CANADIAN™ HEARING SERVICES

Video Remote Interpreting Platform

Security/Best Practices

July 2020

OVERVIEW

Canadian Hearing Services (CHS) has undertaken careful consideration in the design and deployment of the VRI platform to ensure the highest level of security and reliability.

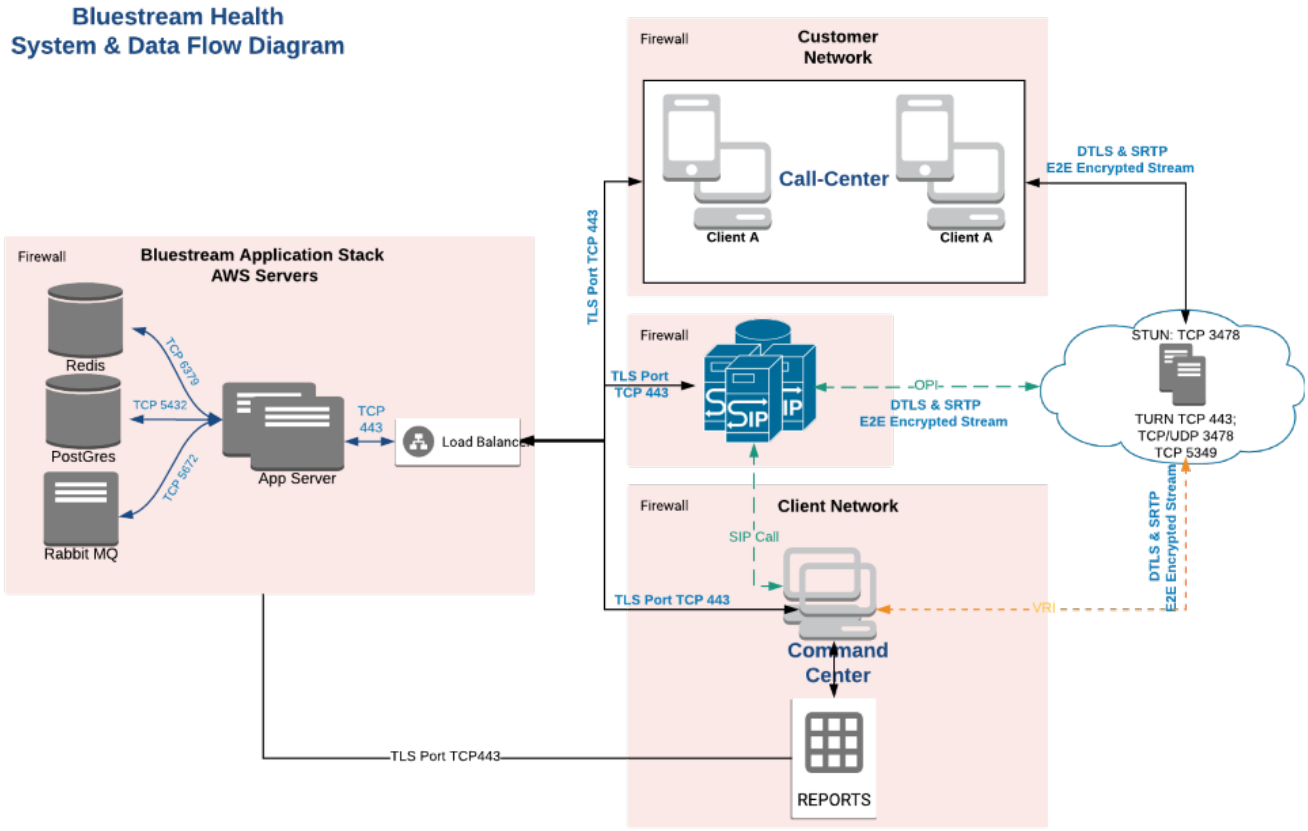
The CHS-VRI platform is built on a proprietary web-based platform leveraging WebRTC that is compliant with PIDEDA, PHI and HIPAA. The CHS-VRI platform enables high quality video conferencing and collaboration services.

This document is a security overview based on the AICPA guide to reporting on controls at a service organization relevant to three trust principles of security, availability, and privacy in alignment with the needs of the CHS-VRI platform. It is structured in a question-answer format and intended to be a comprehensive document to cover current and future CHS clients' security inquiries, as well as potential security audits. Accordingly, this document is structured under the following system components that are evaluated during a typical audit:

1. Infrastructure: an illustration of the physical and virtual components of the system and how they securely interconnect.
2. Software: a description of the programs and operating software of the system including results of external security tests.
3. People: a list of the personnel involved in the operation and use of the system with associated access permissions.
4. Procedures: a document of the automated and manual procedures involved in the operation of the system.
5. Data: a catalogue of the information used, stored and supported by the system.

INFRASTRUCTURE

Have you illustrated how the physical and virtual components of the system interconnect? (include a network architecture diagram to show VPNs, firewalls, servers, etc.)



1. **WHICH CLOUD PLATFORM ARE YOU OPERATING ON?**

   Canadian Hearing Services CHS-VRI platform is a white-label solution of the Bluestream Health platform which is hosted on Amazon Web Services (AWS) with all data residing in Canada. CHS also utilizes bespoke interpreting booking software for appointments that runs locally in a separate secured data centre. The two systems are not connected.

2. **WHERE ARE YOUR DATA SERVERS LOCATED?**

   The AWS data centre is located in the Canada Central Region (Montreal). The other local data centre is hosted internally at the Canadian Hearing Services head office located at 271 Spadina Road, Toronto.

3. **ARE YOUR SERVERS HARDENED ACCORDING TO THE NIST STANDARD?**

   No, NIST standard is not part of our PII compliance framework.

4. **WHAT IS YOUR SERVER REDUNDANCY AND/OR REPLICATION LIKE?**

   All servers are running with redundant servers in another location as well as daily, weekly and monthly backups to a cloud service provider with a data center located in Canada.

5. **WHAT IS YOUR SERVER UPTIME AND IS THIS DOCUMENTED IN AN SLA?**

   99.999%. Yes, documented in License Agreement.

6. **DOES YOUR CLOUD PLATFORM HAVE SECURITY CERTIFICATIONS?**

   AWS has SOC 1, 2 and 3 and ISO27001 certifications as documented here: https://aws.amazon.com/compliance/programs/

   Bluestream Health platform on AWS is HIPAA and as well as PIDEDA compliant.

7. **HAVE YOU IDENTIFIED POTENTIAL THREATS TO THE SYSTEM USING VULNERABILITY SCANS, PENETRATION TESTING, AND/OR SECURE CODE REVIEWS?**

   We run weekly vulnerability scans and all code is put under code review before deployment.

8. **HOW OFTEN ARE THESE TESTS PERFORMED?**

   These are performed weekly.

9. **DO YOU EMPLOY THE USE OF PRIVATE NETWORKS FOR ADDITIONAL CLOUD SECURITY?**

   Production database and other non-public servers' access is restricted to production servers (no public IP address for servers).

SOFTWARE

10. **IS SOFTWARE, HARDWARE, AND INFRASTRUCTURE UPDATED REGULARLY AS NECESSARY?**

    Due to the secure web-based platform, CHS-VRI does not require any downloads or software applications. All that is required is access to the internet and the ability to open internet webpages either through Internet Explorer or Google Chrome. The CHS-VRI platform is updated based on the AWS hardware and infrastructure update schedule.

11. **HAVE YOU IMPLEMENTED AN ACCESS CONTROL SYSTEM AND IMPLEMENTED MONITORING TO IDENTIFY INTRUSIONS?**

    AWS Guard Duty is run across BlueStream production environment.

12. **DOES THE WEB SERVER HOSTING THE APPLICATION HAVE A VALID SSL CERTIFICATE? (DESCRIBE THE ISSUING SSL AUTHORITY AND EXPIRATION)**

    Yes. For our AWS Canada instance, it is issued by Amazon and expires on January 18, 2022. There are no other security certifications outside of AWS Canada. SOC2 certification is underway.

13. **DO YOU USE 2-FACTOR AUTHENTICATION?**

    All AWS access accounts use multi-factor authentication in addition to a strong password.

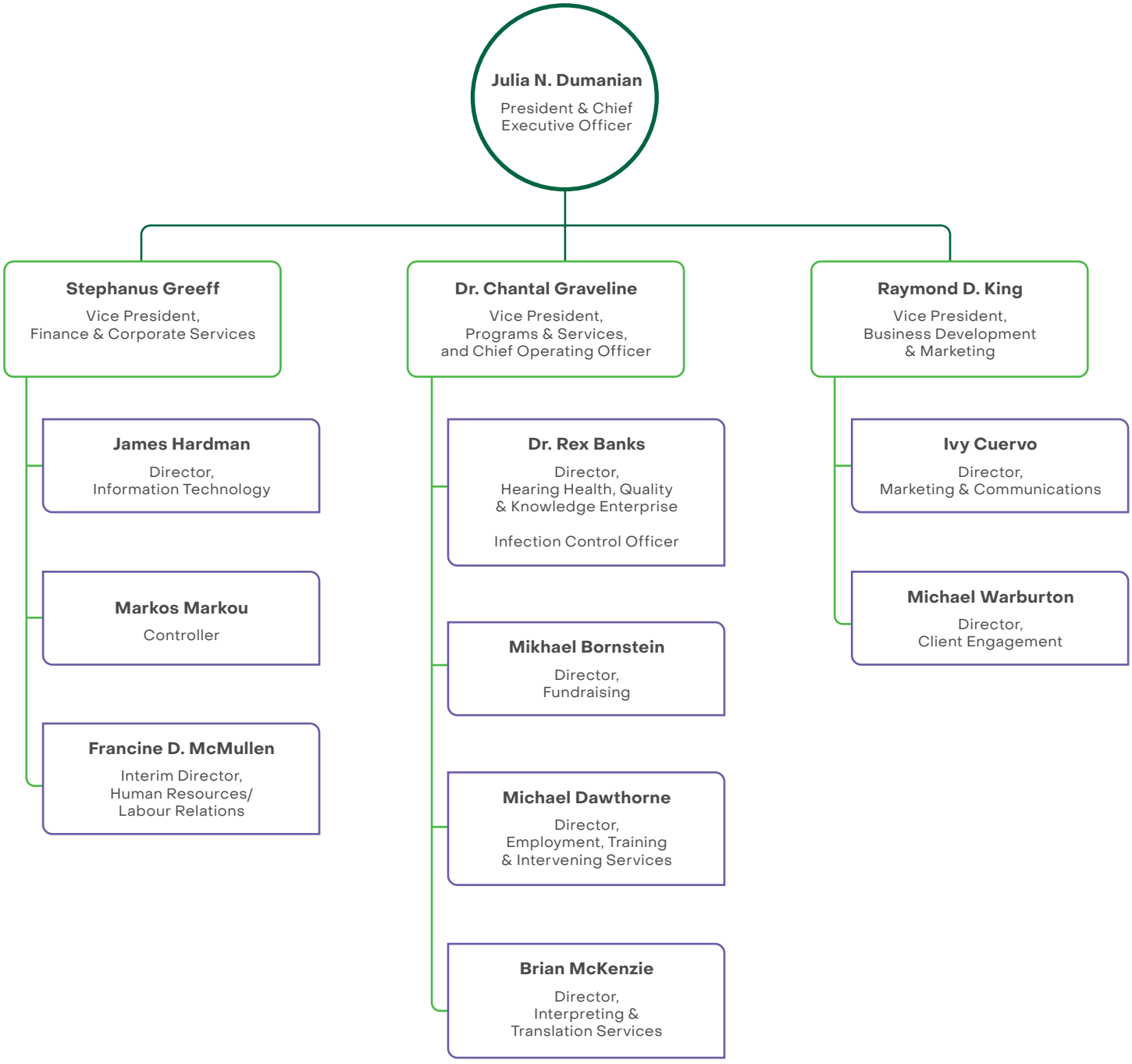
14. **HOW ARE USERS AUTHENTICATED?**

    User authentication done using Json Web Tokens (JWT) that are verified by server on each request. JWTs are digitally signed using HMAC SHA-256 to prevent forging. JWTs come with short expiration dates and need to be refreshed regularly during a user session. JWTs required for all secured server queries. API calls are limited by user role authorization, user clients without proper roles cannot attempt API calls.

"No Trust" policy with user interface code, backend servers do not depend on client for any security. WebRTC->WebRTC calls are encrypted on an end-to-end level, if a relay (TURN) server is used to connect the call it will not have the ability to decrypt the call.

PEOPLE

15. DO YOU HAVE A DEFINED ORGANIZATIONAL STRUCTURE?



16. HAVE YOU DESIGNATED AUTHORIZED EMPLOYEES TO DEVELOP AND IMPLEMENT POLICIES AND PROCEDURES?

For technical policies and procedures belongs to the Information Technology Department, Jim Hardman, Director, Information Technology and operational policies belong to Human Resources.

17. IS ACCESS TO DATA, SOFTWARE, FUNCTIONS, AND OTHER IT RESOURCES LIMITED TO AUTHORIZED PERSONNEL BASED ON ROLES?

Yes.

All appointments or on demand services are booked through our Interpreting Services Call Centre located in Ottawa, Ontario.

All VRI services are collected by specific staff and entered into the CHS scheduling database. Access to the database is limited by role, and only dedicated interpreting team-members have access to the health care organization information.

Access to our database equally requires username and password, and staff have role-limited access to data. Data containing organization information is separated from all other data.

For on-demand services, organizations will have a dedicated URL that will be the organization URL as well as department like so: https://facilities.organizationname.vri-chs.ca. For example, Smith River Hospital would be:

https://xray.smithriverhospital.vri-chs.ca

https://cardiology.smithriverhospital.vri-chs.ca

This approach provides clear location-based services based on client requirements. Only staff members in that department would have access to their department login information. Statistics can be gathered to provide department by department usage of the services.

18. HAVE YOU RESTRICTED PHYSICAL ACCESS TO SENSITIVE LOCATIONS TO AUTHORIZED PERSONNEL ONLY?

Employee access to production servers is heavily restricted and requires temporary fully logged permissions for specific time frames to prevent internal leaks.

PROCEDURES

19. HAVE YOU DEVELOPED AND TESTED INCIDENT RESPONSE PROCEDURES?

CHS has formal processes in place to address any information security incident. This was also part of our most recent Accreditation Canada process. Through our Incident Report policy, we have a process that would address any security situation from the outset through to conclusion.

20. HAVE YOUR RECOVERY PLAN PROCEDURES BEEN TESTED ON A PERIODIC BASIS AND DOCUMENTED?

Yes, we do yearly reviews of our disaster recovery site.

21. WHAT ARE YOUR BACKGROUND SCREENING PROCEDURES?

All CHS staff require system and security clearance to access our IT systems, which includes the VRI platform and scheduling software, all of which are self-contained and follow our strict privacy policies.

Do you have established workforce conduct standards?

Yes, we have two policies in terms of workforce conducts. They are the "Business Code of Conduct and Principles of Services guidelines that all staff are expected to follow.

22. DO YOUR CLIENTS AND EMPLOYEES UNDERSTAND THEIR ROLE IN USING YOUR SYSTEM OR SERVICE?

CHS Interpreters and employees must equally follow a comprehensive Confidentiality and Privacy Policy, which is applied not only to our customers, but apply equally in all aspects of our everyday business operations.

In addition, all CHS-VRI services are delivered from dedicated VRI Suites which are secure, private and sound-proofed VRI rooms located within dedicated CHS offices across Canada. These CHS-VRI suites are equipped with state of the art VRI technology including High-Definition video cameras, headsets, and reliable high-speed internet access.

23. DO YOU PERFORM REGULAR VENDOR MANAGEMENT ASSESSMENTS?

We utilized a procurement procedure and review our vendor relationships every 3 years.

24. DO YOU HAVE AN ANNUAL POLICY AND PROCEDURE REVIEW IN PLACE?

Yes, all our policies and procedures are reviewed annually.

25. WHAT IS YOUR PASSWORD POLICY?

The password policy for the CHS-VRI application is that passwords must be at least 8 characters long. Passwords cannot be in list of 10,000 most common passwords (including variations). Password cannot be recently used (admin only). All passwords are hashed with a unique salt, then the hash is encrypted before stored in database so even if database column in DB was leaked, passwords are safe.

All password are required to change every 90 days.

26. HOW OFTEN ARE PASSWORDS CHANGED?

Administrator passwords must change every 90 days (admin only).

DATA

27. WHAT ARE YOUR DATA BACKUP AND RECOVERY POLICIES?

Our back up policies is all data is back-up daily, weekly and monthly. Off-site cloud back-up in Canada as well as tape back-up to storage based on data retention policy.

28. DO YOU HAVE A FULLY DOCUMENTED DATA RETENTION POLICY?

Yes, we have a full documented data retention policy.

29. HOW ARE YOU ENSURING DATA IS BEING PROCESSED, STORED, AND MAINTAINED, ACCURATELY AND TIMELY AS COMMITTED?

User machines store no application data other than session tokens (JWTs) which expire frequently. Public-facing application servers do not store any business data such as login information, records of calls, user data, client information. All business data is stored on non-publicly accessible encrypted databases. Active data such outstanding calls, remote expert status, etc. are stored in a secured non-publicly accessible Redis Server. No user interfaces except Administrative Portals have any access to stored data. Server logs are secured on servers and access is restricted as strongly as any other data. All database queries are properly escaped at Database Abstraction Object/Service level, even if query data comes from a hard-coded string, constant, or other trusted source

30. HOW ARE YOU PROTECTING CONFIDENTIAL INFORMATION (PII) AGAINST UNAUTHORIZED ACCESS, USE, AND DISCLOSURE?

Encryption is based on AES-256. PII is individually encrypted when saved to prevent loss, and hides data from employees who may have database access. Any access to PII is logged, and access is individually white listed per use case. Server logs are sanitized of PII to prevent information leakage.

31. IS DATA ENCRYPTED AT REST AND IN TRANSIT?

Encryption based on AES-256. Databases are encrypted, preventing data loss from physical security breach on AWS. Password hashes are encrypted for added security layer. Production servers can only be accessed through an HTTPS/SSL protocol (port 443).

32. IS SOURCE CODE BEING STORED IN A SECURE REPOSITORY?

Yes. Additionally, API secret keys are not checked in to the code repository. MFA shared secrets are not checked in to code repository. Any other key, password, or protected values are not checked in to code repository.