HPE POINTNEXT SERVICES

HPE VULNERABILITY ANALYSIS SERVICE

Advisory and Professional Services from HPE Pointnext

SERVICE OVERVIEW

HPE Vulnerability Analysis Service is designed to help you understand the risk that your business assets and applications are exposed to. By joining forces with Synack, a global and leading provider of crowdsourced penetration testing services, the HPE Vulnerability Analysis Service allows you to conduct a vulnerability scan, penetration testing, threat modeling, and phishing assessment on your critical assets in a simple, flexible, and timely manner.

By leveraging Hydra, the Synack proprietary vulnerability intelligence platform as the base testing system, you can choose to engage the expert researchers from HPE Pointnext Services or Synack's crowdsourced ethical researchers. This service provides you with comprehensive results to help you identify risk and determine remediation steps.

HPE Vulnerability Analysis Service is available with the following pre-packaged options. Each of these options is available using either Synack crowdsourced or HPE Pointnext Services researchers for the vulnerability scan and penetration testing components of the service:

- **HPE Vulnerability Analysis Service—Essential**
  - A two-week engagement with a choice of one of the following targets:
    - one (1) application
    - one (1) mobile application
    - one (1) infrastructure set (up to 250 IP addresses)
  - A choice of either Synack crowdsourced (service provided by Synack) or HPE Pointnext Services researchers
  - A report and debrief session on findings
- **HPE Vulnerability Analysis Service—Advanced**
  - A two-week engagement
  - Includes HPE Vulnerability Analysis Service—Essential
  - Includes the Detect and Defense Advisory add-on (performed by HPE security experts)
- **HPE Vulnerability Analysis Service—Premium**
  - Three-week engagement
  - Includes HPE Vulnerability Analysis Service—Essential
  - Includes the Threat Modeling add-on (performed by HPE security experts)
  - Includes the Phishing Assessment add-on (performed by HPE security experts)

- **HPE Vulnerability Analysis Service—Continuous**
  - 1 Year Continuous Service with a choice of one of the following targets:
    - one (1) application, or
    - one (1) mobile application, or
    - one (1) infrastructure set
      - Option 1—up to 50 IP addresses or
      - Option 2—up to 250 IP addresses
- Dedicated Program Manager per project
- Premium Mission Check (up to 70 checkpoint based on OWASP Top 10 list)
- Attacker resistance scores
- Synack crowdsourced delivery
- A comprehensive report and debrief session on findings
- Bi-Weekly Check-ins during the service period

SERVICE BENEFITS

- Gain insights on the risks that organizational assets and applications are exposed to/from an external or internal perspective
- Evaluate the effectiveness of security detecting/monitoring/responding capabilities (Advanced)
- Obtain an understanding of the threat statistics and the impact that a phishing attack could have on the customer organization (Premium)
- Experienced researchers and experts that develop actionable mitigation suggestions

The Service features table provides additional information on the features available under these penetration testing services.

SERVICE FEATURE HIGHLIGHTS

- Leverages HPE and crowdsourced researchers and experts to identify asset and application risk in a thorough, but controlled manner
- Supports highly customizable engagement rules (time of scanning, in-depth vulnerability exploit, finding workflows, and more), which allows you to consume this service in the way that best fits your environment
- Gives access to the assessment dashboard during the engagement, which provides real-time observations on what the researchers are working on and their findings to help maximize transparency and reduce uncertainty introduced by the penetration test
- Delivers PCI cross-map scan report for auditing purposes form Synack's Hydra platform
- Shortens overall engagement cycle and delivers faster results with pre-packaged model

COVERAGE

- Services will be provided during local HPE standard business days and hours excluding HPE holidays.
- Only upon written agreement between HPE and customer will vulnerability scanning and penetration testing activities be conducted outside of business hours and on holidays.

TABLE 1. SERVICE FEATURES

FEATURE	DELIVERY SPECIFICATIONS
HPE Vulnerability Analysis Service—Essential	Total engagement length is two (2) weeks. This service includes the following: • One remote vulnerability scan and penetration test on pre-agreed target(s) Under this service feature, Hewlett Packard Enterprise provides the following: • Work with the customer to determine the engagement model: – HPE Pointnext Services researchers, or – Crowdsource researchers (service provided by Synack) • Initial scoping: – Determine and finalize the scope target(s) of the engagement: ▫ One application, or ▫ One mobile application, or ▫ One set of infrastructure (up to 250 IP address) – Determine and finalize engagement rules including, but not limited to: ▫ Time of scan and exploit ▫ Finding notification workflows and escalation rules ▫ Exploit rules ▫ Set up customer portal access (if applicable) • Conduct a vulnerability scan (up to 7 days) on the targets—leverage Synack's Hydra Technology Platform and LaunchPoint tools • Conduct penetration test (exploit) on the targets where applicable—leverage Synack's Hydra Technology Platform and LaunchPoint, as well as other exploit tools where necessary • Conduct basic Mission checklist (~25 checkpoints) that covers common weaknesses on the OWASP Top 10 (where applicable) • Full scanning report in PDF format • Full report for PCI audit (where in-scope) in PDF format • Reports (in Microsoft® Word format) on highlighted (high-severity) findings and remediation suggestions • Remote customer debrief session (up to two hours) to be delivered via teleconference
HPE Vulnerability Analysis Service—Advanced	HPE Vulnerability Analysis Service Advanced includes HPE Vulnerability Analysis Service Essential plus Detect and Defense Advisory add-on. Total engagement length is two (2) weeks. • **Detect and Defend Advisory add-on:** Engagement length—Two (2) weeks to be conducted concurrently with vulnerability scan and penetration test service. An off-site HPE security expert will be assigned to work with customer team to evaluate and advice on the customer's capability to detect/react to cyberattack during a live vulnerability scan and penetration test session on the predefined target(s). Under this service feature, HPE Pointnext Services provides the following: • Initial scoping – Review customer environment and determine in-scope monitoring/detecting/notification technology and processes – Schedule workshop(s) – Determine resources and workshop coordination requirements • Conduct two (2) Detect and Defend workshops, of up to two (2) hours each, to be held concurrently with live vulnerability scan and penetration test session conducted by HPE Pointnext Services or Synack researchers. During the workshop, the HPE Pointnext Services assigned security expert reviews and monitors the behavior of the pre-identified detection system(s), detection response and escalation workflow with the customer to evaluate the level of the defensive measures implemented. • Report (in Microsoft Word format) on concluded status and recommendations

TABLE 1. SERVICE FEATURES (CONTINUED)

FEATURE	DELIVERY SPECIFICATIONS
HPE Vulnerability Analysis Service Premium	HPE Vulnerability Analysis Service Premium includes HPE Vulnerability Analysis Service Essential plus Threat Modeling and Phishing Assessment add-ons. Total engagement length is three (3) weeks. • **Threat Modeling add-on:** Engagement length—One (1) week; to be conducted prior to the vulnerability scan and penetration test service. An off-site HPE security expert will be assigned to conduct a threat modeling analysis on the predefined targets and to quantify vulnerabilities according to their potential to damage the organization. The expert will also identify effective information security solutions that can be deployed to mitigate identified risks, along with recommendations for how to focus resources to provide balanced protection. The Threat Modeling add-on will be conducted approximately one (1) week prior the start of the vulnerability scan and penetration test. Under this service feature, HPE Pointnext Services provides the following: – Remote information gathering ▫ Collect information about the target via documentation review, remote interviews, and more ▫ Perform analysis on the target – Report (in Microsoft Word format) on the analysis results and recommendations • **Phishing Assessment add-on:** Engagement length—Two (2) weeks to be conducted concurrently (beginning at the first week of engagement) with the Threat Modeling add-on, and vulnerability scan and penetration test service. An email-based social engineering assessment will be conducted to a selected group of target customer employees to provide insights into the size and impact that a phishing attack could have on the organization. Under this service feature, HPE Pointnext Services provides the following: – Generic phishing email to random sample of up to 250 employees – Advanced social engineering scenario testing and spear phishing for a sample of up to 25 employees – Phishing assessment report containing results and recommendations
HPE Vulnerability Analysis Service Continuous	Total Service length is 1 year This service includes the following: • One year remote continuous vulnerability scan and penetration test on pre-agreed target(s) Under this service feature, Hewlett Packard Enterprise provides the following: • Work with the customer to determine the engagement model: – The Continuous model will be delivered by Crowdsource researchers (service provided by Synack) • Initial scoping: – Determine and finalize the scope target(s) of the engagement: ▫ One application, or ▫ One mobile application, or ▫ One set of infrastructure (Two options, Up to 50 IPs or Up to 250 IPs) – Determine and finalize engagement rules including, but not limited to: ▫ Time of scan and exploit ▫ Finding notification workflows and escalation rules ▫ Exploit rules ▫ Set up customer portal access (if applicable) • Conduct a vulnerability scan continuously on the targets for one year—leverage Synack's Hydra Technology Platform and LaunchPoint tools • Conduct penetration test (exploit) continuous on the targets where applicable—leverage Synack's Hydra Technology Platform and LaunchPoint, as well as other exploit tools where necessary • Dedicated Program Manager to organize and report activities • Perform Premium Mission Check (up to 70 checkpoint based on OWASP Top 10 list of vulnerability) • Continuous access to attacker resistance Scores (part of Hydra Platform) • Continuous Triage and analysis of findings • Continuous access to PCI audit report (where in-scope) in PDF format • Bi-Weekly Check-ins during the service period up to (1) hours each • QBR (Total 4) during the service period • Creation of document deliverables at the end of the service period • Reports (in Microsoft Word format) on highlighted (high-severity) findings and remediation suggestions at the end of the service period • Remote customer debrief session, of up to two (2) hours, to be delivered remotely via teleconference at the end of the service period • Unlimited Patch verification testing during the service period

CUSTOMER RESPONSIBILITIES

- Obtain necessary approvals for conducting vulnerability and penetration testing activities
- A contact person must be made available to organize project logistics and act as the escalation point
- Respond to all requests for information and artifacts as requested by HPE
- Provide subject matter experts (SMEs) as required to clear up any areas of confusion or uncertainty
- Review and approve deliverables
- Provide VPN access (and access tokens if required) to internal environment where necessary; whitelist IP addresses and modify firewalls and related security access rules to facilitate vulnerability scanning activities where necessary
- Customer participation at the appropriate level to determine the workflow, engagement rules, and escalation procedure for the vulnerability scan and penetration test service
- Customer participation at the appropriate level to determine engagement scope, rules, and discovery of escalation workflows, as well as Detect and Defend workshop scope (Advanced only)
- Provide access or viewing capability on pre-defined monitoring and detection system(s) to the HPE consultant during the Detect and Defend workshop (Advanced only)
- Customer participation at the appropriate level to provide adequate information for threat modeling-related activities (Premium only)
- Customer participation at the appropriate level to provide target information for phishing activities (Premium only)
- Whitelist required email server IP address(es) for phishing activities (Premium only)
- Obtain necessary approvals for conducting phishing activity (Premium only)

SERVICE LIMITATIONS

- Limitation of each service feature is outlined in the Service features table. Additional charges incur for any additional services required.
- The scope of “one application” or “one mobile application” is subject to scoping agreement between HPE and customer in the form of a duly executed statement of work. For example, “www.customer.com” is considered as one application, however, the sub-domain that it may be linked to, such as “www.paymentsystem.com” may not be included as part of the “one application” scope.
- This service cannot be used to satisfy any formal audit requirement but can serve to prepare for a formal audit by identifying potential problem areas.
- Findings highly depend on the target status and network at the time the service is conducted. There is no guarantee that all vulnerabilities of the in-scope target(s) will be discovered.
- The continuous model can only be ordered on a per-year basis, target must be identified before the start of the service period and cannot be change during the service period. A full year service fee will still be charge to the customer for early termination.
- The entire deliverable documentation created for this engagement will be available in Microsoft Office or PDF electronic format.
- Services are deemed accepted upon performance.
- Services may result in damage to or loss of data. Customer will ensure that no personal data resides on the systems to be tested and agrees that HPE shall not be liable for any loss or damage to the data or the systems tested.

GENERAL PROVISIONS AND OTHER EXCLUSIONS

- Our ability to deliver this service is dependent upon the customer's full and timely cooperation with HPE, as well as the accuracy and completeness of any information and data the customer provides HPE.
- To the extent that HPE will have access to personal data, the HPE Data Processing and Security Agreement for HPE Vulnerability Analysis Services shall apply.

SUPPLEMENTAL TERMS

The following supplemental terms apply to these services and take precedence in the event of any conflict:

- Upon receipt of an acceptable order, HPE will contact the Customer within seven (7) business days to organize a service delivery date. Service delivery dates are subject to resource availability and may be scheduled up to 30 days from the order acceptance date.
- The Customer must schedule and receive delivery of these services within 180 days from order acceptance. HPE reserves the right to reprice for services not scheduled and delivered within 180 days. Backorders or shipment delays may affect the delivery timeline. Orders for services will expire after 365 days (one year) from the order acceptance date for services not scheduled and delivered, and the Customer will not be entitled to a refund for the unused services.

ORDERING INFORMATION

Availability of service features and service levels may vary according to local resources and may be restricted to eligible products and geographic locations. To obtain further information or to order HPE Vulnerability Analysis Service, contact a local HPE sales representative and reference the service name and the option.

Using Synack crowdsourced researchers:

(Synack crowd researchers are provided on a resell basis and subject to the terms and conditions listed on synack.com/master-service-agreement/)

- HPE Vulnerability Analysis Essential Service
- HPE Vulnerability Analysis Advanced Service
- HPE Vulnerability Analysis Premium Service
- HPE Vulnerability Analysis 1 Year Continuous Service

Using HPE researchers:

- HPE Vulnerability Analysis Essential Service
- HPE Vulnerability Analysis Advanced Service
- HPE Vulnerability Analysis Premium Service

LEARN MORE AT

hpe.com/us/en/services/consulting/security.html

HPE Data Processing and Security Agreement

HPE VULNERABILITY ANALYSIS SERVICES ("SERVICES")

This Data Processing and Security Agreement ("DPSA") governs the Processing of Personal Data by HPE in connection with the Services on Customer's behalf and is made a part of the agreement between HPE and Customer, or if no agreement exists, HPE's standard terms and conditions ("Agreement").

1. This DPSA forms part of the Agreement. To the extent there are any conflicts between the terms of this DPSA and the Agreement, the DPSA shall prevail.

2. Scope, Type, and Purpose of the planned collection, processing, or use of Data.

2.1. Data Subjects

The Personal Data transferred may include, without limitation, the following categories of data subjects:

- Full and part time employees, agents, advisors, or freelancers of Customer
- Partners, (prospective) customers, vendors of Customer
- Employees or contact persons of Customer's prospects, customers, business partners, and vendors
- Further affected data subjects may be described in the Agreement

2.2. Categories of Personal Data

The Personal Data transferred to HPE may include, without limitation, the following categories of data:

- Master data (Name etc.)
- Contact data (phone number, Email etc.)
- Contract data
- HR data
- Communication data (IP etc.)
- Tax data
- Financial/Bank data
- ID number
- Further data categories as may be described in the Agreement

2.3. Special categories of data (if appropriate)

The personal data transferred may include, without limitation, the following special categories of data:

- Racial or ethnic origin of a data subject
- Political opinions of a data subject
- Religious or philosophical beliefs of a data subject
- Trade Union membership of a data subject
- Genetic data, biometric data, for the purpose of uniquely identifying a natural person (data subject)
- Data concerning the health or sex life of a data subject

2.4. Processing Operations

HPE may process Personal Data solely to the extent necessary to perform its Services as described in the applicable transaction document.

3. Definitions

3.1. "Personal Data" or "Customer Personal Data" means any (Customer) information relating to an identified or identifiable natural persons or as otherwise defined in applicable Privacy Laws that HPE will Process on Customer's behalf in the provision of the Services.

3.2. "Business Contact Data" means contact information of Customer's representatives for invoicing, billing, and other business inquiries, (ii) information on Customer's usage of Services, and (iii) other information that HPE collects and needs to do business with Customer.

3.3. "Privacy Laws" mean all applicable laws and regulations relating to the Processing of Personal Data and privacy that may exist in the relevant jurisdictions, including HIPAA and the GDPR.

3.4. "HIPAA" means the federal Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 1320d-1320d-8.

3.5. "General Data Protection Regulation" ("GDPR") means the Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (and its implementing legislation) with effect from 25th May 2018.

3.6. "Controller" means the natural or legal person, public authority, agency, or any other body which alone or jointly with others determines the purposes and means of the Processing of Personal Data in accordance with applicable Privacy Law.

3.7. "Processor" means any natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of a Controller or on the instruction of another Processor acting on behalf of a Controller.

3.8. "Process," "Processing," or "Processed" means an operation or set of operations performed on or with Personal Data whether or not by automatic means (including, without limitation, accessing, collecting, recording, organizing, retaining, storing, adapting or altering, retrieving, consulting, using, disclosing, making available, aligning, combining, blocking, erasing, and destroying Personal Data) and any equivalent definitions in Privacy Law to the extent that such definition should exceed this definition.

4. This DPSA incorporates by reference:

Schedule 1—Data Protection—Base Terms

Schedule 2—Security

Schedule 3—EEA & Swiss Personal Data & EU Model Contract

Schedule 4—HIPAA & Business Associate Agreement

Schedule 1—Data Protection—Base Terms

HPE shall Process Customer Personal Data in accordance with the terms of the DPSA. All capitalized terms shall have the meaning defined in the DPSA.

1. Appointment and Instructions

1.1. HPE shall Process Customer Personal Data as necessary to provide the Services and to meet HPE's obligations under this DPSA, the Agreement, and applicable law as a service provider and Processor of Customer Personal Data. The type of Customer Personal Data Processed includes that set out in Section 2 of the DPSA. Subject to Section 7 of this Schedule 1, HPE shall Process Customer Personal Data for the duration of the Agreement.

1.2. HPE shall Process Customer Personal Data in accordance with Customer's instructions as set out in this DPSA, the Agreement, or other documented instructions between HPE and Customer. Potential costs and charges associated with such additional instructions shall be agreed pursuant to the terms of the Agreement.

1.3. HPE may Process Customer Personal Data other than on the instructions of Customer if it is required under law applicable to HPE. In this situation, HPE shall inform Customer of such a requirement before HPE Processes Customer Personal Data unless the law prohibits this on important grounds of public interest. If HPE is unable to comply with Customer's instructions or this DPSA due to changes in legislation or, if HPE believes (without having to conduct a comprehensive legal analysis) that any instruction from Customer will violate applicable law or for any other reason, HPE shall promptly notify Customer in writing.

1.4. HPE acknowledges that HPE has no right, title, or interest in Customer Personal Data (including all intellectual property or proprietary information contained therein). HPE may not sell, rent, or lease Customer Personal Data to anyone.

1.5. If Customer uses the Services to Process any categories of data not expressly covered by this DPSA, Customer acts at its own risk and HPE shall not be responsible for any potential compliance deficits related to such use.

2. Compliance with Laws

2.1. The Parties shall at all times comply with their respective obligations under this DPSA and Privacy Laws that apply to their respective processing of Personal Data.

2.2. HPE shall also comply with all applicable laws and HPE's privacy policy with respect to the Processing of Business Contact Data and use Business Contact Data only for legitimate business purposes, including, without limitation, invoicing, collections, service usage monitoring, service improvements, maintenance, support, communications relating to contract renewals (directly or through a subcontractor acting on HPE's behalf or an HPE approved reseller for contract renewal purposes), and information about new and additional services.

2.3. Where HPE discloses its personnel's personal data to Customer or HPE personnel provide their personal data directly to Customer, which Customer Processes to manage its use of the Services, Customer shall Process that data in accordance with its privacy policies and applicable Privacy Laws. Such disclosures shall be made by HPE only where lawful for the purposes of contract management, service management, or Customer's reasonable and lawful background screening verification or security purposes.

3. Security

3.1. HPE shall implement and maintain the physical, technical, and organizational security measures set out in Schedule 2—Security, as may be supplemented or modified in the applicable transaction document, to protect Customer Personal Data and Business Contact Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, or access.

3.2. Customer acknowledges that HPE may change the security measures through the adoption of new or enhanced security technologies and authorizes HPE to make such changes provided that they do not diminish the level of protection. HPE shall make information about the most up to date security measures applicable to the Services available to Customer upon request.

4. Sub Processing & Location of Processing

4.1. Customer authorizes HPE to engage affiliated and unaffiliated subcontractors ("Subcontractors") to perform some or all of its obligations under the Agreement. Only where necessary to provide the Services, HPE will provide its affiliates and subcontractors with access to Customer Personal Data.

4.2. The Subcontractors listed in the applicable transaction document are deemed as approved by Customer. In the event of changes to approved Subcontractors, HPE will notify Customer. Customer shall have ten (10) business days from receipt of the information on subcontractors to object to the appointment or replacement of a subcontractor and the parties shall use all reasonable endeavors to resolve Customer's objection. If the parties fail to resolve Customer's objection within a reasonable period of time, the matter shall be addressed pursuant to the dispute resolution procedure in the Agreement. In case HPE and customer fail to agree on an amicable resolution to the proposed subcontractor change, HPE shall have a right to terminate the contract without further obligations.

4.3. HPE shall conduct appropriate due diligence of its subcontractors and execute valid, enforceable and written contracts with subcontractors requiring the subcontractor to abide by terms no less protective than those in this DPSA regarding the Processing and protection of Customer Personal Data (including the EU Model Contract terms relating to data importers in the case of an onward transfer of EU, EEA, or Swiss Personal Data to a non-adequate country).

4.4. HPE remains responsible for the acts and omissions of the affiliates and subcontractors it engages to provide the Services to Customers giving rise to a breach of this DPSA as if they were its own acts or omissions.

5. Audit & Assurance

5.1. HPE shall arrange for audits of HPE's data Processing and protection practices to confirm compliance with this DPSA by reputable third party auditors and provide Customer with a report summary and additional information on request.

5.2. Customer shall have the right to conduct additional audits of HPE's compliance with its obligations under this DPSA in accordance with the Agreement. The audit rights are generally exercised in consultation with HPE. HPE is obliged to assist Customer in such controls and any controls of the competent authorities. These controls must be carried out in consideration of the business processes and HPE's need for security and confidentiality.

5.3. Certain information about HPE's security standards and practices are sensitive confidential information which will not be disclosed by HPE to Customer. Upon request, HPE agrees to respond, no more than once per year, to a reasonable information security questionnaire concerning security practices specific to the Services provided hereunder.

5.4. On Customer's request, HPE shall within a reasonable timeframe make appropriate information available to Customer to demonstrate its compliance with this DPSA, save where that information is readily available to Customer direct through its use of the Services.

6. Providing Customer Assistance

6.1. At Customer's request HPE shall co-operate with Customer and provide Customer with assistance necessary to facilitate the Processing of Customer Personal Data in compliance with Privacy Laws applicable to Customer in relation to HPE Pointnext Services including by way of example:

6.1.1. Assist Customer by implementing appropriate and reasonable technical and organizational measures, insofar as this is possible, to assist with Customer's obligation to respond to requests from individuals seeking to exercise their rights under the Privacy Laws applicable to Customer;

6.1.2. Provide reasonable assistance to Customer in Customer's assessment and implementation of appropriate technical and organizational measures to ensure a level of security appropriate to the risks represented by the Processing and the nature of Customer Personal Data;

6.1.3. The notification of Security Incidents pursuant to Schedule 2;

6.1.4. Provide reasonable assistance to Customer in carrying out a privacy impact assessment

6.2. If Customer requests cooperation or assistance pursuant to this Section 6, Customer shall notify HPE in writing of the requirements and formulate Customer's instructions. HPE shall respond within a reasonable period of time and provide Customer with approximate time and fee estimates for the implementation of any changes necessary to accommodate Customer's compliance needs. To the extent that compliance with this Section 6 constitutes a change to the scope of the Services, the parties shall, acting reasonably, agree on appropriate amendments to the Agreement.

7. Data Quality, Retrieval & Destruction, Repair or Replacement Service

7.1. To the extent that Customer is not able to access Customer Personal Data itself, HPE shall on Customer's written request (i) update, correct, or delete Customer Personal Data; and/or (ii) provide copies of Customer Personal Data.

7.2. Upon termination of the Agreement, HPE shall at the election of Customer return or delete Customer Personal Data and HPE shall not retain copies of Customer Personal Data unless otherwise agreed with Customer or where it is required to do so under applicable law, in which case HPE shall stop actively Processing the data and maintain the security and confidentiality of the data.

7.3. With regard to the repair or replacement of data carriers (server, hard-disks, SSD, flash-disks, memory etc.), Customer will either use the optional (C)DMR Service or adequately wipe (following the NIST Standard) carriers prior to providing them to HPE.

Schedule 2—Security

In this Schedule, HPE describes its commitment to technical and organizational security measures to protect customer data and the IT environment. The technical and organizational measures will be subject to technical advances and further development. In this respect, HPE will be allowed to implement adequate alternative measures.

1. HPE shall maintain an information and physical security program for the protection of Customer Personal Data and confidential information (the "HPE Security Program").

2. As part of the HPE Security Program, HPE conducts periodic reviews of security practices against various leading industry standards, such as NIST, ISO 27001, and SOC. HPE regularly re-evaluates and updates the HPE Security Program as the industry evolves, new technologies emerge or new threats are identified. Upon request, HPE agrees to respond to a reasonable information security questionnaire concerning HPE Security Program specific to the Services provided hereunder no more than once per year.

3. HPE Personnel

Employees and contractors are trained on HPE's privacy and security policies and made aware of their responsibilities with regard to privacy and security practices. HPE employees and contractors are contractually bound to maintain the confidence of Customer Personal Data or confidential information and comply with applicable HPE policies, standards or requirements in relation to the Processing of Customer Personal Data. Failure to comply with those policies, standards or requirements will be subject to investigation which may result in disciplinary action up to and including termination of employment or engagement by HPE.

4. Security Breach Notification and Security Incident Management

4.1. In the event HPE confirms a security breach leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, Customer Personal Data or Confidential Information ("Security Incident"), HPE will, without undue delay, notify Customer of the Security Incident. HPE will provide Customer with updates on the status of the Security Incident until the matter has been remediated. The reports will include, without limitation, a description of the Security Incident, actions taken and remediation plans. If Customer becomes aware of a Security Incident that affects the Services, Customer shall promptly notify HPE of such and inform HPE of the scope of the Security Incident. Notice shall be provided to HPE Security Operations Center via email at soc@hpe.com and/or to 1-877-762-6139.

4.2. HPE shall, at the request and cost of the Customer, (i) provide reasonable assistance to the Customer in notifying a security breach to the supervisory authority competent under the Privacy laws applicable to the Customer; and (ii) provide reasonable assistance to the Customer in communicating a data breach to data subjects in cases where the data breach is likely to result in a high risk to the rights and freedoms of individuals.

Schedule 3—EEA & Swiss Personal Data & EU Model Contract

1. To address the transfer of EU, EEA, or Swiss Personal Data by Customer or a Customer affiliate to HPE or an HPE affiliate located in a country which is not approved by the European Commission as providing adequate protection for personal data pursuant to Article 25(6) of the Directive 95/46/EC or Article 45(3) of the GDPR, the execution of a controller to processor EU Model Contract ("EU Model Contract") is required in connection with the Services. Customer hereby authorizes HPE to execute an EU Model Contract on its and its affiliates' behalf.
2. When interpreting the EU Model Contract, the term "Member State in which the data exporter is established" will be interpreted to mean (as appropriate) Switzerland or the EU or EEA member state in which the Data Exporter (as defined in the EU Model Contract) is established.
3. In the case of any conflict between the EU Model Contract, the terms of this DPSA, and the Agreement, to the extent HPE Processes the Personal Data of EEA or Swiss residents, the EU Model Contract shall prevail but only to the extent necessary to resolve the conflict or inconsistency.
4. Any audit pursuant to an EU Model Contract shall be conducted in accordance with the general procedures for audits provided in the Agreement and Schedule 1 except to the extent expressly required by a regulatory authority or Privacy Laws. Customer shall use commercially reasonable efforts to notify the regulatory authority of the audit requirements of the Agreement and to request that the audit be conducted in accordance with those requirements.
5. Any losses suffered by the parties or their respective affiliates under the EU Model Contract shall be treated as if they had been suffered by Customer or HPE respectively and shall in all cases be recovered by Customer or HPE subject to any limits on that party's liability in the Agreement. Nothing in this Section 1.5 shall limit the liability of either party in relation to a claim by a data subject under an EU Model Contract.
6. Customer agrees that HPE may appoint subcontractors in accordance with the provisions of Schedule 1.
7. In the event that EU Model Contracts are no longer a valid transfer mechanism or where HPE commits to an alternative valid transfer mechanism (e.g. Binding Corporate Rules for Processors), HPE shall notify Customer of the mechanism and seek Customer's agreement to rely on this mechanism instead of the EU Model Contract.

Schedule 4—HIPAA & Business Associate Agreement
If and to the extent HPE is acting as a business associate or subcontractor with respect to Customer Personal Data pertaining to US patients that qualifies as protected health information under HIPAA, the terms of the following BAA shall apply.

BUSINESS ASSOCIATE AGREEMENT ("BAA")
For purposes of this BAA, Customer will be referred to as "Covered Entity" and HPE will be referred to as "Business Associate", and this BAA is applicable when referenced in or attached to a transaction document.

Covered Entity is subject to the federal Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. §§ 1320d – 1320d-8 ("HIPAA"), as amended from time to time, and is required to safeguard individually identifiable health information that the Covered Entity creates, receives, maintains, or transmits (hereinafter "Protected Health Information" or "PHI") in accordance with the requirements HIPAA establishes and also the requirements set forth in the Health Information Technology for Economic and Clinical Health ("HITECH") Act and their respective implementing regulations;

1. Definitions

The following terms shall have the meaning ascribed to them in this Section. Other capitalized terms shall have the meaning ascribed to them in the context in which they first appear. Terms used but not otherwise defined in this BAA shall have the same meaning as those terms in the federal Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 subpart A and 164 subparts A and E (the "Privacy Rule"); the federal Security Standards for the Protection of Electronic Protected Health Information, 45 CFR Parts 160 subpart A and 164 subparts A and C (the "Security Rule"); and the Notification in the Case of Breach of Unsecured Protected Health Information, 45 CFR Part 164 subpart D (the "Breach Notification Rule") (collectively the "HIPAA Rules").

(a) **Breach**: "Breach" shall have the same meaning as the term "Breach" as defined in 45 CFR 164.402.

(b) **Business Associate**: "Business Associate" shall have the same meaning as the term "Business Associate" in 45 CFR 160.103 and, as used in this BAA, refers to Business Associate in its capacity as an entity that creates, receives, maintains, or transmits Protected Health Information in providing services to a Covered Entity.

(c) **Covered Entity**: "Covered Entity" shall have the same meaning as the term "Covered Entity" in 45 CFR 160.103 and, as used in this BAA, refers to the Covered Entity identified above.

(d) **Individual**: "Individual" shall have the same meaning as the term "Individual" in 45 CFR 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

(e) **Protected Health Information**: "Protected Health Information" or "PHI" shall have the same meaning as the term "Protected Health Information" in 45 CFR 160.103, and shall refer to PHI obtained from Covered Entity or created, received, maintained, or transmitted by Business Associate on behalf of Covered Entity, including any PHI that is created, received, maintained, or transmitted in an electronic form ("Electronic PHI").

(f) **Required By Law**: "Required By Law" shall have the same meaning as the term "Required By Law" in 45 CFR 164.103.

(g) **Secretary**: "Secretary" shall mean the Secretary of the Department of Health and Human Services or his/her designee.

(h) **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 as defined at 45 CFR 164.304.

(i) **Unsecured Protected Health Information**: "Unsecured Protected Health Information" or "Unsecured PHI" shall mean Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L. 111-5, as defined at 45 CFR § 164.402.

2. Obligations and Activities of Business Associate

(a) **Uses and Disclosures of PHI**: With respect to each use and disclosure of PHI Business Associate makes pursuant to this BAA, or otherwise, Business Associate agrees as follows:

(1) Business Associate agrees not to use or disclose PHI other than as permitted or required by this BAA or as Required By Law. To the extent that Business Associate performs any of Covered Entity's obligations under the Privacy Rule, Business Associate will comply with the requirements of the Privacy Rule that apply to Covered Entity in the performance of such obligation.

(2) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this BAA.

(3) Business Associate agrees to report to Covered Entity any use or disclosure of PHI not provided for by this BAA of which it becomes aware.

(4) If applicable, in accordance with 45 CFR 164.504(e)(1)(ii) and 164.308(b)(2), Business Associate agrees to enter into written BAAs with any subcontractors that create, receive, maintain, or transmit Protected Health Information on behalf of Business Associate, and the terms of such BAAs shall incorporate substantially similar restrictions, conditions, and requirements that apply to Business Associate through this BAA.

(5) At the sole cost and expense of the Covered Entity, Business Associate agrees to make available and provide Covered Entity with access to PHI to meet the requirements under 45 CFR 164.524. The obligations of Business Associate in this paragraph apply only to PHI in Designated Record Sets in Business Associate's possession or control as such term is defined at 45 CFR § 164.501. Such access shall be in a timely and reasonable manner, as agreed upon by the Parties.

(6) At the sole cost and expense of the Covered Entity, Business Associate agrees to make any amendment(s) to PHI that Covered Entity directs or agrees to pursuant to 45 CFR 164.526 at the request of Covered Entity, in a time and manner reasonably agreed upon by the Parties. The obligations of Business Associate in this paragraph apply only to PHI in Designated Record Sets in Business Associate's possession or control as such term is defined at 45 CFR § 164.501.

(7) Business Associate agrees to make its internal practices, books, and records, including any policies and procedures, relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity, available to the Secretary, in a time and manner reasonably agreed upon or designated by the Secretary, for purposes of the Secretary determining a Covered Entity's compliance with the Privacy and Security Rule.

(8) Business Associate agrees to maintain and make available, in a time and manner reasonably negotiated between the Parties, the information required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI, as necessary to satisfy Covered Entity's obligations under 45 CFR 164.528.

(b) **Securing Electronic PHI**:

(1) Business Associate agrees to use appropriate safeguards and comply with applicable and mandatory requirements of the Security Rule set forth at 45 CFR 164.308, 164.310, 164.312, and 164.316 with respect to Electronic PHI to prevent the use or disclosure of Electronic PHI other than as provided for by this BAA.

(2) Business Associate shall report to Covered Entity any Security Incident that results in the unauthorized disclosure of Electronic PHI of which Business Associate becomes aware with respect to Electronic PHI Business Associate creates, transmits, receives or maintains on behalf of Covered Entity. Business Associate shall report unsuccessful Security Incidents to Covered Entity upon request. Parties recognize, however, that a significant number of meaningless attempts to access, without authorization, use, disclose, modify, or destroy PHI in Business Associate's systems will occur on an ongoing basis and could make a real-time reporting requirement formidable for Parties. Therefore, Parties agree that the following are illustrative of unsuccessful Security Incidents that, if they do not result in a pattern of Security Incidents or the unauthorized access, use, disclosure, modification, or destruction of PHI or interference with an information system, do not need to be reported:

(i) Pings on a firewall;

(ii) Port scans;

(iii) Attempts to log on to a system or enter a database with an invalid password or user name; and

(iv) Malware (e.g., worms, viruses)

(c) **Notification of Breaches of Unsecured PHI**: Business Associate will notify Covered Entity of Breaches of Unsecured PHI without unreasonable delay and in no case later than thirty (30) calendar days after the Discovery of such a Breach of the Covered Entity's Unsecured PHI, as those terms are defined at 45 CFR Part 164 subpart D. Business Associate's notice to the Covered Entity shall include the applicable elements as set forth at 45 CFR 164.410(c).

3. Permitted Uses and Disclosures by Business Associate

In accordance with the limitations in this BAA, Business Associate may use or disclose PHI as necessary to perform functions on behalf of and/or provide services to Covered Entity to the extent such uses or disclosures are permitted by the Privacy Rule, as it may be amended from time to time.

4. Specific Use and Disclosure Provisions

(a) In accordance with the limitations in this BAA, Business Associate may use PHI as necessary for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, to the extent such use is permitted by the Privacy Rule, as it may be amended from time to time.

(b) In accordance with the limitations in this BAA, Business Associate may disclose PHI as necessary for the proper management and administration of Business Associate or to carry out the legal responsibilities of the Business Associate, provided that such disclosures are (i) Required By Law, (ii) Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as Required By Law or for the purposes for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been Breached, or (iii) are otherwise permitted by the Privacy Rule, as it may be amended from time to time.

(c) Business Associate may use PHI as necessary to report violations of law to appropriate federal and state authorities, to the extent permitted by 45 CFR 164.502(j)(1).

(d) In accordance with 45 CFR 164.504(e)(2)(i)(B), Business Associate may use PHI to provide data aggregation services.

5. Specific Use and Disclosure Restrictions

(a) Business Associate will restrict the disclosure of an Individual's PHI in accordance with 45 CFR 164.522(a)(1)(i)(A), notwithstanding paragraph (a)(1)(ii) of that section, when, except as otherwise Required By Law, the Covered Entity notifies Business Associate that the Individual has made such a restriction request, and each of the following conditions is satisfied:

(1) The disclosure would be to a health plan for the purposes of carrying out payment or healthcare operations, as that term may be amended from time to time, and

(2) The PHI pertains solely to a healthcare item or service for which the healthcare provider involved has been paid out-of-pocket in full.

(b) In accordance with 45 CFR 164.502(b)(1), Business Associate will limit to the extent practicable the use, disclosure, or request of PHI to the minimum necessary to accomplish the intended purposes of such use, disclosure, or request, respectively, except that the restrictions set forth herein shall not apply to the exceptions set forth in CFR 164.502(b)(2).

(c) Business Associate shall not directly or indirectly receive remuneration in exchange for any PHI unless the Business Associate obtains written authorization (from the Individual) that includes a specification of whether the PHI can be further exchanged for remuneration by the entity receiving the PHI of that Individual, except that this prohibition shall not apply in the following cases, which Business Associate will limit remuneration to a reasonable, cost-based fee to cover the cost to prepare and transmit the Protected Health Information for such purpose or a fee otherwise expressly permitted by other law:

(1) The purpose of the exchange is for research or public health activities, as described at 45 CFR 154.501, 164.512(i), 164.512(b) and 164.514(e), or

(2) The purpose of the exchange is for the treatment of the Individual, subject to 164.506(a) and any regulation that the Secretary may promulgate to prevent PHI from inappropriate access, use or disclosure, or

(3) The purpose of the exchange is the healthcare operation specifically described in subparagraph (iv) of paragraph (6) of the definition of healthcare operations at 45 CFR 164.501 and pursuant to 164.506(a), or

(4) The purpose of the exchange is for remuneration that is provided by Covered Entity to the Business Associate for activities involving the exchange of PHI that Business Associate undertakes on behalf of and at the specific request of the Covered Entity as set forth in this BAA, or

(5) The purpose of the exchange is to provide an Individual with a copy of the Individual's PHI pursuant to 45 CFR 164.524 or an accounting of disclosures pursuant to 164.528, or

(6) The purpose of the exchange is otherwise determined by the Secretary in regulations to be similarly necessary and appropriate.

6. Obligations of Covered Entity

(a) Covered Entity shall notify Business Associate of any limitation(s) in a Covered Entity's notice of privacy practices, in accordance with 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

(b) Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

(c) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that a Covered Entity has agreed to or is required to abide by in accordance with 45 CFR 164.522, or as mandated pursuant to Section 13405(c) of the HITECH Act, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

(d) Covered Entity agrees to disclose to Business Associate only the minimum amount of PHI necessary to accomplish the services covered in the Transaction Document.

(e) Covered Entity understands and agrees that in addition to obligations Required By Law, Business Associate provides services in the Transaction Document on the express condition that the Covered Entity fulfills its additional obligations set forth therein.

7. Permissible Requests by Covered Entity

Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy or Security Rules if done by Covered Entity.

8. Termination

(a) **Termination for Cause for Failure to Comply with this BAA by Business Associate**: Upon any material failure to comply with this BAA by Business Associate, Covered Entity shall either:

(1) Provide an opportunity for Business Associate to cure the failure to comply or end the violation and terminate this BAA if Business Associate does not cure the failure to comply or end the violation within a reasonable time specified by Covered Entity; or

(2) Immediately terminate this BAA if Business Associate has failed to comply with a material term of this BAA and cure is not possible and the Business Associate has not implemented reasonable steps to prevent a reoccurrence of such failure to comply.

(b) **Termination for Cause for Failure to Comply with this BAA by Covered Entity**: Upon any material failure to comply with this BAA by Covered Entity, Business Associate shall either:

(1) Provide an opportunity for Covered Entity to cure the failure to comply or end the violation and terminate this BAA if Covered Entity does not cure the failure to comply or end the violation within the time specified by Business Associate;

(2) Immediately terminate this BAA if Covered Entity has failed to comply with a material term of this BAA and cure is not possible and the Covered Entity has not implemented reasonable steps to prevent a reoccurrence of such failure to comply.

(c) **Effect of Termination**:

(1) Except as provided below in paragraph (2) of this subsection, upon termination of this BAA, for any reason, Business Associate shall return or destroy all PHI received from Covered Entity or created, received, maintained, or transmitted by Business Associate on behalf of Covered Entity in accordance with HIPAA. This provision shall apply to PHI in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of PHI.

(2) In the event Business Associate determines returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon written notification that return or destruction of PHI is infeasible, Business Associate shall extend the protections of this BAA to such PHI and limit further uses and disclosures of PHI for so long as Business Associate maintains such PHI.

Make the right purchase decision.
Contact our presales specialists.


Chat


Email


Call


Share now


Get updates

Hewlett Packard Enterprise

a00044841ENW, October 2019, Rev. 4