Protecting the Confidentiality of Social Security Numbers

Status: Published

Origination Date: 06/07, 09/10, 3/14

Effective Date: 6/2007

Next Review: 3/2017

Introduction

This is an OPTIONAL section. Include a brief description of the purpose and/or other background topics related to the Policy. This section would typically be 1 to 2 sentences.

Definitions

Duke Health Enterprise (DHE)

The Duke Health Enterprise includes Duke's Affiliated Covered Entity and the Organized Health Care Arrangement that covers the following entities: Duke University Health System, Duke University Hospital, Duke Regional Hospital, Duke Raleigh Hospital and corresponding medical staffs, Duke University Affiliated Physicians (aka Duke Primary Care), Private Diagnostic Clinic, PLLC, Duke Home Care and Hospice, Duke Connected Care, Associated Health Services, Inc., (dba Davis Ambulatory Surgical Center), Patient Revenue Management Organization, LLC, Duke University School of Medicine, Duke University School of Nursing, Duke Clinical Research Institute, Sexual Assault Support Services, Personal Assistant Services, Counseling and Psychological Services (CAPS), Duke University Student Health, Duke University Police Department, and Live for Life.

Duke Medicine

The clinical settings (hospitals, clinics and community-based care of Duke University Health System), billing operations (Patient Revenue Management Organization, LLC) and the academic and research entities (School of Medicine and School of Nursing) as well as the Private Diagnostic Clinic, PLLC.

Encryption

The use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key.

Identifying Information

Includes the following:

1. Social security or employer taxpayer identification numbers
2. Driver's license, State identification card, or passport numbers
3. Checking account numbers
4. Savings account numbers
5. Credit card numbers
6. Debit card numbers
7. Personal Identification (PIN) Code which is a numeric and/or alphabetical code assigned to the cardholder of a financial transaction card by the issuer to permit authorized electronic use of that financial transaction card. (NCGS § 14-113.8(6))
8. Electronic Identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names
9. Digital signatures
10. Any other numbers or information that can be used to access a person's financial resources
11. Biometric data
12. Fingerprints

13. Passwords
14. Parent's legal surname prior to marriage

Person

Any individual, partnership, corporation (includes both for-profit and non-profit), trust, estate, cooperative, association, government, or governmental subdivision or agency, or other entity.

Personal Information

A person's first name or first initial and last name in combination with identifying information as defined above. Personal information does not include a publicly available directory containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address, and telephone number, and does not include information made lawfully available to the general public from federal, state, or local government records.

Protected Health Information (PHI)

For purposes of this policy, PHI includes: 1. Individually identifiable health information in any form (paper, electronic, oral) that is transmitted and/or stored by DHE or a business associate that relates to the past, present, or future health of an individual, provision of health care, or payment for health care that is linked to a patient; or 2. Identifying or Personal Information, as defined in Federal Trade Commission's Red Flags Rules or the NC Identity Theft Protection Act of 2006 regulations, including any name or number that may be used in conjunction with any other information to identify a specific person, e.g. social security number, credit card number or passwords.

Records

Any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.

Required Resources

This is an OPTIONAL section. This section lists equipment and supplies necessary to perform procedures or activities. Forms, agreements, equipment, supplies, etc…

Policy

Duke Medicine has procedures in place to protect the confidential nature of social security numbers ("SSNs") without creating unjustified obstacles to the conduct of the business of Duke Medicine and the provision of services to its many constituencies. This policy is consistent with the North Carolina Identity Theft Protection Act of 2005 which requires businesses to take measures to protect against unauthorized access or use of personal information. This policy addresses the specific mandates within the North Carolina Identity Theft Protection Act to protect an individual's SSN.

Nothing in this policy is intended to prohibit or restrict the collection, use, and maintenance of SSNs as required by applicable law.

Procedure

A. Reduce Use and Collection of Social Security Numbers

1. The use of the SSN as an individual's primary identification number is not to be used unless required or permitted by law. The SSN may be stored as a confidential attribute associated with an individual and used to verify identity.
2. If the collection and use of SSN is permitted, but not required by applicable law, the SSN will only be used and collected as reasonably necessary for the proper administration or accomplishment of Duke Medicine business, educational and medical purposes, including but not limited to:
    a. As a means of identifying an individual for whom another form of unique identification is not known
    b. For internal verification or administrative purposes

c. As a secondary identifier if other identification is questionable

3. Except in those instances in which an entity is legally required to collect the SSN, an individual shall not be required to disclose his or her SSN, nor shall the individual be denied access to services if the individual refuses to disclose his or her SSN.

4. Unique identifiers for each patient, employee, insured dependent, research subject, donor, contractor, student, volunteer or other individuals who become associated with Duke Medicine will be assigned at the earliest possible point of contact. The unique identifier will be used in all future electronic and paper data systems to identify, track and serve individuals.

5. In order to collect, store, or use SSNs, electronically or on paper, the Department must receive prior authorization. Approval Requests are submitted to the Information Security Office at: https://www.iso.duke.edu/iso/isop/infosec.php. Requests are reviewed and approved by the Duke University Health System Compliance Office, Duke Medicine Information Security Office and Chief Information Officer. Information Security Office submits the systems' SSN inventory to the Duke University Executive Vice President annually.

B. Reduce Public Display of Social Security Numbers Text

1. The display of the SSN will be redacted to the last four digits in the electronic medical record. The full SSN should only be displayed for use or disclosures that are required for treatment, payment or healthcare operations or when required by law. For those systems that display the full number, these will be redacted to the last four digits as soon as the system has the ability to do so.

2. Social security numbers will not be printed on materials mailed to individuals unless required by law. If an entity is required by law to send materials containing SSNs through the mail, it shall take reasonable steps to place the SSN on the document so as not to reveal the SSN in an envelope window. Duke Medicine will not print or cause an individual's SSN to be printed on a card or other device required to access products or services provided by or through Duke Medicine.

3. Transmission of data, either electronically, by fax, or text paging, will be done only in accordance with the Duke Medicine Information Security policies (including but not limited to Electronic Communications and Mobile Computing and Storage Devices) and Information Security Standards. SSNs will not be sent over the Internet unless the connection is secure and only when required for treatment, payment, healthcare operations, formally authorized research or when required by law. Exceptions from these standards must be requested through the Information Security Office, approved by the Chief Information Officer, and recorded in the Information Security Operations Plan (ISOP) system.

C. Control Access to Social Security Numbers

1. Duke Medicine procedures limit access to records containing SSNs to those individuals who need to see the number for the performance of their job responsibilities. If it is determined that an individual requires access to SSNs, then the Manager should submit the request to Duke Health Technology Solutions (DHTS) Help Desk by calling 919-684-2243 or by visiting their website at http://dhts.duke.edu/modules/dhts_home/index.php?id=3.

2. Duke Medicine will monitor and control access to records containing SSNs by the use of appropriate measures as reasonably determined by each entity within Duke Medicine.

3. Duke Medicine will protect the security of records containing SSNs during storage using physical and technical safeguards (such safeguards may include encrypting electronic records, redacting display of the number to the last four and locking physical files) as outlined in the Duke Medicine Security Standards.

4. Access to paper records containing SSNs should be protected by key or card access. Paper records in transit should never be left unattended.

5. SSNs will not be shared with third parties except:

a. As required or permitted by law
b. With the consent of the individual
c. When the third party is an agent or contractor with Duke Medicine or one of its entities

6. Before SSNs are shared with a third party that is an agent or contractor for Duke Medicine or one of its entities, a written agreement including Data Security Agreement and as appropriate Business Associate Agreement must be executed. The written agreement will prohibit the third party from disclosing the SSN, except as required or permitted by law, and require the third party to use adequate safeguards to protect the confidentiality of records or systems containing SSNs.

D. Disposal of Information Containing Social Security Numbers

1. Any data that contains SSNs shall be properly shredded or otherwise destroyed prior to disposal in accordance with the DUHS Policy on Retention, Preservation and Destruction of Records.

2. Disposal of any computers or devices that contain records with SSNs must be done in accordance with the Information Security Standards on Media Control.

E. Reports of Inappropriate Access, Use or Release of Social Security Numbers

1. If an individual becomes aware of inappropriate access, use or release of SSNs, s/he should follow appropriate entity procedures for reporting. Entity procedures should be consistent with reporting requirements outlined in the DUHS Compliance Reporting (Non-Retaliation/Non-Retribution) and Security Breach policies. For any inappropriate access, use or release of SSNs, the involved person(s) will be subject to disciplinary action in accordance with the DUHS Breach of Protected Health Information/Patient Privacy Policy.

2. The DUHS Security Breach Policy outlines the requirements for reporting to those individuals whose SSN may have been breached and for alerting government agencies where required.

References

DUHS Compliance Reporting (Non-Retaliation/Non-Retribution)

DUHS Security Breach Policy

DUHS Breach of Protected Health Information/Patient Privacy

DUHS Electronic Communications

DUHS Policy on Record Retention, Preservation & Destruction

Duke Human Resources Policies and Duke Staff Handbook - Workplace Expectations & Guidelines: Confidentiality, Safety and Use of Duke Property

Duke Medicine Information Security Policy: Mobile Computing and Storage Devices

Duke Medicine Security Standards

Applicable Standards

NC Identity Theft Protection Act

Owner:	DUHS Chief Compliance Officer, Duke Medicine Social Security Workgroup
Category:	<One of the following: Administrative | Clinical | Environmental>
Domain:	<One of the following: Finance | Human Resources | Information Technology | Labs | Nursing | Research | Safety>
Application:	All Duke Medicine Entities
Audience:	All Duke Medicine Workforce