|  |  |  |  |
| --- | --- | --- | --- |
| **Question** | **Question:** |  | **Prognos Response** |
| **3PRA\_I\_ThirdPartyProfile\_13** | Description of ALL services provided to Horizon BCBSNJ |  | Risk Alerts and Care Alerts (REPORTS)- collection, harmonization, analyzation of laboratory test data on behalf of client for permitted uses falling under the HIPAA definition of "Health Care Operations" |
| **3PRA\_II\_Administrative\_1.31** | Mobile device policy (MDM/BYOD) | DB | No. PHI is only accessible in the VCR (no access via mobile devices) |
| **3PRA\_II\_Administrative\_2.02** | ≥ 2 full reference verification | HW | No. We do not require personal references but our third party does verify prior employers |
| **3PRA\_III\_Technical\_3.05** | Does a documented process exist by which Commercial off-the-shelf (COTS) software vulnerabilities are periodically reviewed, prioritized and acted upon? | DB | We don’t use COTS so no process is required |
| **3PRA\_III\_Technical\_4.01** | Are users prevented by the system from installing non-approved software? | DB | [answered “no” should be yes] Users with access to VCR are prohibited from installing non-approved software on their laptops |
| **3PRA\_III\_Technical\_5.03** | Are all remote users forced through a "clean access" chokepoint to ensure patch levels are verified, antivirus controls are on and other security controls are active prior to allowing access? | DB | [answered “yes”] |
| **3PRA\_III\_Technical\_5.04** | Are tablets/smartphones equipped with encrypted containers for company data? | DB | No - PHI is not accessible or stored there |
| **3PRA\_III\_Technical\_6.06** | Are users blocked from accessing dangerous websites? | DB | [answered no but should be yes]. Limited only to very specific websites when in the clean room - EPP |
| **3PRA\_III\_Technical\_6.07** | Are users blocked from access to personal web mail? | DB | [answered no but should be yes]. Limited only to very specific websites when in the clean room - EPP |
| **3PRA\_III\_Technical\_6.09 / 6.09a** | Are users blocked from accessing cloud-based storage services? (e.g. DropBox, Box.com, OneDrive, etc.). / How is access to cloud-based storage services monitored and secured? | DB | [answered no but should be yes]. Limited only to very specific websites when in the clean room - EPP |
| **3PRA\_III\_Technical\_8.01a** | Are logs fed into a SIEM tool? | VD | No. EPP captures Admin logs which is audited monthly. We do not have SIEM/SOC at Prognos to monitor logs in the real time. As we leverage on ClearDATA for SIEM, they have SOC in place and any suspicious/malicious activity if they come across is reported to the security team and fixed as their incident response. |
| **3PRA\_III\_Technical\_8.04 / 8.04a** | Has Intrusion Detection/Prevention been implemented? / Specify type of IDS/IPS in place (e.g. Host, Network, or both) | VD | What we answered: ClearDATA as our Managed Services provider of AWS provides cloud security integration and tools. They use network based IPS. The IPS is utilized to analyze network events and report possible or actual network events. ClearDATA also installs an Intrusion Detection System (IDS) (TrendMicro) on all compute resources (e.g. EC2 instances) to satisfy 45 CFR 164.308(a)(6)(ii) |
| **3PRA\_III\_Technical\_8.05 / 8.05a / 8.05b / 8.05c** | Has a Data Leakage Prevention (DLP) solution been implemented? / Specify Type / Specify Protocols Monitored / What data does DLP look for? | VD | What we answered:  End point Protecter (EPP) on the Virtual Cleanroom end points and ClearDATA has deployed DLP technology on network jump servers and SMTP connections to detect and prevent the loss of sensitive information.  Cleardata also inspect all servers, services, data buckets, etc to ensure that there is no erroneous activity. They utilize software like Trendmicro and Alertlogic's service to alert. Clearlogic maintains a system of record and logging for all systems and we can retrieve upon request as needed. |
| **3PRA\_III\_Technical\_11.02** | Do you authenticate devices that attach to your network? | DB | We don’t have a network |
| **3PRA\_III\_Technical\_24.01** | Do you PGP encrypt a file before sending it securely to an external party? | DB | We have other ways of securely transferring |
| **3PRA\_III\_Technical\_24.04** | Do you support sending events to a Horizon logging and monitoring solution? | VD |  |
| **3PRA\_IV\_BCM\_12.02** | Cameras at all entrances/exits (with at least 30 days or archived video) | HW | No physical location with PHI; cameras at main entrance but not company office entrance |
| **3PRA\_IV\_BCM\_12.06** | Process for screening visitors and their luggage | HW |  |
| **3PRA\_IV\_BCM\_12.10** | Is sensitive data housed behind two or more physical security checkpoints (guards, locked doors, access control systems, etc.) | HW | No physical location with sensitive data |
| **3PRA\_IV\_BCM\_13.01** | Do you have certified Business Continuity Management Professionals on staff or under contract? | HW |  |
| **3PRA\_V\_Compliance\_15.10** | Is there a procedure to identify and disclose any potential or actual conflict of interest with Horizon BCBSNJ or any of its employees? | HW |  |
| **3PRA\_V\_Compliance\_17.04** | If applicable, is there a similar monitoring and auditing process that addresses the compliance requirements associated with Medicare Parts C and D? | HW |  |
| **3PRA\_V\_Compliance\_17.05** | Is oversight, monitoring, and auditing conducted for contractors and subcontractors to ensure their compliance including, if applicable, their compliance with Medicare Part C and Part D requirements? | HW | N/A we have no subcontractors that work on any Medicare business |
| **3PRA\_V\_Compliance\_17.07** | Is there a procedure to evaluate the effectiveness of the compliance monitoring and auditing processes? | HW |  |
| **3PRA\_V\_Compliance\_17.08** | Is an assessment conducted to identify various areas of compliance risk? | HW |  |