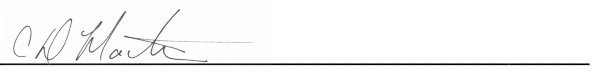
HARRIS COMPUTER SYSTEMS

Corporate Policy Definitions

Corporate Officer: Dwayne Martin, Vice President of Corporate IT

Signature: 

REVISION

Rev	Date	Author	Type	Description	Approval
1.0	3/31/2021	Katie Rose	Major	Initial version of document.	Dwayne Martin

PURPOSE:

Harris Computer Systems (Harris or Company) maintains an Information Security Management Program to ensure the confidentiality, integrity and availability of its systems and information. The purpose of this document is to define key terms used in the Information Security Management Program and associated policies.

DEFINITIONS:

1. Breach means the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of the PHI. For purposes of this definition, compromises the security or privacy of the PHI means poses a significant risk of financial, reputational, or other harm to the individual(s) who is(are) the subject of the PHI. An unauthorized acquisition, access, use or disclosure of PHI is presumed to be a breach unless it can be demonstrated that there is a low probability that the PHI has been compromised based on a risk assessment of the following factors:
    a) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

b) The unauthorized person who used the PHI or to whom the disclosure was made;

c) Whether the PHI was actually acquired or viewed; and

d) The extent to which the risk to the PHI has been mitigated.

2. Business Associate means an entity which, on behalf of a Covered Entity or an organized health care arrangement in which the Covered Entity participates, but other than in the capacity of a Workforce Member of such Covered Entity or arrangement, creates, receives, maintains, or transmits protected health information to perform a function or activity of the Covered Entity.

3. Covered Entity means a health plan, healthcare clearinghouse or a health care provider (all as defined by 45 C.F.R. §160.103) who transmits any health information in electronic form in connection with a transaction covered by the transaction and code set rule under the Administrative Simplification Provisions of HIPAA.

4. Data Incident means any suspected or actual impermissible use or disclosure, Security Incident, Breach of PHI, or breach of Personal Information as defined by state law. Examples of Data Incidents include, but are not limited to: loss of service, equipment or facilities, system malfunctions or overloads, human errors, non-compliance with policies or guidelines, breaches of physical security arrangements, uncontrolled system changes, malfunctions or software or hardware, access violations and breaches of confidentiality and integrity of information.

5. Director of Compliance is the Company official for regulatory compliance across the Company including compliance for information security assets and activities as required by law.

6. Electronic Protected Health Information (ePHI) is PHI that is produced, saved, transferred or received in an electronic form and therefore covered under HIPAA security regulations.

7. Governance, Risk and Compliance Committee (GRCC) is a committee that provides oversight to ensure the security and privacy of Company information. Members of the committee includes Senior Legal Counsel, the Corporate Privacy Officer, the Director of Compliance and the Information Security Officer.

8. Information Owner is the organization official with statutory or operational authority for specified information and is responsible for establishing the controls for information generation, collection, processing, dissemination and disposal.

9. Information System Owner is the organization official responsible for the overall procurement, development, integration, modification, operation and maintenance of the information system.

10. Minimum Necessary shall have the meaning given to such term as 45 CFR §164.502(b) and 45 CFR §164.514(d). The minimum necessary standard requires covered entities and business associates of a covered entities that uses and discloses PHI or when it requests PHI from another covered entity or business associate to make reasonable efforts to limit PHI to accomplish the intended purpose of the use, disclosure or request and to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information.

11. Personally Identifiable Information (PII) is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual.

12. Privacy Officer is the organization official for privacy compliance across the organization, including privacy compliance measures that apply to information security assets and activities.

13. Protected Health Information ("PHI") is information (whether oral or recorded in any form or medium) that is:
    a. created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse that relates to –
        i. the past, present, or future physical or mental health or condition of any individual,
        ii. the provision of health care to an individual, or
        iii. the past, present, or future payment for the provision of health care to an individual,

    b. identifies the individual; or there is a reasonable basis to believe the information can be used to identify the individual, and

    c. transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium.

Protected Health Information is covered under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy regulations.

14. The Secretary means the Secretary of the U.S. Department of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.

15. Security Incident means:

    a) Any attempted or successful unauthorized access to the Company's computer network or information systems, specifically excepting "pings."

    b) Any attempted or successful interference with the normal operations of the Company's computer network or information systems.

    c) The unauthorized access, interception, alteration, use, disclosure, or deletion of Electronic Protected Health Information ("ePHI"), whether secured or unsecured.

16. Security Officer is the Company official responsible for serving as the VP of IT's primary liaison to the Company's Information Owners and Information System Owners for compliance of the security program across the organization, including security compliance measures that apply to information security assets and activities.

17. Sensitive Information is defined as any information that is protected against unwarranted disclosure including but not limited to PHI, ePHI or PII. Access to sensitive information should be safeguarded. Protection of sensitive information may be required for legal or ethical reasons, for issues pertaining to personal privacy, or for proprietary considerations.

18. Subcontractor means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a Workforce Member of such business associate.

19. Third Party Vendor is a separate individual or organization that provides a product or service (not supplied by Harris) to Harris or to a Harris end user with whom PHI, ePHI or other sensitive data is being shared.

20. Unsecured PHI is PHI that is not secured through the use of a technology or methodology identified by the Secretary to render the PHI unusable, unreadable

and undecipherable to unauthorized users.[1] Unsecured Protected Health Information may be in written, oral, or electronic form.

21. User means a person or entity with authorized access.

22. Vice President of Information Technology (VP of IT) is the organization official responsible for ensuring the development, maintenance and implementation of an organization-wide information security program.

23. Workforce Member means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

24. Workstation means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.