becomes aware; and

(d) Authorize termination of the contract by the Plan if the Security Official determines that the Business Associate has violated a material Security Rule provision of the contract.

6.2 Plan Document. The Plan shall be amended to require SDIS to:

(a) Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the e-PHI that it creates, receives, maintains or transmits on behalf of the Plan.

(b) Ensure that Workforce Members with a need to access e-PHI are supported by reasonable and appropriate security measures;

(c) Ensure that any agent, including a subcontractor, to whom it provides e-PHI agrees to implement reasonable and appropriate security measures to protect the information; and

(d) Report to the Security Official any Security Incident of which it becomes aware.

6.3 Documentation Standard. The Security Policies, as may be amended from time to time, shall be maintained in written or in electronic form. The documentation shall be maintained for no less than six years from the date the document was created or the date when it was last in effect, whichever is later. The documentation shall be made available to the Workforce Members responsible for implementing the procedures to which the documentation pertains.