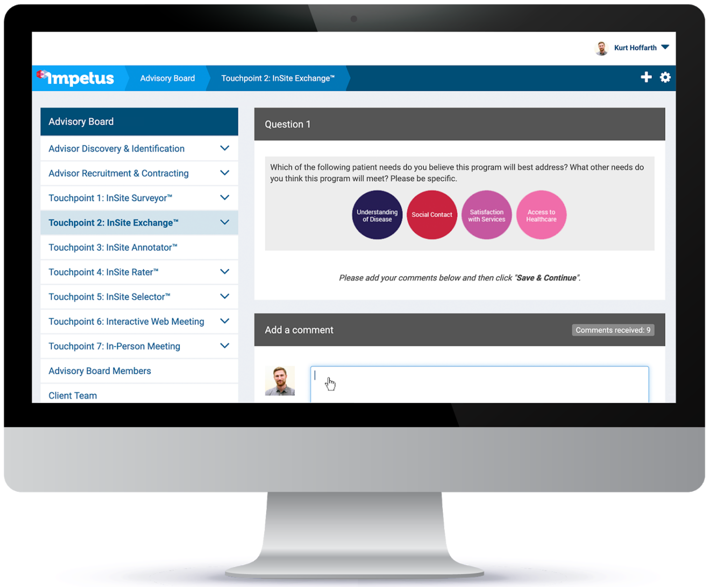
Impetus InSite Platform® Security White Paper

Compliant Synchronous and Asynchronous Virtual Collaboration


Kurt Hoffarth
Impetus
Advisory Board
Touchpoint 2: InSite Exchange™
Advisory Board
Advisor Discovery & Identification
Advisor Recruitment & Contracting
Touchpoint 1: InSite Surveyor™
Touchpoint 2: InSite Exchange™
Touchpoint 3: InSite Annotator™
Touchpoint 4: InSite Rater™
Touchpoint 5: InSite Selector™
Touchpoint 6: Interactive Web Meeting
Touchpoint 7: In-Person Meeting
Advisory Board Members
Client Team
Question 1
Understanding of Disease
Social Contact
Satisfaction with Services
Access to Healthcare
Add a comment
Comments received: 9

Which of the following patient needs do you believe this program will best address? What other needs do you think this program will meet? Please be specific.

*Please add your comments below and then click "**Save & Continue**".*

Last updated: May 2020

Quick facts

Asynchronous collaboration platform security

The Impetus InSite Platform® is 100% pharma-compliant, with over 11 years of IT assessments and penetration tests under its belt. It is rigorously tested on an on-going basis, and a number of fail-safes are in place. All employees who interact with the platform and/or client data also go through annual data handling policy reviews and training. Among other features and protocols, Impetus Digital's technology employs:

- ✓ Robust identity management, password enforcement, and access control systems
- ✓ Thorough regression testing executed for each new feature or update deployed
- ✓ Cutting-edge intrusion detection and prevention systems
- ✓ Automated daily backups, encrypted in transfer and at rest
- ✓ Automated SSL renewals to prevent issues with HTTPS connectivity
- ✓ Ongoing security updates to frameworks, open source modules, and operating systems
- ✓ Region-specific cloud hosting
- ✓ Adherence to the following IT Standards:

EU-US and Swiss-US Privacy Shield	GDPR	ISO 27001 ISO 20017 ISO 27018	SOC I SOC II SOC III	PIPEDA	HIPAA	Innovative Medicines Canada

Please see the Asynchronous collaboration platform security section below for more details.

Synchronous collaboration platform security

Your IT department will approve of the secure technology and protocols used in the planning, hosting, and reporting of your web meeting or webinar. We can assure you that Impetus Digital's web meeting services and technology management protocols employ numerous safeguards to ensure a private and secure meeting experience. Specifically, we employ:

- ✓ Strict control over screen sharing, annotation, polls, audio/muting, and webcam sharing
- ✓ Unique meeting IDs and Impetus-specific meeting URLs
- ✓ Careful sharing of meeting links through restricted calendar invites
- ✓ Vetting of logged-in attendees vs. list of invitees
- ✓ Meeting-specific passwords
- ✓ Enterprise-level accounts (not consumer-level)
- ✓ Minimal collection of personal information for participant registration and identification

Please see the Synchronous collaboration platform security section below for more details.

Asynchronous collaboration platform security

This part of the white paper provides an overview of the measures Impetus Digital takes in securing data on the Impetus InSite Platform® and is divided into the following sections: hardware redundancy and physical security, data protection, network security, application software security, and internal policies.

Hardware redundancy and physical security

All of the hardware that runs every portal is owned and managed by Google Cloud Platform. Google Cloud Platform is a service provider that hosts hundreds of thousands of cloud based solutions for their various clients and Google's own services.

Numerous security measures included within our hardware are:

- All hardware uses industry-standard practices for on-disk storage, including writing to multiple physical disks with hardware-level RAID.
- We at Impetus also take into account power outages by equipping our data center machines with Uninterruptible Power Supplies and N+1 redundant Uninterruptible Power Supplies for every server and on-site diesel generators in the event of prolonged power outages. All of this equipment will ensure that your portal is up and running no matter what.
- Impetus and our Google Cloud Platform partners make sure that there are a number of physical security measures put in place to ensure that no unauthorized people get into our datacenter premises. These measures include:
    - Keycard protocols, biometric scanning protocols, and around-the-clock interior and exterior surveillance.
    - Access limited to authorized data center personnel.
    - Stringent security background checks on data center employees.
- An addition to this, our facilities are equipped with advanced fire suppression systems to make sure that none of your data is lost.

Data protection

In the event that we need to restore portal data to a time in the past, or dig into past data that was accidentally deleted, our infrastructure is well equipped to provide this kind of functionality. We provide the following services that protect your data:

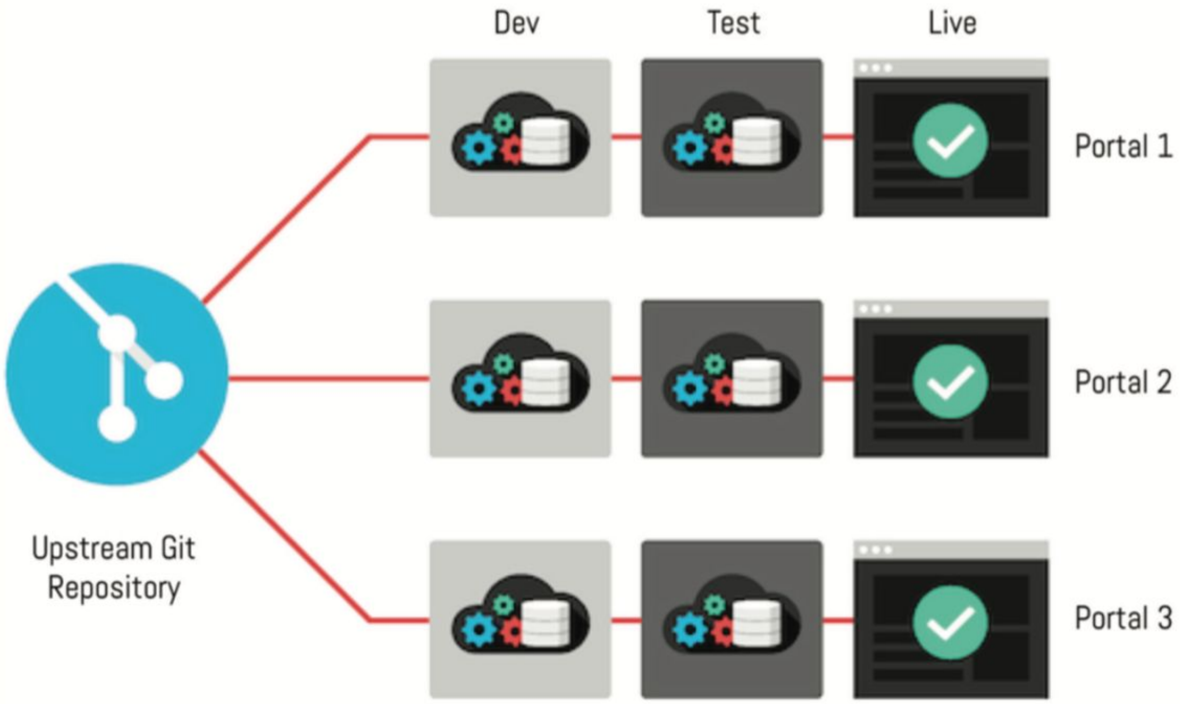
Automated and secure data backups and redeployment process

All Impetus-hosted portals are backed-up daily, automatically, and sites can be redeployed in as little as 30 minutes. Backup retention is 2 weeks (snapshots for each of the past 14 days), and snapshots can be restored to live or picked apart on a separate development environment. Each backup, containing all site-related customer data, is security transferred to Google Cloud storage as a compressed archive.

Furthermore, backups are encrypted during transfer and at-rest with 256-bit Advanced Encryption Standard ciphers, storing private keys and encrypted backup data on separate servers.

Data separation

Customer data is logically separated from other customer data using separate databases and portal instances. Therefore, it would not be possible for one of Impetus' customers to access your portal's data or stored files. Customer-specific customizations are separated from other portals using git and other code versioning techniques.



Network security

Impetus secures its network infrastructure from all networking attacks that one would typically face at work or at home. These include viruses, worms, malware, spyware, etc. This infrastructure boasts a 99.9% average uptime throughout the year. We secure our network infrastructure by using the following tools.

Software whitelists and antivirus protection

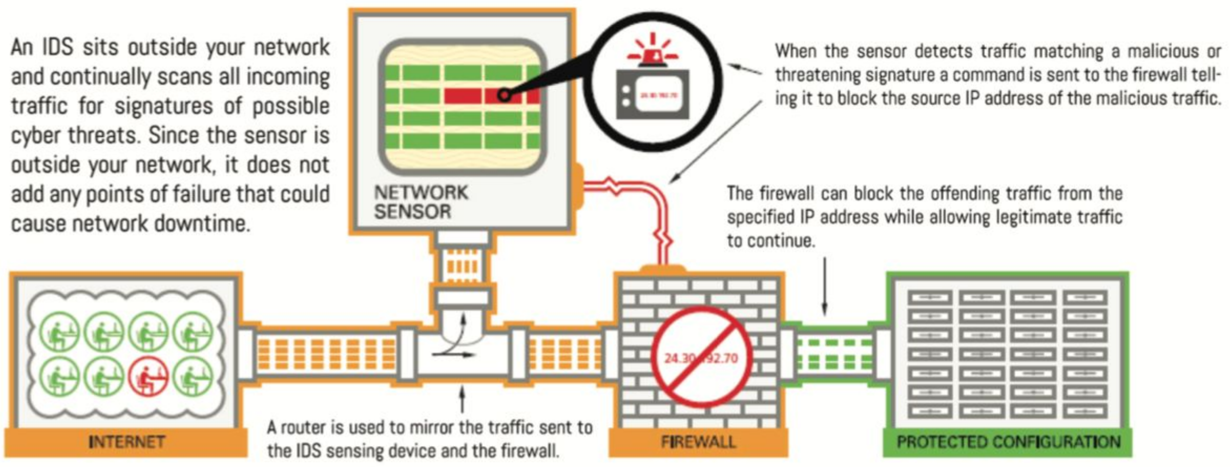
Through Linux operating systems, Impetus uses only established vendor repositories for software, and software package signature verification. It is only through these repositories that we get our server software. If any executable files were to make it past the portal's built-in security, Impetus also prevents direct execution of files uploaded through the portal.

Impetus utilizes ClamAV antivirus/anti-malware for all of its portals. It provides a high performance multi-threaded scanning daemon, and an intelligent tool for automatic signature updates. This utility's databases are updated on a regular basis.

Intrusion detection systems

In cooperation with Google Cloud Platform, Impetus implements a state of the art intrusion detection system to prevent unauthorized access to the server through root privileges and to prevent any DOS or DDOS attacks. Any intrusions will be brought to Impetus' attention via Alert Logic.

How an Intrusion Detection System Protects Your Hosted Solution



An IDS sits outside your network and continually scans all incoming traffic for signatures of possible cyber threats. Since the sensor is outside your network, it does not add any points of failure that could cause network downtime.

When the sensor detects traffic matching a malicious or threatening signature a command is sent to the firewall telling it to block the source IP address of the malicious traffic.

The firewall can block the offending traffic from the specified IP address while allowing legitimate traffic to continue.

A router is used to mirror the traffic sent to the IDS sensing device and the firewall.

In addition to Google Cloud Platform's IDS, we employ centralized IPS to detect failed logins via multiple ingress points and prevent dictionary and brute-force attacks for logging into our server as a root user, administrator or programmer. Security logs from the servers for these failed attempts are centrally collected, processed, secured and stored for 60 days. Access to servers via ssh include use of RSA key pairs in place of passwords, x.509 certificates for API and web-based administration tools, and centralized tamper-evident security log collection.

Network redundancy and load balancing

Our networking infrastructure boasts over nine network providers with a network configuration developed in collaboration with Google Cloud Platform, Cisco and Arbor Networks. We exclusively use fully redundant, enterprise-class routing equipment under managed networks. In addition to this, our fiber carriers enter at disparate points to guard against service failure.

All portal requests go through a load balancing server before being distributed to other servers and php workers deeper within our network infrastructure. This will ensure that your portal will stay up and running through peak traffic times.

Application software security

Our software is based on the popular, open source CMS Drupal, a system that is widely regarded as one of the most secure platforms in the world. Thousands of developers and a dedicated security team work to resolve reported security issues, review security concerns and provide security expertise and assistance. Furthermore, Impetus IT receives immediate notification of the latest security fixes and core upgrades; these updates are prioritized to be tested and deployed within as little as two working days.

With the rich set of APIs Drupal provides us, security flaws such as Cross Site Scripting, Insecure Direct Object References and Cross Site Request Forgeries are easily mitigated, ensuring that your platform's information stays in the right hands.

Our software is programmed using an MVC framework that separates front-end logic from back-end, ensuring easy maintainability and increased security

Secure database API

This is a robust way of accessing your data when you need it. With this API, all database calls are sanitized and enforce an interface. In addition to this, our file system interaction layer limits where files can be written and alters dangerous file extensions that the server could potentially execute.

Secure password storage

Like all good web-based password storage methods, we use one way hash functions to encrypt your passwords, specifically SHA512 via the Portably PHP Password Hashing Framework. Passwords are additionally salted before being hashed for added security.

Account security and session management

In addition to password protection, we use honeypots in order to protect against bots that want to automatically log in. Administrator accounts have an extra layer of security that disable them if there are too many failed login attempts.

All things relating to a user's session are managed by our server in order to prevent a user from escalating authorization up to the admin level. All session data is destroyed upon logging out and completely new session data is created when logging in to avoid session fixation.

Permissions system, access controls, and input filtering

Our platform has a very sophisticated permissions system that allows administrators to configure permissions for our users on the fly, whether they need more or less permissions for a particular task. New roles can also be created on the fly if permissions need to be separated.

Anything that users can store on our database and show to others are filtered for malicious code such as malicious JavaScript, malicious flash embeds, and malicious PHP code.

Code versioning systems

Impetus uses git for all of its platform software releases to ensure that code changes are logged and tracked with their associated programmer. This also ensures that per-platform customizations are done correctly and only for their intended customer. All code pushes, releases and updates require password authentication through an HTTPS connection.

Internal policies and employee training

We have a number of policies in place that allow us to ensure that your portal and the data contained within that portal are as secure as possible.

Disaster recovery, incidence reporting, and auditing

In the event that data does need to be recovered after a disaster, rest assured that your portal will be back up and running in a very short timespan. We've implemented the following to ensure the continuity of your business.

- Scheduled daily backups of all customer data are initiated within 2 hours of the scheduled time
- Backups are stored in multiple geographically distinct data centers
- Backups are encrypted for both transfer and storage
- Backups include the all files and database tables required to get a portal back up and running.
- In the event of a disaster, we will restore customer portals.

Impetus and its hosting services will consistently report and resolve any known or suspected security or privacy problems, incidents or breaches. These procedures will identify, contain and notify affected parties within 24 hours.

Our network and hosting infrastructure is subject to quarterly internal risk assessments, and leverages external risk-assessments as necessary. Known risks are catalogued by severity and added to a prioritized backlog. Impetus keeps a close relationship with external hosting partners to ensure that backlogged issues found in testing are resolved.

Compliance and privacy

Impetus conducts all of its business in compliance with all US and Canadian laws, regulations, industry guidelines and codes including, but not limited to:

- DDMAC
- Health Canada
- ASC
- Rx&D
- PAAB
- PIPEDA
- GDPR
- all anti-corruption policies

It is Impetus' policy to use the personally identifiable information Impetus acquires in Impetus communities for internal business purposes only in order to provide the services that you have requested. Impetus maintains security measures to keep this information private and agrees not to re-distribute, market, share or sell this information to others.

We use a variety of security technologies and procedures to help protect Personal Information from unauthorized access, use or disclosure. We store Personal Information on computer systems with limited access, which are located in controlled facilities. When highly confidential information is transmitted over the internet, Impetus protects it through the use of encryption technologies such as the Secure Socket Layer (SSL) protocol. See our Privacy Policy for more details.

Synchronous collaboration platform security

Impetus Digital's web meeting services and technology management protocols employ numerous safeguards to ensure a secure meeting experience, from client planning and meeting pre-work to hosting and reporting. Specifically, we employ:

- Enterprise-level accounts (not consumer-level)
- Strict control over screen sharing, annotation, polls, audio/muting, and webcam sharing
- Unique meeting IDs and Impetus-specific URLs
- Careful sharing of meeting links through restricted calendar invites
- Vetting of logged-in attendees vs. list of invitees
- Meeting-specific passwords
- Minimal collection of personal information for participant registration and identification

Meeting access is secure

- Each meeting has a unique Impetus Digital ID and is set to private
- Impetus vets all logged-in attendees against the list of invitees
- Pre-registration can be set to mandatory for all attendees
- Meeting-specific passwords are used by default
- Meetings can be locked once started (i.e. no new attendees after a certain time)
- Attendees placed in a Waiting Room until the meeting start time
- Limits to the number of attendees can be enforced

Robust web meeting host controls

Impetus Digital will always be the "meeting host" and will maintain strict control over:

- Screen sharing
- Audio and attendee muting
- Webcam Sharing
- Chat and file sharing functionality
- Annotation capabilities
- Attendee renaming

Personal information and user accounts

Meeting attendees are not required to have an account to attend a web meeting: Personal information is not collected for use of the web platform

Personal information collected to participate in an online activity within the Impetus portal (E.g. physician email addresses) is retained in accordance with our privacy policy and GDPR/PIPEDA and other jurisdictional regulations.

Web meeting service comparison

Impetus Digital leverages industry-standard web meeting collaboration technologies in the delivery of its web meeting professional services. Zoom is our preferred virtual meeting technology for a number of reasons:

- Regardless of the meeting type (standard web meetings, internal collaboration meetings, training sessions, etc.), meeting tools like breakout rooms, polling, whiteboarding, optimized video sharing, and virtual backgrounds are standard — there's no need to request extra subscriptions or add-ons, which result in delays and extra fees
- Zoom has the most robust feature set and granular permissions options on the market.
- Zoom has multilingual meeting support (i.e. real-time interpretation)
- Zoom has virtual background replacement, which our clients often use to create a professional branded experience
- Zoom has undisputed connection reliability; we have rigorously tested it against several other meeting tools on the market and have found it provides the most reliable connection

With this said, Impetus Digital is happy to work with your team if another web meeting platform is required by your compliance/IT department. As of May 2020, Webex Training is the closest professional-grade alternative to Zoom, however it presents a number of limitations and has overall lower user satisfaction ratings. Here is a high-level comparison of key features:

	Zoom	**Webex Training**
Login requirements	Meeting ID and numerical password	Session ID, name, email, and session password made up of uppercase letters, lowercase letters and number
Time to join	Typically <1 minute	Typically 1-2 minutes
Computer audio	Available	Available
Phone audio	Available	Available
Multilingual support	Real time interpretation available	Not available
Webcam sharing	Available	Available
Virtual backgrounds for webcam video	Available	Not available on PC, only through certain iOS devices
Ability to see webcams when presenting	Available	Can only see two speakers at a time when presenting

Gallery/speaker view	Available	Not available
Screen sharing	Available	Available
Optimized video and audio clip streaming	Available	Not available
Whiteboarding	Available	Available
Annotations	Available	Available
Record meetings	Available	Automatic recording is only possible with purchase of unlimited storage
Polling	Available	Available
Creating polls	Hosts and co-hosts can launch polls	Only the presenter can launch polls
Breakout rooms	Available	Available
Adjusting breakout rooms	Ability to move attendees around in breakout rooms	Unable to adjust breakout rooms while they are running. Attendees cannot enter a second breakout room
Webcams in breakout rooms	Available	Not available
Screen sharing in breakout rooms	Available	Not available for main room