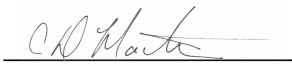
HARRIS COMPUTER SYSTEMS

CORPORATE DATA INCIDENT POLICY

Corporate Officer: Dwayne Martin, Vice President of CIT

Signature: 

REVISION

Rev	Date	Author	Type	Description	Approval
1.0	08/22/16	Gina Martin/Katie Rose	Major	Initial version of policy.	Todd Richardson
1.1	10/22/18	Katie Rose	Minor	Annual Review	Dwayne Martin
1.2	3/25/2020 *2019 review waived as approval for 2018 review cycle completed end of Q1 2019	Katie Rose	Minor	Annual Review	Dwayne Martin
1.3	3/24/2021	Katie Rose	Minor	Annual Review, Added Definitions Document	Dwayne Martin

SCOPE

This policy applies to Data Incidents as defined below. This policy applies to all Workforce Members of Harris Computer Systems (Harris), contract employees, as well as subcontractors. Any violation by a Workforce Member of this policy or associated policies and procedures will be grounds for disciplinary action up to, and including, termination of employment. The Corporate Incident Response Plan should be referenced and followed as appropriate.

POLICY

1. All Workforce Members, contractors and subcontractors must report any information regarding Data Incidents as quickly as possible to the Security Officer (Security_Officer@harriscomputer.com) or the Privacy Officer (Privacy_Officer@harriscomputer.com). If the Security Officer or the Privacy Officer is not available, the individual shall report the issue to the Vice President of CIT or General Counsel or their designee. Workforce Members are made aware of their responsibilities during training and as set forth in the procedure below.

2. Harris will identify and respond to suspected or actual Data Incidents that are known to the company, determine root cause, mitigate, if possible, any harmful effects of the Data Incident, and document the Data Incident and its resolution.

3. Data Incidents will be quickly analyzed to determine the level of risk and potential harm and to determine the level of response and are tracked appropriately.

4. Harris will provide notification of any Breach of Unsecured PHI, PII or other Sensitive Information as required by law. Further, as described in the section below, Harris will provide notification as appropriate to comply with any state law or regulatory requirement that requires notification.

5. The Security Officer in conjunction with the members of the Governance Risk Compliance Committee (GRCC) and executive leadership are responsible for this policy and procedure, and will work together to implement the policy, make determinations as required and updating this policy on a periodic basis based on changing organizational needs.

6. The Privacy Officer in conjunction with the Harris' legal counsel will rely upon external legal counsel for access to lists of applicable law enforcement and state/federal agency contact information, in the event of a Data Incident, as external legal counsel would have the most up-to-date information on the appropriate law enforcement officials or agencies that should be contacted regarding the Data Incident as well as when said officials/agencies should be contacted.

REPORTING OF ANY SUSPECTED DATA INCIDENT

Harris requires all Workforce Members, contractors and subcontractors to immediately report any suspected Data Incident to the Security Officer or the Privacy Officer. Harris will also report any known Data Incident as required by law, applicable regulation or contract.

INVESTIGATION OF ALL SECURITY INCIDENTS NOT INVOLVING PHI, PII OR OTHER SENSITIVE INFORMATION

1. The report of suspected Security Incidents will be made to the Security Officer or designee. At the time of the report, the Security Officer or designee will ask for specific information regarding the suspected Security Incident and will identify with as much specificity as possible the types of data that may be involved. The individual is encouraged to provide as much detail to assist with the investigation and mitigation efforts. If it is suspected that the Security Incident involves PHI, PII or other Sensitive Information, the Security Officer or his designee will immediately notify the Privacy Officer, who will assume primary responsibility for processing the incident under this policy.

2. The Security Officer or his designee assigns a severity level based on the information known and determined. The following questions, among others, may be relevant to this determination:

    a) Is the incident real or perceived?

    b) Is there any potential for PHI, PII or other Sensitive Information to be, or has any PHI, PII or other Sensitive Information been, exposed?

    c) Is the incident still in progress?

    d) What data or property are threatened and how critical is the threat?

    e) What is the impact on the business should the attack succeed? Minimal, serious or critical?

    f) What systems are targeted, where are they located physically and on the network?

    g) Is the incident inside the trusted network?

    h) Is the response urgent?

    i) Can the incident be quickly contained?

    j) Will the response alert the attacker and do we care?

    k) What type of incident is this (i.e., virus, worm, intrusion, abuse, damage, etc.)?

3. The Security Officer or his designee will contact all relevant members of the workforce, contractors or Business Associate to work as a team to promptly investigate.

4. The Security Officer or his designee will assign the Security Incident one of the following four category levels, which will dictate the response expectations:

    a) Level 1 – A threat to sensitive date (such as PHI) See Section F below.

    b) Level 2 – A threat to computer systems.

    c) Level 3 – A disruption of services.

    d) Level 4 – No threat.

5. Once all mitigation attempts have been completed and services have been restored, the Security Officer will document the Security Incident. The level and amount of documentation required will vary based upon the level of severity (levels 1-4 discussed above).

6. In addition to documenting the Security Incident, the Security Officer will recommend any near or long term changes to the system and/or policies and procedures that may be necessary as a result of the Security Incident.

7. Any Security Incident involving PHI, PII or other Sensitive Information will be investigated as a potential breach involving PHI, PII or other Sensitive Information and requiring notice as described below.

INVESTIGATION OF DATA INCIDENTS INVOLVING PHI, PII OR OTHER SENSITIVE INFORMATION:

1. Harris will identify and investigate all suspected Data Incidents to determine whether there has been a Breach of PHI, PII or other Sensitive Information as defined in this Policy. The Privacy Officer, with the assistance of the Security Officer (if necessary), will be responsible for the investigation.

2. The Privacy Officer will consult Harris' legal counsel to ensure the investigation remains in compliance with the law, and may also seek assistance from outside experts, such as external legal counsel, as necessary.

3. At the outset of an investigation, the Privacy Officer will also alert the following individuals or groups when appropriate:

    Security Officer (if the Breach involves PHI, PII or other Sensitive Information)

    Local Police (if the Breach involves the theft of information)

    Compliance Officer

    Insurance Carrier

4. All Suspected Breaches will be investigated. All reports of suspected Breaches of PHI, PII or other Sensitive Information and Security Incidents from workforce members, individuals, Business Associates and others will be investigated.

    a) Risk Assessment. To determine whether a breach of PHI, PII or other Sensitive Information has occurred, a risk assessment will be conducted, which will include but not be limited to, the following questions:

        i. Is the PHI Unsecured as defined by law?

        ii. Is the use or disclosure impermissible under the HIPAA Privacy Rule or other relevant regulatory requirement?

        iii. Is there a low probability that the PHI, PII or other Sensitive Information has been compromised based on a risk assessment?

        iv. Who impermissibly used the information or to whom the information was impermissibly disclosed?

        v. To what extent has the risk to the PHI, PII or other Sensitive Information been mitigated?

        vi. Was the impermissibly disclosed PHI, PII or other Sensitive Information actually acquired or viewed?

        vii. What is the type and amount of PHI, PII or other Sensitive Information involved in the impermissible use or disclosure?

        viii. Is the impermissible use or disclosure ongoing?

    b) Documentation. All facts gathered throughout the investigation, the risk assessment, and any conclusions derived from the investigation and risk assessment will be fully documented by the Privacy Officer and maintained by Harris for no less than six (6) years.

5. Review of Business Associates. Investigations of any suspected Breaches of PHI, PII or other Sensitive Information by contractors or Business Associate will also be reviewed by the Privacy Officer and the Security Officer.

CONCURRENT INVESTIGATION UNDER OTHER LAWS:

State Data Breach Laws. The Privacy Officer, in conjunction with Harris' legal counsel, will determine, simultaneously with the procedure outlined in this Policy, whether a suspected Data Incident qualifies as a breach under applicable state data breach laws, and whether such laws require Harris to take any action, including providing notification to individuals, media, law enforcement, state agencies or any other entity or individual.

MITIGATION OF DATA INCIDENTS:

1. Harris and (if applicable) its Business Associate, will engage in immediate and circumstance-appropriate efforts to mitigate the scope, nature, and potential for harm of any suspected Data Incident. Depending on the circumstances, mitigation efforts may include:

    a) Contacting law enforcement officers or other government officials or agencies;

    b) Correcting computer system errors;

    c) Shutting down access to affected systems;

    d) Changing any procedures that may have led to the Data Incident;

    e) Taking corrective action (including termination, if appropriate) against workforce members involved in the Breach;

    f) Retraining workforce members.

    g) Offering credit monitoring protection to individuals affected by the Data Incident.

The above list is only intended to illustrate the types of efforts that may be appropriate in certain circumstances. The list is not exhaustive. The circumstances of each particular breach, as well as any applicable Business Associate agreements with clients, should dictate what mitigation efforts are employed, as determined by the Privacy Officer and the Security Officer.

NOTIFICATION OBLIGATIONS:

1. Once sufficient information has been gathered through the investigation process, Harris will simultaneously assess any notification obligations that may arise as a result of a Data Incident under the HIPAA Breach Notification Rule, any applicable state data breach laws and any other relevant regulatory notification requirements. If Harris determines that notice is required under one or more of these rules, it shall follow the procedures for notice as set forth below.

2. Breach of PHI, PII or Other Sensitive Information

    a) Plan for Notification. After sufficient information has been gathered through investigation, and a determination has been made that a Breach of PHI, PII or other Sensitive Information has occurred, Harris will develop a plan to notify either the Covered Entity or Business Associate client, or if appropriate, all individuals affected by the Breach of PHI, PII or other Sensitive Information.

b) Notification Methodology and Timing. Notification to Covered Entity or Business Associate clients will be made as soon as possible and in compliance with contractual and legal requirements, but in no case later than 60 days after discovery. If required by a Business Associate agreement with a client to directly notify individuals, Harris will notify each affected individual in writing by first class mail or by e-mail (if the individual has indicated a preference to receive information by e-mail), of any Breaches of PHI, PII or other Sensitive Information as soon as possible, but in any event, no later than 60 days following the discovery of the Breach. In urgent cases, an alternative form of notification, such as by telephone, may be used in conjunction with written notification. Urgency will be determined on a case-by-case basis by the Privacy Officer.

3. State Law Breach

a) Plan for Notification. After a complete investigation and a determination that a breach of personal information has occurred, Harris will develop a plan to notify all individuals affected by the breach if so required under state law.

b) Notification and Methodology. Harris will notify individuals affected by a Breach in the manner and method required by state law. If the law in the state where the Breach occurred does not specify the manner and methodology of notification, Harris will notify each affected individual as outlined above for Breaches of PHI, PII or other Sensitive Information.

4. Contents of Notice

a) The notices required under this policy shall be written in plain English and will include each of the following:

i. Description of Breach. A brief description of what happened, including the date of the breach and the date of its discovery, if known;

ii. Description of Information. A description of the types of PHI or Personal Information as defined by state law involved in the breach (such as full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information);

iii. Mitigation. Steps the individual should take to protect himself/herself from potential harm resulting from the breach;

iv. Actions. A brief description of the actions Harris is taking or has taken to investigate the breach, mitigate harm to individuals, and protect against any further breaches; and,

v. Resources. Contact information, including a toll-free telephone number, e-mail address, website or postal address to permit the individual to ask questions or obtain additional information.

5. Breaches by Business Associates.

As previously stated, all Subcontractors shall have a Business Associate agreement that outlines responsibilities in case of a Data Incident. If notification to individuals affected by a Data Incident is required, the parties shall agree upon which party shall send the notification.

DEFINITIONS

See attached policy definitions or click here.

REGULATORY REFERENCES

45 C.F.R. § 164.304
45 C.F.R. § 164.308(a)(6)
45 C.F.R. §§ 164.400-164.414
16 C.F.R. § 318, *et seq.*