
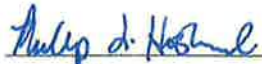


DC | HEALTH

District of Columbia Department of Health <h2>Electronic Signature</h2>		PROCEDURE 760.000 Implementing Office: Office of the Director/Office of Information Technology Training Required: Yes Originally Issued: Revised/Reviewed:
Approved by:  LaQuandra S. Nesbitt MD, MPH; Agency Director	Review by Legal Counsel:  Phillip Husband, Esq.; General Counsel	Effective Date: FEB 25 2021 Valid Through Date: FEB 25 2024

I. Authority	Reorganization Plan No. 4 of 1996; Mayor's Order 1997-42; Mayor's Order 2009-118.
II. Reason for the Policy	The District of Columbia Department of Health ("DC Health" or "the Department") serves a wide range of internal and external customers. As technology has improved, and as customer expectations continually evolve, the operational need for electronic signature has grown, and is projected to continue growing. A protocol is necessary ensure that DC Health electronic signature processes meet the nine criteria recommended by the National Archives and Records Administration, and reiterated in Mayor's Order 2009-118.
III. Applicability	This policy applies to all Department of Health (DC Health) employees, contract employees, volunteers, interns, summer youth employees, and federal employees assigned to the District government (collectively referred to herein as "employees" or "DC Health employees").
IV. Policy Statement	<p>Managing electronic signature is part of the portfolio of the DC Health Office of Information Technology (DC Health IT). The Chief Information Technology Officer (CITO) is the accountable manager over this office</p> <p>All electronic signature features on all information technology (IT) applications the Department uses must be pre-approved by the CITO before they may be implemented. This includes applications</p>

	<p>DC Health builds internally, as well as applications purchased or licensed from a third party.</p> <p>In every instance of electronic signature used in a DC Health application, the CITO, or designee, will evaluate it based upon the nine criteria recommended by the National Archives and Records Administration, and reiterated in Mayor's Order 2009-118:</p> <ol style="list-style-type: none">1. Reliability: record can be trusted as a full and accurate representation of the transaction, activities, or facts to which it attests and can be depended upon in the course of subsequent transactions or events.2. Authenticity: a record proven to be what it claims to be and to have been created or sent by the person who claims to have created and sent it; assurance of identity.3. Integrity: proof that a record is complete and has not been altered.4. Usability: a record can be located, retrieved, presented, and interpreted in connection with the business transaction that created it.5. Signature intent: the process used to obtain the electronic signature must demonstrate that the user intended to sign the record. Establishing intent includes:<ol style="list-style-type: none">a. Identifying the purpose for signing the electronic record (could be apparent within the content of the transaction);b. Being reasonably certain the signer knows which record is being signed; andc. Providing notice to the signer that their electronic signature is about to be applied to, or associated with, the electronic record (such as an online notice advising the signer that continuing with the process will result in an electronic signature).6. Trustworthiness of the process: The process used to conduct transactions must be documented, such as in a formal procedure, and followed consistently.7. Trustworthiness of the system:<ol style="list-style-type: none">a. Consistent: the system processes information in a manner that assures the records they create are credible;b. Complete: contains the content, structure, and context generated by the transaction they document;
--	---

	<ul style="list-style-type: none"> c. Accurate: quality controlled at input to ensure the information in the system correctly reflects what was communicated in the transaction; and d. Preserved: continue to reflect content, structure, and context within any system by which the records are retained over time. <p>8. State agencies shall maintain adequate documentation of the system design, implementation, use, and migration. The documentation shall include a narrative description of the system, physical and technical characteristics, and any other technical information required to access or process the records.</p> <p>9. Non-repudiation: a property that reflects against an individual or entity from denying having performed a certain action, related to the data. Non-repudiation services protect the reliability, authenticity, integrity, usability, confidentiality, and legitimate use of electronically-signed information. Essential elements of a non-repudiation model include:</p> <ul style="list-style-type: none"> a. Evidence of the origin of the message b. Evidence of being sent c. Evidence of being received d. Timestamp, as needed, by the agency of origin e. Long-term storage of the evidence f. Designated adjudicator of prospective disputes <p>The CITO, or designee, will include the evaluation in the security assessment of an application in accordance with directives from the District of Columbia Office of the Chief Technology Officer (OCTO).</p> <p>This SOP, and subsequent revisions, are subject to approval from the District of Columbia Office of the Secretary prior to implementation.</p> <p>Any employee not in compliance with any part of this SOP may be subject to commensurate disciplinary action.</p>
<p>IV. Definitions & Acronyms</p>	<p>CITO: Chief Information Technology Officer. The DC Health manager who oversees DC Health IT</p> <p>DC Health IT: The DC Health Office of Information Technology</p>

Electronic Signature: A basic term for a variety of methods used as an alternative to a traditional ink signature on paper. Three basic classifications of electronic signatures exist, each with an increased level of cost, integrity, authenticity, security, and non-repudiation:

1. **Common Electronic Signatures:** Common electronic signatures are any signature method that does not employ a specific technology to increase the security, authenticity, or evidentiary value of a signature. Common electronic signatures include a digitized image of a handwritten signature, a password or PIN (Personal Identification Number), "click-wrap" signature method where the user clicks a button onscreen to accept what is being stated, or a mark or symbol indicating intent to sign.
2. **Secure Electronic Signatures:** Secure electronic signatures typically use technology to link the electronic signature to an individual or device. Secure electronic signatures may use biometric, biorhythmic, holographic and cryptographic technology
 - a. **Biometric Signature:** the automatic identification of a person based upon their physical characteristics, such as a thumbprint or retinal scan.
 - b. **Biorhythmic Signature:** the comparison of physical signature characteristics, typically speed and pressure of the stroke, to a previously provided and stored sample.
 - c. **Holographic Signature:** a physical likeness of a signature, applied electronically and bound to the content via cryptographic technology.
 - d. **Cryptography:** the science of mapping readable text, called plaintext, into an unreadable format through encryption, and back into readable text through decryption. This process affects the appearance of the data, without altering its content.
3. **Digital Signatures:** The digital signature process, in conjunction with a digital certificate, uses a private key to sign and encrypt the document and a public key to de-crypt and authenticate the signature. Digital signatures are typically used by a trusted third party that verifies facts about your identity and issues a certificate that attests to those facts. Digital signatures offer the highest level of

DC | HEALTH

	<p>authenticity, security, and integrity and issues a certificate that attests to those facts.</p> <p>OCTO: District of Columbia Office of the Chief Technology Officer</p>
VI. Procedures	None
VII. Contacts	Chief Information Technology Officer
VIII. Related Documents, Forms and Tools	None