Below is a summary of your responses

Download PDF

Welcome!

Thank you for responding to this Supplier Risk Assessment Questionnaire (“Questionnaire”). This Questionnaire is important to us as part of our ongoing business relationship. The following information may be helpful to you in preparing to complete this Questionnaire.

Who? It is important that individual(s) who are knowledgeable of the processes and activities related to Information Security activities related to the areas below provide the responses to the Questionnaire (Information Security Officer, Privacy Leader(s), IT Infrastructure Leader(s), et. al).

More than one user may access the Questionnaire at one time. If you previously started, but did not complete the survey, the link you received will take you back to where you left off.

How Long? This Questionnaire should take a few hours to complete. Time may vary based on the size and complexity of your organization. We recommend that all responses be reviewed for accuracy prior to submission.

What's Covered? This Questionnaire will cover activities in the following areas relative to your Information Security policies, procedures, practices, and internal control environment:

Resource Management
Information Security
Governance
Encryption
Incident Management & Incident Response
Privacy
Physical Security
Electronic Security | User Access Management
Electronic Security | Network Infrastructure
Wireless Access Management
Electronic Security | Technology Infrastructure
Technology Asset Management
Use of Subcontractors
Cloud Services
Mobile Device Management
Business Continuity & Disaster Recovery
Ransomware
European Union (EU Data Protection Law (e.g., General Data Protection Regulation (GDPR))

By When? The Questionnaire should be completed within ten (10) business days of receipt. After 10 business days the Questionnaire will automatically expire and information you have provided will be recorded as a final submission. You will be unable to modify a partially completed Questionnaire after 10 business days.

Highmark reserves the right to follow-up with your organization to seek clarification or to perform additional validation of your responses as deemed necessary by Highmark. After the Questionnaire is completed and submitted, you will be notified of any necessary next steps. If there are any changes to your responses after submitting this Questionnaire, you must notify us immediately by contacting SupplierRisk@highmark.com.

About this Questionnaire: Please use the "Previous" button within the Questionnaire to return to prior questions. Your progress will be automatically saved. Responses can be updated up until submitting the Questionnaire. Upon submission, your responses will be recorded as a final submission and provided back to Highmark. If you experience difficulty viewing the content while responding to the Questionnaire, please contact Supplier Risk using the link at the bottom of your screen. All information gathered in conjunction with this Questionnaire will be maintained within the United States. Highmark retains sole access to the information provided.

This electronic Questionnaire is powered by Qualtrics. For additional information regarding Qualtrics please refer to the following link: http://www.qualtrics.com/security-statement/.

Please enter the name of your company:

Prognos Health Inc.

Please provide the name(s) and job title(s) of the individual(s) responsible for completing this assessment:

Hilary Weckstein, General Counsel & Chief Privacy Officer Daniel Berlinger, Head of Technology & Chief Security Officer Aviral Srivastava, Information Security Manager Pavan Kumar, Engineering Manager

VRA 1.0 - Do information security roles and responsibilities take into consideration risk designations and/or elements based on the individuals' access level to the organization's information and information systems?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 1.1 - Are these information security job position risk designations reviewed at least every 12 months?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 1.2 - Please specify how often information security job positions and risk designations are reviewed over a 12 month period.

- [ ] Never
- [ ] Monthly
- [ ] Weekly
- [ ] Daily
- [x] Annually
- [ ] Other -

VRA 2.0 - Are job positions with information security roles and responsibilities reviewed by Human Resources and communicated to job candidates?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 2.1 - Please explain method of communication to job candidates:

Posted Job description; part of interview process

VRA 3.0 - Are job applicants required to complete an I-9 form?

- [ ] Yes
- [x] No
- [ ] Not Applicable - Please explain why

VRA 3.0.1 - Why do job applicants not complete at I-9 form? How does your organization obtain job applicant Employment Eligibility Verification information? Please explain.

Only confirmed hires complete I-9s as per Federal law.

VRA 4.0 - Do Human Resource (HR) policies require criminal background checks and other security or clearance screenings of employees, contractors, and temporary workers to be completed prior to start date?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 4.1 - Are HR policies that require criminal background checks and other security or clearance screenings reviewed and re-affirmed at least annually by management?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 5.0 - Are HR procedures documented which define background check criteria, explain why background checks are performed, and specify who is eligible to screen and perform background checks?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 6.0 - Prior to employment start date, are background checks performed on all candidates?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 6.2 - Do background checks include verification of current address, identity, and previous employment?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 6.2.2 - How long are security screening and background check records stored by the company?

- [ ] Less than 1 year
- [ ] 1 - 2 years
- [ ] 3 - 4 years
- [ ] 5 - 7 years
- [x] Greater than 7 years

VRA 6.5 - Are background checks performed for contractors and other third parties who will have access to our company's confidential information?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 7.0 - Prior to employment, are new hires, temporary workers, and contractors required to sign a Confidentiality or Non-Disclosure Agreement with your company?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 8.0 - Are employees, contractors and third party users with access to confidential information required to sign terms and conditions of employment?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 8.1 - Do the terms and conditions of employment include all of the following:
1) User's legal responsibilities
2) Responsibilities for the classification of information
3) Responsibilities for the ownership and management of organizational assets
4) Responsibilities for handling of information received from other companies or external parties
5) Responsibilities for handling of covered information
6) Responsibilities of remote access to organizational systems
7) Responsibilities for complying with all information security and privacy policies
8) Denote the conditions relating to security policies survive the completion of the employment in perpetuity?

- [x] Yes
- [ ] No

VRA 9.0 - For all company employees, contractors, and third-party users, are responsibilities for information security clearly defined and documented?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 9.1 - Do these roles and responsibilities address physical and electronic security, information security training, and human resource information security practices?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 10.0 - Are all employees, temporary workers, and contractors required to complete information security and privacy awareness training before gaining access to systems (i.e. network, applications, databases, etc.)?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 10.1 - Are all employees, temporary workers, and contractors required to complete information security and privacy awareness training within 60 days of the individual's date of service?

- [x] Yes
- [ ] No

VRA 11.0 - Are all employees, temporary workers, and contractors required to reaffirm their responsibility to maintain information security, privacy, and Confidentiality at least every 12 months?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 12.0 - Are all employees, temporary workers, and contractors with information security and privacy job roles provided training on information security and privacy policies, practices, processes, and controls?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 12.1 - How long are information security training records stored by the company?

- [ ] Less than 1 year
- [ ] 1 - 2 years
- [ ] 3 - 4 years
- [ ] 5 - 7 years
- [x] Greater than 7 years

VRA 13.0 - Are clinical staff employed or contracted by your organization?

- [ ] Yes
- [x] No
- [ ] Not Applicable - Please explain why

VRA 14.0 - Are individuals who are considered to have significant information technology roles and responsibilities required to complete more in-depth training (e.g., user access provisioning, systems or database administrators, network infrastructure, intrusion detection or firewall management)?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 14.1 - Are documented training records maintained upon completion of this role-based, in-depth information technology training?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 14.2 - Does this role-based, in-depth information technology training occur when there are significant changes to information systems or system environments?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 14.3 - Are information technology personnel required to complete any information security training at least annually?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 14.4 - Please list/describe the information security trainings that information technology personnel are taking at least annually.

Information technology personal undergo security trainings Prognos security and privacy training mainly on HIPAA AWS (Amazon Web Services) cloud security training

VRA 15.0 - Is there an Information Security Officer named within your organization?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 15.1 - Please indicate the position level held by the Security Officer.

- [ ] Manager
- [ ] Director
- [x] Vice President
- [ ] Executive
- [ ] Other - Please describe

VRA 15.1.1 - Please list the title of the Security Officer.

Head of Technology - Chief Security Officer

VRA 15.2 - Please indicate all active professional certifications and / or credentials held by the Security Officer.

- [ ] CISSP
- [ ] CISA
- [ ] SCCP
- [ ] CCFP
- [ ] PMP
- [ ] CIA
- [ ] U.S. Government Clearance
- [ ] Other - Please specify

- [x] None

VRA 15.2.1 - Does your Information Security Officer have any plans to obtain professional security certifications and/or credentials? Please explain.

Not at this time.

VRA 16.0 - Is there an information security and technology risk management program that identifies, assesses, prioritizes, and performs ongoing risk assessments and residual risk mitigation activities?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 16.1 - Please indicate what risk methodology and / or compliance framework(s) are used to complete information security risk assessments (e.g., ISO27001, NIST 800-30, COSO, COBIT, HITRUST).

HITRUST

VRA 16.2 - Please attach all assurance reports and certifications (e.g., SOC 2, HITRUST, etc) that cover the scope of services and products provided.
(Note: If providing more than 1 report, please zip the files and attach.)

HITRUST Summary Prognos CONFIDENTIAL.pdf

0.4 MB

application/pdf

VRA 16.3 - Is an information security risk assessment performed at least every 12 months?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 16.4 - Does senior management assist with risk mitigation decision making activities (e.g., avoid, accept, mitigate, transfer)?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 16.5 - Are any information security risk assessment activities conducted offshore?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 16.5.1 - What data elements of the information security risk assessment are being stored or accessed at offshore locations?

No PHI is ever stored or accessed from offshore but security operations functions can occur offshore.

VRA 17.0 - Please indicate who is provided with results of the information security risk assessment(s).

- [ ] Chief Executive Officer (CEO) / President
- [ ] Chief Information Officer (CIO)
- [x] Chief Technology Officer (CTO)
- [x] Chief Privacy Officer (CPO)
- [ ] Chief Risk Officer (CRO)
- [ ] Chief Audit Executive (CAE)
- [ ] Audit Committee
- [ ] Board of Directors
- [x] Other - Please specify

Information Security Committee

- [ ] None

VRA 18.0 - Is the management and / or maintenance of information security activities outsourced to third-parties?

- [x] Yes
- [ ] No

VRA 18.1 - Please indicate the name of the company where information security activities are outsourced to.

Only partially outsourced: AWS (Storage); Drummond Group (Pen Testing)

VRA 18.2 - Please indicate the type(s) of information security activities which are outsourced.

- [ ] Anti-Virus
- [ ] Network / Firewall Administration
- [ ] Incident Management
- [ ] Infrastructure (Hosted)
- [ ] Information Security Risk Assessments
- [ ] Intrusion Detection
- [x] Software as a Service (SaaS)
- [x] Storage (Cloud)
- [ ] Backup / Redundancy
- [ ] Help Desk / Troubleshooting
- [ ] Workstation / Server Installation and Maintenance
- [ ] User Access and Password Management
- [x] Vulnerability Assessments / Penetration Tests
- [ ] Other - Please specify

VRA 19.0 - Do the individuals responsible for day-to-day information security operations have active professional certifications in information security?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 19.1 - What percentage of the information security workforce is credentialed?

- [ ] Less than 10%
- [x] 10% - 29%
- [ ] 30% - 59%
- [ ] 60% - 89%
- [ ] Greater than 90%

VRA 19.1.1A - Is there a plan to increase your credentialed information security workforce to 60% or greater? Please explain.

Based on the need we will evaluate the team who need to undergo the training and certification

VRA 20.0 - Is there an Information Security policy which is communicated to all employees and contractors across the company?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 20.1 - Explain how the Information Security policies are communicated to all employees and contractors.

All policies are available on the company intranet site and monthly security reminders with links to policies are circulated to all employees. Annual training also references specific policies and procedures

VRA 20.2 - Are information security policies reviewed and reaffirmed at least annually?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 20.3 - Are information security policies communicated to part time employees, contractors, and temporary employees at or before time of hire?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 20.4 - Is there a disciplinary process for non-compliance with information security policy?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 21.0 - Is there a security incident and privacy event, escalation, and communication management policy?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 21.1 - Is it reviewed and reaffirmed at least annually?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 21.2 - Explain how the Incident Response policies and procedures are communicated to employees and contractors.

All policies are available on the company intranet site and monthly security reminders with links to policies are circulated to all employees. Annual training also references specific policies and procedures

VRA 22.0 - Are exceptions to information security policies escalated to appropriate individuals based on the level of risk associated with the exception and the authority delegated to the individual making the decision?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 22.1 - Are all information security policy exceptions documented?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 22.2 - Please explain who is responsible for reviewing and approving information security policy exceptions and how often are known exceptions reviewed?

The information security manager is responsible for documenting the exception for review and approval by the information security committee which must include either the Chief Privacy Officer or Chief Security Officer sign off

VRA 22.3 - Once security policy exceptions are initially approved, how frequently are the exceptions reviewed for validity?

- [ ] Monthly
- [ ] Quarterly
- [ ] Annually
- [ ] Never
- [x] Other - Please specify

Each exception is time boxed, usually 1-3 months depending on nature of exception and compensating controls. All exceptions are timeboxed and a reviewed prior to expiration as part of the weekly information security committee meetings

---

VRA 23.0 - Is there a data handling policy which is communicated across the company?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 23.1 - Is the data handling policy reviewed and reaffirmed at least annually?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 24.0 - Is there a security awareness training program?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 24.1 - Does information security awareness training include content on recognizing and reporting potential indicators of an insider threat?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 24.2 - Does the security awareness training program include:
1) Appropriate use of information assets (e.g., workstation logon / logoff procedures)
2) Facility physical security behavioral requirements (e.g., anti-piggybacking, ID badge display, visitor escorts)
3) Incident and contingency response training
4) (Potential) incident reporting and awareness responsibilities
5) Maintaining secure system logon credentials
6) Responsibilities to perform refresher security awareness training at least every twelve months?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 25.0 - Are individuals within your organization (or used by your organization) responsible for performing program development and logical coding activities?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 25.1 - Are these developers trained in secure coding techniques and other logical code development security practices?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 26.0A - Please select the following activities that apply to our company's data outside the United States by your company or sub contractors.

- [ ] Store
- [ ] Process
- [ ] Transmit
- [ ] Access Only
- [ ] Other - Please explain
- [x] No offshoring of our company data

VRA 27.0 - Are external and / or internal security-related audits performed on all significant information security threats at least annually?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 28.0 - Is there an internal audit, risk management or compliance department with responsibility for identifying and tracking resolution of information security issues and audit findings?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 29.0 - Have there been any information security breaches in the past twelve (12) months that either did or could have compromised the information processed, stored, or managed based on the nature of your company's agreement(s) with us?

- [ ] Yes
- [x] No
- [ ] Not Applicable - Please explain why

VRA 30.0 - Is confidential information encrypted at rest and/or in storage?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 30.1 - Is confidential information encrypted while in transit over public or unsecure networks (e.g., the Internet)?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 30.4 - Please describe the encryption approach (e.g., full disk, virtual disk, volume disk, file and folder).

Full Disk encryption is applied on all laptops. For Mac, we use and for windows machine, we use bit locker encryption. All data storage in production (S3) is encrypted using AWS S3 server side encryption

VRA 30.5 - Please describe the encryption approach (e.g., SSL, TLS).

They both use the AES-XTS mode of AES with 128 bit blocks and a 256 bit key to encrypt the disk

VRA 30.6 - Are encryption and key management policies and procedures documented?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 30.7 - Are encryption keys encrypted prior to sharing with another individual, customer, or third party?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 31.0 - Is there an Incident Response policy?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 31.1 - Is the Incident Response policy reviewed and re-affirmed by appropriate constituents (e.g., Information Security, Privacy, Operations, Business Continuity) at least every 12 months?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 32.0 - Are security incidents promptly reported to responsible individual(s) for investigation?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 33.0 - Does the organization maintain an Information Security and Privacy Incident Response plan?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 33.1 - Is the incident response plan reviewed and revised at least every 12 months?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 33.2 - Does the Incident Response plan contain a clear communication and escalation path?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 34.0 - Is there an information security incident response team ready to be deployed in the event of known or suspected unauthorized access to confidential information?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 35.0 - Is there a process to provide notification to internal and external customers in the event of unauthorized access, information security events, and / or a breach occurs?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 36.0 - Does your organization use SQL Server with an accessible front end application?

- [ ] Yes
- [x] No

VRA 37.0 - When an individual is accountable for performing Incident Response and / or Incident Management activities, is relevant training on your company's own Incident Management activities completed by the individual at the time of assuming responsibility?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 38.0 - Is there formal privacy awareness training for employees, contractors, volunteers (and other parties, as appropriate)?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 38.1 - Please provide frequency of privacy awareness training activities.

- [ ] Every 6 months
- [x] Every 12 months
- [ ] Every 24 months
- [ ] Every 36 months
- [ ] Other - Please explain

VRA 39.0 - Does the company maintain cyber insurance?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 39.1 - Please specify the range of coverage.

- [ ] Less than $1M
- [x] $1M - $5M
- [ ] $5M - $10M
- [ ] Greater than $10M

VRA 40.0 - Is there a "clean-desk" policy to protect confidential information within your organization?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 40.1 - Explain how the "clean desk" policy is communicated to all employees and contractors.

Policy is available to all on the company intranet and is communicated via announcement and annual training. It is also part of the handbook

VRA 40.2 - Is the "clean desk" policy reviewed and reaffirmed at least annually by applicable policy owners?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 41.0 - Is there a secure disposal of physical media (e.g., hard drives, back-up tapes, removable media) policy to protect confidential information within your organization?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 41.1 - Is the secure disposal of physical media policy reviewed and reaffirmed at least annually by applicable policy owners?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 42.0 - Is destruction of physical media (e.g., hard drives, back-up tapes, removable media) performed by a third party?

- [ ] Yes
- [ ] No
- [x] Not Applicable - Please explain why

PHI is never locally stored under any circumstances. PHI is only stored on the cloud. It cannot be downloaded onto machines or printed. Laptops are wiped and reformatted internally before re-issue but by policy do not have information downloaded

---

VRA 43.0 - Are there multiple physical security controls and intrusion detection mechanisms (e.g., door locks, access badge readers, man-traps, alarms, security cameras) in use which prevent and detect unauthorized access to facilities and secure areas?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 43.1 - Please identify all visitor physical access controls in place.

- [ ] Numbered visitor badges
- [ ] Non-numbered visitor badges
- [x] Visitor access sign-in logs
- [x] Escorted access
- [x] Other - Please describe

Security Guard at front desk; Badge required to enter building and floor

---

VRA 44.0 - Are all physical assets immediately revoked from employees, temporary workers, and contractors upon termination?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 45.0 - Is access to facilities and locations which store, transmit, and/or process our data (e.g., call centers, data centers, mail rooms, loading docks, storage rooms, filing cabinets) restricted to only appropriate personnel?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 45.1 - Please identify all physical access controls in place to monitor or prevent unauthorized access to facilities and locations which store, transmit and/or process our data.

- [ ] CCTV
- [x] Proximity badge access
- [ ] Cypher lock
- [x] Security guard
- [ ] Biometric readers
- [ ] Door alarms
- [x] Anti-piggybacking
- [ ] Other - Please explain

VRA 46.0 - Is there an Acceptable Use Policy which addresses proper and improper use of information systems (including end user computing devices, e-mail, Internet, social media, social networking, removable storage devices, etc.)?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 46.1 - Explain how the Acceptable Use policy is communicated to all employees and contractors.

Available on company intranet, annual training, circulated in handbook

VRA 46.2 - Is the Acceptable Use policy reviewed and reaffirmed at least annually by applicable policy owners?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 47.0 - Is there a Password Management policy which is communicated to all employees across the organization?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 47.1 - Explain how the Password Management policy is communicated to all employees and contractors.

Password requirements are part of Prognos' Acceptable Use Policy. All policies are available on company intranet, annual training, circulated in handbook. We also issue security reminders which previously have discussed password management

VRA 47.2 - Is the Password Management policy reviewed and reaffirmed at least annually by applicable policy owners?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 48.0 - Is access to sensitive or confidential information restricted to users on a "need to know" or "least privilege" basis?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 49.0 - Is there a formally documented process to periodically review whether access is only granted to those with a business need to know?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 49.1 - How frequently are non-administrator user access privileges reviewed?

- [x] Monthly
- [ ] Quarterly
- [ ] Annually
- [ ] Other - Please specify

VRA 49.2 - How frequently are administrative user access privileges reviewed?

- [x] Every 30 days
- [ ] Every 60 days
- [ ] Every 90 days
- [ ] Semi-annually
- [ ] Annually
- [ ] Other - Please specify

VRA 50.0 - Are users who access electronic information required to authenticate using a unique user name and password?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 51.0 - Are logs generated for applications that access, store and/or process our company's data?

- [x] Yes
- [ ] No

VRA 51.1 - Can logs be shared for applications that access, store and/or process our company's data?

- [x] Yes
- [ ] No

VRA 52.0 - Are reports of user authentication to systems available which include a date and time stamp indicator?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 53.0 - Is password reset authority restricted to authorized individuals?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 54.0 - Please identify the processes available for a user to reset or unlock user access accounts or passwords.

- [x] Help desk
- [ ] Contact administrator
- [ ] Self-service tool with challenge response questions
- [ ] Other - Please describe

VRA 55.0 - Do authentication procedures enforce the use of strong passwords and prevent password re-use?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 56.0 - Along with a user's password, are multi-factor authentication mechanisms used where our data can be accessed, processed and/or stored in your environment (e.g., token, biometric)?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 57.0 - Are remote access (Virtual Private Network (VPN)) utilities configured for at least two-factor authentication?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 57.1 - Does VPN authentication enforce unique usernames, passwords, and workstation connection encryption?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 58.0 - Are user IDs locked-out after 3 to 5 failed access attempts?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 58.1 - Is a systems administrator required to unlock the user account and / or reset the password?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 59.0 - Are user access accounts used by third party vendors / sub-contractors enabled only during the time needed?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 59.1 - Are user access accounts configured to automatically expire?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 60.0 - Is access to all electronic information immediately revoked from employees, temporary workers, and contractors upon termination?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 61.0 - Does your organization allow end users who are not IT administrators to install and execute software on their workstations (e.g., Laptop, PC, Server)?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 61.1 - What processes or controls are in place to verify non-IT administrators install company-approved programs that do not violate IT Security Policies and any software license agreements?

- [x] Automated workstation and server scans
- [x] Notification of installed programs to system administrator or security function
- [x] Whitelist of approved applications
- [x] License availability review
- [ ] Other - Please explain

VRA 61.2 - Are print jobs which generate confidential information secured (i.e. configured to be physically released by an authorized user via PIN, user credentials, ID card, etc.)?

- [ ] Yes
- [ ] No
- [x] Not Applicable - Please explain why

For resources having access to PHI, printing is disabled.

VRA 62.0 - Is there a remote access (VPN) information security policy which is communicated to all users (employees and other external parties) with remote access?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 62.1 - Explain how the remote access policy is communicated to all users with remote access.

Virtual Clean room SoP is posted on the company's intranet and also the users go through a Prognos Security and Privacy training annually

VRA 62.2 - Is the remote access policy reviewed and reaffirmed at least annually by IT Security policy owners?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 63.0 - Are all router, switches, wireless access points, and firewall configurations physically and logically secured?

- [ ] Yes
- [ ] No
- [x] Not Applicable - Please explain why

We do not have physical router, switches and WAP as we leverage AWS cloud infrastructure for this

VRA 64.0 - Is a firewall used to protect the organization's network?

- [ ] Yes
- [ ] No
- [x] Not Applicable - Please explain why

We do not have physical organization network and leverage cloud infrastructure but we have firewall enabled on our endpoints

VRA 65.0 - Are web servers located on public facing network segments separated from the internal network by a firewall?

- [ ] Yes
- [ ] No
- [x] Not Applicable - Please explain why

We do not have an internal network.

VRA 66.0 - Are changes to the firewall firmware, software, configuration, and placement subject to a change control processes?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 67.0 - Are all passwords on network devices (e.g., routers, switches, firewalls) and intrusion detection systems encrypted?

- [ ] Yes
- [ ] No
- [x] Not Applicable - Please explain why

Those systems are a service to us, we do not run the hardware directly

VRA 68.0 - Is all covered electronic information that passes through public networks encrypted?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 68.2 - Is all covered electronic information that passes through private networks encrypted?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 69.0 - Are vulnerability assessments, scans and penetration tests performed on internal and externally facing networks?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 69.1 - Are vulnerability assessments, scans and penetration tests performed at least every 12 months?

- [x] Yes
- [ ] No

VRA 70.0 - Are network devices configured to prevent communications from unapproved or untrusted networks?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 71.0 - Is wireless access to internal systems permitted?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 71.1 - Are egress and ingress filters installed on all border routers to prevent impersonation with spoofed IP addresses?

- [ ] Yes
- [x] No
- [ ] Not Applicable - Please explain why

VRA 71.2 - Do perimeter firewalls exist between wireless networks and sensitive information?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 71.3 - Is all wireless communication encrypted using industry standard encryption techniques?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 71.1.1 - Please describe if there are plans to implement egress and ingress filters. If not, what controls or processes are in place to prevent impersonation with spoofed IP addresses?

No white-listed IP address can access any data without further authentication.

VRA 72.0 - Are scans run periodically to identify unauthorized wireless devices?

- [ ] Yes
- [ ] No
- [x] Not Applicable - Please explain why

We do not control the wireless access in our HQ

VRA 73.0 - Is there an information security and configuration policy in place around software applications, servers, operating systems, databases, routers, hubs, etc.?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 73.1 - Is the configuration policy reviewed and reaffirmed at least every 12 months by applicable policy owners?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 74.0 - Does your organization have a process to formally review and verify new technology acquisitions that are in line with your strategic and operational objectives?

- [ ] Yes
- [ ] No
- [x] Not Applicable - Please explain why

We do not purchase technology in this fashion

VRA 75.0 - Is there a mobile device policy which is communicated to all employees across the organization?

- [ ] Yes
- [ ] No
- [x] Not Applicable - Please explain why

No access to systems is permitted from mobile devices.

VRA 76.0 - Is there a policy related to the secure disposal of electronic information which is communicated to all employees across the organization?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 76.1 - Is the secure disposal of information policy reviewed and reaffirmed every twelve months by applicable policy owners?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 77.0 - Is there a system software and operating system patch management policy which is communicated to applicable employees in the organization?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 77.1 - Is the system software and operating system patch management policy reviewed and reaffirmed every twelve months by applicable policy owners?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 77.2 - Does your organization have a process for applying critical vendor recommended operating system and application security updates and/or patches?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 77.3 - Does your security update and/or patch schedule include the prompt implementation of recommended updates or patches?

- [x] Yes
- [ ] No

VRA 77.4 - Does your security update and/or patch schedule include the documentation of exceptions?

- [x] Yes
- [ ] No

VRA 78.0 - Is there a change control process which ensures information security vulnerabilities or weakness are addressed when additions, deletions, and changes to information technology assets (including application systems, servers, network devices, databases, operating systems, etc.) are made?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 79.0 - Are development, quality assurance, and production application and operating system software updated with security patches?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 80.0 - Is there a removable media policy (CDs, DVDs, tapes, disk drives, USB / thumb drives, etc.) which restricts usage?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 80.1 - Is the removable media policy reviewed and reaffirmed at least annually by applicable policy owners?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 81.0 - Are there technological controls implemented which restrict the use of removable media?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 81.1 - Please specify all removable media controls.

- [x] Read / Write / Copy Prevention
- [ ] BIOS
- [x] I/O Settings
- [ ] Group Policy
- [ ] Other - Please explain

VRA 82.0 - Are users able to access data from any form of removable media (i.e., USB Drive, recordable CD, external hard drive, smart phone, etc.) without detection?

- [ ] Yes
- [x] No
- [ ] Not Applicable - Please explain why

VRA 83.0 - Is encryption required when removable media is used?

- [ ] Yes
- [ ] No
- [x] Not Applicable - Please explain why

We do not allow the use of removable media

VRA 84.0 - Is all confidential electronic information that is transported off site via physical media (tape, disk, USB / thumb drive, DVD, CD, etc.) encrypted?

- [ ] Yes
- [ ] No
- [x] Not Applicable - Please explain why

We do not allow the transport of any data via physical media

VRA 85.0 - Is our production data used for testing and development purposes?

- [ ] Yes
- [x] No
- [ ] Not Applicable - Please explain why

VRA 86.0 - Are the logs of critical infrastructure assets such as firewalls, routers, wireless access points, and authentic servers reviewed for unauthorized traffic and configuration changes?

- [ ] Yes
- [ ] No
- [x] Not Applicable - Please explain why

ClearDATA provides critical service monitoring

VRA 87.0 - Are all critical system clocks synchronized?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 88.0 - Do system security and user activity logs include date and time stamps?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 89.0 - Are there procedures in place to ensure that default passwords are changed on all information technology assets (systems, databases, routers, hubs, firewalls, etc.) before placing the asset into production?

- [ ] Yes
- [ ] No
- [x] Not Applicable - Please explain why

We do not run any of the hardware or software at this level.

VRA 90.0 - Are secure, encrypted communications sessions utilized for all remote administrator activities?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 91.0 - Is all confidential electronic information maintained on employee, temporary worker, and contractor workstation devices (laptops, desktops, smart phones, tablets, etc.) encrypted to prevent sensitive information from being compromised in the event the device is lost or stolen?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 92.0 - Are there anti-virus and anti-malware protection programs which prevent employees, temporary workers, contractors, and customers from introducing unauthorized access to, or destruction of, information assets via servers and end-user computing devices (e.g. laptops, desktops, smart phones, tablets)?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 93.0 - Is there virus / malware scanning in place at all times on servers and end-user computing devices (e.g. laptops, desktops, smart phones, tablets)?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 93.1 - Please specify how often anti-virus, anti-malware, and other system security software definitions are updated.

- [ ] Less than 12 hours
- [ ] 12 - 18 hours
- [x] 18 - 24 hours
- [ ] Greater than 24 hours

VRA 94.0 - Is there a Data Loss Prevention program in place to automatically detect and prevent the unauthorized transmission and/or storage of confidential information?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 95.0 - Is an Intrusion Detection System (IDS) implemented and calibrated to identify, alert and respond to information security attacks?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 96.0 - Is there an inventory of all information technology assets including software application systems, systems, databases and data stores, network devices, web services, etc.?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 96.1 - Does the asset inventory specify individual(s) who are considered the custodians of the company owned asset(s)?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 97.0 - Is there an information technology asset management policy which is communicated to applicable personnel?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 97.1 - Is the asset management policy reviewed and reaffirmed every twelve months by applicable policy owners?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 98.0 - Do any third parties of your organization collect, process and/or manage our confidential information?

- [ ] Yes
- [x] No
- [ ] Not Applicable - Please explain why

VRA 101.0 - Does your organization permit access to external websites including file sharing, public email, social media (e.g. Personal Box.com, Dropbox, Google Docs, Gmail, Yahoo, Hotmail, Facebook, Twitter, Snapchat, Filezilla, Torrents) that do not have a business justification?

- [ ] Yes
- [x] No
- [ ] Not Applicable - Please explain why

VRA 102.0 - Does your company provide cloud services to customers?

- [ ] Yes
- [x] No
- [ ] Not Applicable - Please explain why

VRA 103.0 - Please describe your data retention/destruction schedule and how customer data is removed, returned, and/or destroyed in the cloud and/or any other means of storage (e.g. NAS, database).

Data retention is for 90 days unless otherwise negotiated. Any storage we may directly control is scrub and zero'ed as per NIST guidelines

VRA 104.0 - Does your company have a Bring Your Own Device (BYOD) program?

- [ ] Yes
- [x] No
- [ ] Not Applicable - Please explain why

VRA 109.0 - Does your company use Microsoft Operating System products?

- [ ] Yes
- [x] No

VRA 110.0 - Does your company have technical safeguards in place to prevent and detect Denial of Service (DDoS) attacks?

- [x] Yes
- [ ] No

VRA 111.0 - Please estimate the number of records which contain our company's confidential information that your company has the ability to access, process and/or store within a calendar year.

- [x] Less than 10,000 records
- [ ] 10,000 to 100,000 records
- [ ] 100,000 to 1,000,000 records
- [ ] 1,000,000 to 10,000,000 records
- [ ] Greater than 10,000,000 records

VRA 112.0 - Does your organization have a Business Continuity Plan (BCP)?

- [x] Yes
- [ ] No

VRA 112.1 - Is the BCP reviewed and updated every 12 months?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 112.2 - Does the BCP contain a clear communication and escalation path to all employees?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 112.3 - Does the BCP cover all of the locations from which our company data will be stored, transmitted, and/or processed?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 113.0 - Does your organization have a Disaster Recovery Plan?

- [x] Yes
- [ ] No

VRA 113.1 - Is the Disaster Recovery Plan reviewed, tested, and revised every 12 months?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 114.0 - Does your organization have an incident response, crisis management, and/or recovery plan specific to ransomware attacks and exploits?

- [x] Yes
- [ ] No
- [ ] Not Applicable - Please explain why

VRA 115.0 - Have any of your systems been infected by ransomware to date?

- [ ] Yes
- [x] No

VRA 116.0 - Identify all Spectre and Meltdown vulnerability remediation activities your organization is under-taking:

- [ ] Apply BIOS fix for each impacted Original Equipment Manufacturer (OEM) (e.g., HP, Dell)
- [x] Operating System Patch(es)
- [ ] Other - Please describe

VRA 117.0 - When is the anticipated date of Spectre/Meltdown remediation plan completion? (mm/dd/yyyy)

12/31/2018

European Union (EU) Data Protection Law

Note: As of May 25, 2018 the General Data Protection Regulation (GDPR) (http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf) is effective and requires full compliance of all relevant data controllers and data processors.

EUP 1.0 - Is your organization a recipient of European Union (EU) "personal data" which includes any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person? Being a "recipient" includes access to personal data that is stored in the EU/European Economic Area (EEA).

- [ ] Yes
- [x] No

EUP 7.0 - Do your organization's employees, contractors, volunteers, and/or others have access to European Union (EU) personal data, as defined in EUP 1.0?

- [ ] Yes
- [x] No

EUP 8.0 - Do your organization's third-parties or subcontractors (sub-processors) have access to personal data, as defined in EUP 1.0?

- [ ] Yes
- [x] No

EUP 20.0 - Has your organization been subject of a privacy-related proceeding, inquiry or audit of an EU data protection agency, or any US agency, or a law suit or threatened law suit of a data subject under applicable data protection law against your organization?

- [ ] Yes
- [ ] No

<< Previous

Next >>

Please direct all questions, clarification requests and survey support inquiries to supplierrisk@highmark.com.
